IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals

- **Code of Professional Ethics**
- **IT Audit and Assurance Standards, Guidelines, and Tools and Techniques**
- **IS Control Professionals Standards**

ISACA®
Trust in, and value from, information systems

Current as of 16 August 2010

ISACA

Standards Disclaimer

ISACA has designed this guidance as of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA *Code of Professional Ethics* for IT audit and assurance professionals. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the security and control professional should apply his/her own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Standards Disclosure and Copyright Notice

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telephone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *standards@isaca.org*
Web site: *www.isaca.org*

Table of Contents

Code of Professional Ethics

ISACA sets forth this *Code of Professional Ethics* to guide the professional and personal conduct of members of the Association and/or its certification holders.

Members and ISACA Certification holder's shall:

1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.

2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.

3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.

4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.

5. Maintain competency in their respective fields and agree to undertake only those activities, which they can reasonably expect to complete with professional competence.

6. Inform appropriate parties of the results of work performed; revealing all significant facts known to them.

7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

Failure to comply with this *Code of Professional Ethics* can result in an investigation into a member's and/or certification holder's conduct and, ultimately, in disciplinary measures.

How to Use this Publication

Relationship of Standards to Guidelines and Tools and Techniques

IT Audit and Assurance Standards are mandatory requirements for certification holders' reports on the audit and its findings. IT Audit and Assurance Guidelines, and Tools and Techniques are detailed guidance on how to follow those standards. The IT Audit and Assurance Guidelines are guidance an IT audit and assurance professional will normally follow with the understanding that there may be situations where the auditor will not follow that guidance. In this case, it will be the IT audit and assurance professional's responsibility to justify the way in which the work is done. The Tools and Techniques examples show the steps performed by an IT audit and assurance professional and are more informative than IT Audit and Assurance Guidelines. The examples are constructed to follow the IT Audit and Assurance Standards and the IT Audit and Assurance Guidelines and provide information on following the IT Audit and Assurance Standards. To some extent, they also establish best practices for procedures to be followed.

Codification

Standards are numbered consecutively as they are issued, beginning with S1
Guidelines are numbered consecutively as they are issued, beginning with G1
Tools and Techniques are numbered consecutively as they are issued, beginning with P1.

Use

It is suggested that during the annual audit program, as well as individual reviews throughout the year, the IT audit and assurance professional should review the standards to ensure compliance with them. The IT audit and assurance professional may refer to the ISACA standards in the report, stating that the review was conducted in compliance with the laws of the country, applicable audit regulations and ISACA standards.

Electronic Copies

All ISACA standards, guidelines and procedures are posted on the ISACA web site at *www.isaca.org/standards*.

Glossary

A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary*.

IT Audit and Assurance Standards Overview

Issued by ISACA

The specialised nature of information technology (IT) audit and assurance and the skills necessary to perform such audits require standards that apply specifically to IT audit and assurance. One of the goals of ISACA® is to advance globally applicable standards to meet its vision. The development and dissemination of the IT Audit and Assurance Standards is a cornerstone of the ISACA professional contribution to the audit and assurance community. There are multiple levels of guidance:

- **Standards** define mandatory requirements for IT audit and assurance. They inform:
  - IT audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
  - Management and other interested parties of the profession's expectations concerning the work of practitioners
  - Holders of the Certified Information Systems Auditor™ (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.
- **Guidelines** provide guidance in applying IT Audit and Assurance Standards. The IT audit and assurance professional should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IT Audit and Assurance Guidelines is to provide further information on how to comply with the IT Audit and Assurance Standards.
- **Tools and Techniques** provide examples of procedures an IT audit and assurance professional might follow. The tools and techniques documents provide information on how to meet the standards when performing IT audit and assurance work, but do not set requirements. The objective of the IT Audit and Assurance Tools and Techniques is to provide further information on how to comply with the IT Audit and Assurance Standards.

CobiT® is an IT governance framework and supporting tool set that allows managers to bridge the gaps amongst control requirements, technical issues and business risks. CobiT enables clear policy development and good practice for IT control throughout enterprises. It emphasises regulatory compliance, helps enterprises increase the value attained from IT, enables alignment and simplifies implementation of the CobiT framework's concepts. CobiT is intended for use by business and IT management as well as IT audit and assurance professionals; therefore, its usage enables the understanding of business objectives and communication of good practices and recommendations to be made around a commonly understood and well-respected framework. CobiT is available for download on the ISACA web site, *www.isaca.org/cobit*. As defined in the CobiT framework, each of the following related products and/or elements is organised by IT management process:

- Control objectives—Generic statements of minimum good control in relation to IT processes
- Management guidelines—Guidance on how to assess and improve IT process performance, using maturity models; Responsible, Accountable, Consulted and/or Informed (RACI) charts; goals; and metrics. They provide a management-oriented framework for continuous and proactive control self-assessment, specifically focused on:
  - Performance measurement
  - IT control profiling
  - Awareness
  - Benchmarking
- *CobiT Control Practices*—Risk and value statements and 'how to implement' guidance for the control objectives
- *IT Assurance Guide*—Guidance for each control area on how to obtain an understanding, evaluate each control, assess compliance and substantiate the risk of controls not being met

A **glossary** of terms can be found on the ISACA web site at *www.isaca.org/glossary*. The words audit and review are used interchangeably in the IT Audit and Assurance Standards, Guidelines, and Tools and Techniques.

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of all proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the controls professional should apply his/her own professional judgement to the specific control circumstances presented by the particular systems or IT environment.

The ISACA Professional Standards Committee is committed to wide consultation in the preparation of the IT Audit and Assurance Standards, Guidelines, and Tools and Techniques. Prior to issuing any documents, the Standards Board issues exposure drafts internationally for general public comment. The Professional Standards Committee also seeks out those with a special expertise or interest in the topic under consideration for consultation where necessary. The Standards Board has an ongoing development programme and welcomes the input of ISACA members and other interested parties to identify emerging issues requiring new standards. Any suggestions should be e-mailed (*standards@isaca.org*), faxed (+1.847. 253.1443) or mailed (address at the end of document) to ISACA International Headquarters, for the attention of the Val IT initiative manager.

Index of IT Audit and Assurance Standards

	Effective Date
S1 Audit Charter	1 January 2005
S2 Independence	1 January 2005
S3 Professional Ethics and Standards	1 January 2005
S4 Competence	1 January 2005
S5 Planning	1 January 2005
S6 Performance of Audit Work	1 January 2005
S7 Reporting	1 January 2005
S8 Follow-Up Activities	1 January 2005
S9 Irregularities and Illegal Acts	1 September 2005
S10 IT Governance	1 September 2005
S11 Use of Risk Assessment in Audit Planning	1 November 2005
S12 Audit Materiality	1 July 2006
S13 Using the Work of Other Experts	1 July 2006
S14 Audit Evidence	1 July 2006
S15 IT Controls	1February 2008
S16 E-commerce	1February 2008

Index of IT Audit and Assurance Guidelines

		Effective Date
G1 Using the Work of Other Auditors	1 June 1998 Revised	1 March 2008
G2 Audit Evidence Requirement	1 December 1998 Revised	1 May 2008
G3 Use of Computer Assisted Audit Techniques (CAATs)	1 December 1998 Revised	1 March 2008
G4 Outsourcing of IS Activities to Other Organisations	1 September 1999 Revised	1 May 2008
G5 Audit Charter	1 September 1999 Revised	1 February 2008
G6 Materiality Concepts for Auditing Information Systems	1 September 1999 Revised	1 May 2008
G7 Due Professional Care	1 September 1999 Revised	1 March 2008
G8 Audit Documentation	1 September 1999 Revised	1 March 2008
G9 Audit Considerations for Irregularities and Illegal Acts	1 March 2000 Revised	1 September 2008
G10 Audit Sampling	1 March 2000 Revised	1 August 2008
G11 Effect of Pervasive IS Controls	1 March 2000 Revised	1 August 2008
G12 Organisational Relationship and Independence	1 September 2000 Revised	1 August 2008
G13 Use of Risk Assessment in Audit Planning	1 September 2000 Revised	1 August 2008
G14 Application Systems Review	1 November 2001 Revised	1 October 2008
G15 Audit Planning Revised		1 May 2010
G16 Effect of Third Parties on an Organisation's IT Controls		1 March 2009
G17 Effect of Nonaudit Role on the IT Audit and Assurance Professional's Independence		1 May 2010
G18 IT Governance		1 July 2002
~~G19 Irregularities and Illegal Acts 1 July 2002~~	Withdrawn	1 September 2008
G20 Reporting	1 January 2003 Revised	16 August 2010
G21 Enterprise Resource Planning (ERP) Systems Review	1 August 2003 Revised	16 August 2010
G22 Business-to-consumer (B2C) E-commerce Review	1 August 2003 Revised	1 October 2008
G23 System Development Life Cycle (SDLC) Review Reviews		1 August 2003
G24 Internet Banking		1 August 2003
G25 Review of Virtual Private Networks		1 July 2004
G26 Business Process Reengineering (BPR) Project Reviews		1 July 2004
G27 Mobile Computing		1 September 2004
G28 Computer Forensics		1 September 2004
G29 Post-implementation Review		1 January 2005
G30 Competence		1 June 2005
G31 Privacy		1 June 2005
G32 Business Continuity Plan (BCP) Review From It Perspective		1 September 2005
G33 General Considerations on the Use of the Internet		1 March 2006
G34 Responsibility, Authority and Accountability		1 March 2006
G35 Follow-up Activities		1 March 2006
G36 Biometric Controls		1 February 2007
G37 Configuration Management Process		1 November 2007
G38 Access Controls		1 February 2008
G39 IT Organisation		1 May 2008
G40 Review of Security Management Practices		1 October 2008
G41 Return on Security Investment (ROSI)		1 May 2010
G42 Continuous Assurance		1 May 2010

Index of IT Audit and Assurance Tools and Techniques

P1 IS Risk Assessment	1 July	2002
P2 Digital Signatures	1 July	2002
P3 Intrusion Detection	1 August	2003
P4 Viruses and other Malicious Code	1 August	2003
P5 Control Risk Self-assessment	1 August	2003
P6 Firewalls	1 August	2003
P7 Irregularities and Illegal Acts	1 November	2003
P8 Security Assessment—Penetration Testing and Vulnerability Analysis	1 September	2004
P9 Evaluation of Management Controls Over Encryption Methodologies	1 January	2005
P10 Business Application Change Control	1 October	2006
P11 Electronic Funds Transfer (EFT)	1 May	2007

IT Audit and Assurance Standards

Issued by ISACA. Note that translations of these standards are posted at *www.isaca.org/standardstranslations*.

S1 Audit Charter

Introduction

01 ISACA Standards contain basic principles and essential procedures, identified in bold type, that are mandatory, together with related guidance.

02 The purpose of this IS Auditing Standard is to establish and provide guidance regarding the Audit Charter used during the audit process.

Standard

03 The purpose, responsibility, authority and accountability of the information systems audit function or information systems audit assignments should be appropriately documented in an audit charter or engagement letter.

04 The audit charter or engagement letter should be agreed and approved at an appropriate level within the organisation(s).

Commentary

05 For an internal information systems audit function, an audit charter should be prepared for ongoing activities. The audit charter should be subject to an annual review or more often if the responsibilities are varied or changed. An engagement letter may be used by the internal IS auditor to further clarify or confirm involvement in specific audit or non-audit assignments. For an external IS audit, an engagement letter should be normally prepared for each audit or non-audit assignment.

06 The audit charter or engagement letter should be detailed enough to communicate the purpose, responsibility and limitations of the audit function or audit assignment.

07 The audit charter or engagement letter should be reviewed periodically to ensure the purpose and responsibility have been documented.

08 The following guidance should be referred to for further information on the preparation of an audit charter or an engagement letter:

- IS Auditing Guideline G5 Audit Charter
- COBIT *Framework*, Control objective M4

Operative Date

09 This ISACA Standard is effective for all information systems audits beginning on or after 1 January 2005.

S2 Independence

Introduction

01 ISACA Standards contain basic principles and essential procedures, identified in bold type, that are mandatory, together with related guidance.

02 The purpose of this IS Auditing Standard is to establish standards and guidance on independence during the audit process.

Standard

03 Professional Independence
In all matters related to the audit, the IS auditor should be independent of the auditee in both attitude and appearance.

04 Organisational Independence
The IS audit function should be independent of the area or activity being reviewed to permit objective completion of the audit assignment.

Commentary

05 The audit charter or engagement letter should address independence and accountability of the audit function.

06 The IS auditor should be and appear to be independent in attitude and appearance at all times.

07 If independence is impaired in fact or appearance, the details of the impairment should be disclosed to the appropriate parties.

08 The IS auditor should be organisationally independent of the area being audited.

09 Independence should be regularly assessed by the IS auditor, and management and the audit committee if one is in place.

10 Unless prohibited by other professional standards or regulatory bodies, there is no requirement for the IS auditor either to be, or to be seen to be, independent where the nature of the involvement in the IS initiative is one of a non-audit role.

11 The following guidance should be referred to for further information on professional or organisational independence:

- IS Auditing Guideline G17 Effect of Nonaudit Role on the IS auditor's Independence
- IS Auditing Guideline G12 Organisational Relationship and Independence
- COBIT *Framework*, Control objective M4

Operative Date

12 This ISACA Standard is effective for all information systems audits beginning 1 January 2005.

S3 Professional Ethics and Standards

Introduction

01 ISACA Standards contain the basic principles and essential procedures, identified in bold, that are mandatory, together with related guidance.

02 The purpose of this IS Auditing Standard is to establish a standard and provide guidance to the IS auditor to adhere to the ISACA Code of Professional Ethics and exercise due professional care in conducting audit assignments.

Standard

05 The IS auditor should adhere to the ISACA Code of Professional Ethics in conducting audit assignments.

06 The IS auditor should exercise due professional care, including observance of applicable professional auditing standards, in conducting the audit assignments.

Commentary

07 The Code of Professional Ethics issued by ISACA will be amended from time to time to keep pace with emerging trends and demands of the auditing profession. ISACA members and IS auditors should keep abreast of the latest Code of Professional Ethics and adhere to the same while discharging duties as IS auditors.

08 The IS Auditing Standards issued by ISACA are periodically reviewed for continual improvement and amended as necessary to keep pace with the evolving challenges in the auditing profession. ISACA members and IS auditors should be aware of the latest applicable IS Auditing Standards and exercise due professional care while conducting audit assignments.

09 Failure to comply with the ISACA Code of Professional Ethics and/or IS Auditing Standards can result in investigation into a member's or CISA holder's conduct and, ultimately, in disciplinary measures.

10 ISACA members and IS auditors should communicate with their team members and ensure the teams adherence to the Code of Professional Ethics and observance of applicable IS Auditing Standards in conducting audit assignments.

11 IS auditors should appropriately deal with all concerns encountered, with regard to the application of professional ethics or IS Auditing Standards during the conduct of the audit assignment. If adherence to professional ethics or IS Auditing Standards is impaired or appears impaired, the IS auditor should consider withdrawing from the engagement.

12 The IS auditor should maintain the highest degree of integrity and conduct, and not adopt any methods that could be seen as unlawful, unethical or unprofessional to obtain or execute audit assignments.

11 The following guidance should be referred to for further information on professional ethics and standards:

- IS Auditing Guideline G19 Irregularities and Illegal Acts
- IS Auditing Guideline G7 Due Professional Care
- IS Auditing Guideline G12 Organisational Relationship and Independence
- COBIT *Framework*, Control objective M4

Operative Date

12 This IS Auditing Standard is effective for all information systems audits beginning on 1 January 2005.

S4 Professional Competence

Introduction

01 ISACA IS Auditing Standards contain basic principles and essential procedures, identified in bold type, that are mandatory, together with related guidance.

02 The purpose of this IS Auditing Standard is to establish and provide guidance so the IS auditor is required to achieve and maintain professional competence.

Standard

03 The IS auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment.

04 The IS auditor should maintain professional competence through appropriate continuing professional education and training.

Commentary

05 The IS auditor should provide reasonable assurance that sufficient professional competencies (skills, knowledge and experience relevant to the planned assignment) are made available prior to the commencement of the work. If not, the IS auditor should decline or withdraw from the assignment.

06 If held, the IS auditor should meet the continuing professional education or development requirements of CISA and other audit-related professional designations. ISACA members not holding a CISA or other audit-related professional designation and involved in information system auditing should have sufficient formal education, training and work experience.

07 Where the IS auditor leads a team to conduct a review, the IS auditor must provide reasonable assurance that all the members have the appropriate level of professional competency for the work they perform.

08 The following guidance should be referred to for further information on professional competence:

- CISA certification and training material
- CISA continuing certification and education requirements
- COBIT *Framework*, Control objectives M2, M3 and M4

Operative Date

09 This IS Auditing Standard is effective for all information systems audits beginning 1 January 2005.

S5 Planning

Introduction

01 ISACA IS Auditing Standards contain the basic principles and essential procedures, identified in bold type, that are mandatory, together with related guidance.

02 The purpose of this IS Auditing Standard is to establish standards and provide guidance on planning an audit.

Standard

03 The IS auditor should plan the information systems audit coverage to address the audit objectives and comply with applicable laws and professional auditing standards.

04 The IS auditor should develop and document a risk-based audit approach.

05 The IS auditor should develop and document an audit plan that lists the audit detailing the nature and objectives, timing and extent, objectives and resources required.

06 The IS auditor should develop an audit program and/or plan and detailing the nature, timing and extent of the audit procedures required to complete the audit.

Commentary

07 For an internal audit function, a plan should be developed/updated, at least annually, for ongoing activities. The plan should act as a framework for audit activities and serve to address responsibilities set by the audit charter. The new/updated plan should be approved by the audit committee, if one is in place.

08 For an external IS audit, a plan should normally be prepared for each audit or non-audit assignment. The plan should document the objectives of the audit.

09 The IS auditor must obtain an understanding of the activity being audited. The extent of the knowledge required should be determined by the nature of the organisation, its environment, risks and the objectives of the audit.

10 The IS auditor should perform a risk assessment to provide reasonable assurance that all material items will be adequately covered during the audit. Audit strategies, materiality levels and resources can then be developed.

11 The audit program and/or plan may require adjustment during the course of the audit to address issues that arise (new risks, incorrect assumptions, or findings from the procedures already performed) during the audit.

12 The following guidance should be referred to for further information on the preparation of an audit charter or an engagement letter:

- IS Auditing Guideline G6 Materiality Concepts for Auditing Information Systems
- IS Auditing Guideline G15 Planning
- IS Auditing Guideline G13 Use of Risk Assessment in Audit Planning
- IS Auditing Guideline G16 Effect of Third Parties on an Organisation's IT Controls
- COBIT *Framework*, Control Objectives

Operative Date

13 This IS Auditing Standard is effective for all information systems audits beginning 1 January 2005.

S6 Performance of Audit Work

Introduction

01 ISACA Standards contain the basic principles and essential procedures, identified in bold type, that are mandatory, together with related guidance.

02 The purpose of this IS Auditing Standard is to establish standards and provide guidance regarding the performance of the audit work.

Standard

03 Supervision—IS audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met.

04 Evidence—During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

05 Documentation—The audit process should be documented, describing the audit work performed and the audit evidence that supports the IS auditor's findings and conclusions.

Commentary

06 The roles and responsibilities of the IS audit team should be established at the commencement of the audit, defining at a minimum decision, execution and review roles.

07 The work performed during the engagement should be organised and documented following predefined documented procedures. Documentation should include such things as the objectives and scope of the work, the audit programme, the audit steps performed, the evidence gathered, findings, conclusions and recommendations.

08 The audit documentation should be sufficient to enable an independent party to re-perform all the tasks performed during the audit to obtain the same conclusions.

09 Audit documentation should include details of who performed each audit task and their roles. As a general rule, every task, decision, step or outcome of the audit executed by a member or group of members of the team should be reviewed by another person of the team, appointed in accordance with the importance of the considered item.

10 The IS auditor should plan to use the best audit evidence attainable consistent with the importance of the audit objective and the time and effort involved in obtaining the audit evidence.

11 Audit evidence should be sufficient, reliable and, relevant and useful to form an opinion or support the IS auditor's findings and conclusions. If, in the IS auditor's judgement, the audit evidence obtained does not meet these criteria, the IS auditor should obtain additional audit evidence.

12 The following guidance should be referred to for further information on performance of audit work:

- COBIT *Framework*, Control Objectives

Operative Date

13 This IS Auditing Standard is effective for all information systems audits beginning 1 January 2005.

S7 Reporting

Introduction

01 ISACA IS Auditing Standards contain basic principles and essential procedures, identified in bold type, that are mandatory, together with related guidance.

02 The purpose of this IS Auditing Standard is to establish and provide guidance on reporting so the IS auditor can fulfill this responsibility.

Standard

03 The IS auditor should provide a report, in an appropriate form, upon completion of the audit. The report should identify the organisation, the intended recipients and any restrictions on circulation.

04 The audit report should state the scope, objectives, period of coverage and the nature, timing and extent of the audit work performed.

05 The report should state the findings, conclusions and recommendations and any reservations, qualifications or limitations in scope that the IS auditor has with respect to the audit.

06 The IS auditor should have sufficient and appropriate audit evidence to support the results reported.

07 When issued, the IS auditor's report should be signed, dated and distributed according to the terms of the audit charter or engagement letter.

Commentary

08 The form and content of the report ordinarily varies in terms of the type of service or engagement. An IS auditor may perform any of the following:

- Audit (direct or attest)
- Review (direct or attest)
- Agreed-upon procedures

09 Where the IS auditor is required to give an opinion on the control environment in terms of the engagement and there is audit evidence of a material or significant weakness, the IS auditor should be precluded from concluding that internal controls are effective. The IS auditor's report should describe material or significant weakness and the effect on the achievement of the objectives of the control criteria.

10 The IS auditor should discuss the draft report contents with management in the subject area prior to finalisation and release and includes management's comments in the final report wherever applicable.

11 Where the IS auditor finds significant deficiencies in the control environment, the IS auditor should communicate these deficiencies to the audit committee or responsible authority and disclose in the report that significant deficiencies have been communicated.

12 Where the IS auditor issues separate reports, the final report should make reference to all separate reports.

13 The IS auditor should consider and assess whether to communicate to management internal control deficiencies that are of a lesser magnitude than significant deficiencies. In such cases, the IS auditor should communicate to the audit committee or responsible authority that such internal control deficiencies have been communicated to management.

14 The IS auditor should request and evaluate appropriate information on previous report findings, conclusions and recommendations to determine whether appropriate actions have been implemented in a timely manner.

15 The following guidance should be referred to for further information on reporting:

- IS Auditing Guideline G20 Reporting
- COBIT Framework, Control objectives M4.7 and M4.8

Operative Date

16 This IS Auditing Standard is effective for all information systems audits beginning 1 January 2005.

S8 Follow-Up Activities

Introduction

01 ISACA Standards contain the basic principles and essential procedures, identified in bold type, that are mandatory, together with related guidance.

02 The purpose of this IS Auditing Standard is to establish standards and provide guidance regarding follow-up activities undertaken during an IS audit process.

Standard

03 After the reporting of findings and recommendations, the IS auditor should request and evaluate relevant information to conclude whether appropriate action has been taken by management in a timely manner.

Commentary

04 If management's proposed actions to implement reported recommendations have been discussed with, or provided to, the IS auditor, these actions should be recorded as a management response in the final report.

05 The nature, timing and extent of the follow-up activities should take into account the significance of the reported finding and the impact if corrective action is not taken. The timing of IS audit follow-up activities in relation to the original reporting should be a matter of professional judgement dependent on a number of considerations, such as the nature or magnitude of associated risks and costs to the entity.

06 A follow-up process should be established by an internal IS audit function to monitor and ensure management actions have been effectively implemented or that senior management has accepted the risk of not taking action. Responsibility for these follow-up activities may be defined in the audit charter of the function.

07 Depending on the scope and terms of the engagement, external IS auditors may rely on an internal IS audit function to follow up on their agreed recommendations.

08 Where management provides information on action taken to implement recommendations and the IS auditor has doubts about the information provided, appropriate testing or other procedures should be undertaken to ascertain the true position or status prior to concluding follow-up activities.

09 A report on the status of follow-up activities, including agreed recommendations not implemented, may be presented to the audit committee if one has been established, or alternatively to the appropriate level of entity management.

10 As a part of the follow-up activities, the IS auditor should evaluate whether findings if not implemented are still relevant.

Operative Date

11 This IS Auditing Standard is effective for information systems audits beginning 1 January 2005.

S9 Irregularities and Illegal Acts

Introduction

01 ISACA standards contain basic principles and essential procedures identified in bold type, which are mandatory, together with related guidance.

02 The purpose of this ISACA Standard is to establish and provide guidance on irregularities and illegal acts that the IS auditor should consider during the audit process.

Standard

03 In planning and performing the audit to reduce audit risk to a low level, the IS auditor should consider the risk of irregularities and illegal acts.

04 The IS auditor should maintain an attitude of professional skepticism during the audit, recognising the possibility that material misstatements due to irregularities and illegal acts could exist, irrespective of his/her evaluation of the risk of irregularities and illegal acts.

05 The IS auditor should obtain an understanding of the organisation and its environment, including internal controls.

06 The IS auditor should obtain sufficient and appropriate audit evidence to determine whether management or others within the organisation have knowledge of any actual, suspected or alleged irregularities and illegal acts.

07 When performing audit procedures to obtain an understanding of the organisation and its environment, the IS auditor should consider unusual or unexpected relationships that may indicate a risk of material misstatements due to irregularities and illegal acts.

08 The IS auditor should design and perform procedures to test the appropriateness of internal control and the risk of management override of controls.

09 When the IS auditor identifies a misstatement, the IS auditor should assess whether such a misstatement may be indicative of an irregularity or illegal act. If there is such an indication, the IS auditor should consider the implications in relation to other aspects of the audit and in particular the representations of management.

10 The IS auditor should obtain written representations from management at least annually or more often depending on the audit engagement. It should:

- **Acknowledge its responsibility for the design and implementation of internal controls to prevent and detect irregularities or illegal acts**
- **Disclose to the IS auditor the results of the risk assessment that a material misstatement may exist as a result of an irregularity or illegal act**
- **Disclose to the IS auditor its knowledge of irregularities or illegal acts affecting the organisation in relation to:**
  - **Management**
  - **Employees who have significant roles in internal control**
- **Disclose to the IS auditor its knowledge of any allegations of irregularities or illegal acts, or suspected irregularities or illegal acts affecting the organisation as communicated by employees, former employees, regulators and others**

11 If the IS auditor has identified a material irregularity or illegal act, or obtains information that a material irregularity or illegal act may exist, the IS auditor should communicate these matters to the appropriate level of management in a timely manner.

12 If the IS auditor has identified a material irregularity or illegal act involving management or employees who have significant roles in internal control, the IS auditor should communicate these matters in a timely manner to those charged with governance.

13 The IS auditor should advise the appropriate level of management and those charged with governance of material weaknesses in the design and implementation of internal control to prevent and detect irregularities and illegal acts that may have come to the IS auditor's attention during the audit.

14 If the IS auditor encounters exceptional circumstances that affect the IS auditor's ability to continue performing the audit because of a material misstatement or illegal act, the IS auditor should consider the legal and professional responsibilities applicable in the circumstances, including whether there is a requirement for the IS auditor to report to those who entered into the engagement or in some cases those charged with governance or regulatory authorities or consider withdrawing from the engagement.

15 The IS auditor should document all communications, planning, results, evaluations and conclusions relating to material irregularities and illegal acts that have been reported to management, those charged with governance, regulators and others.

Commentary

16 The IS auditor should refer to IS Auditing Guideline G19, Irregularities and Illegal Acts, for a definition of what constitutes an irregularity and illegal act.

17 The IS auditor should obtain reasonable assurance that there are no material misstatements due to irregularities and illegal acts. An IS auditor cannot obtain absolute assurance because of factors such as the use of judgement, the extent of testing and the inherent limitations of internal controls. Audit evidence available to the IS auditor during an audit should be persuasive in nature rather than conclusive.

18 The risk of not detecting a material misstatement resulting from an illegal act is higher than the risk of not detecting a material misstatement resulting from an irregularity or error, because illegal acts may involve complex schemes designed to conceal or hide events or intentional misrepresentations to the IS auditor.

19 The IS auditor's previous experience and knowledge of the organisation should assist the IS auditor during the audit. When making inquiries and performing audit procedures, the IS auditor should not be expected to fully disregard past experience, but should be expected to maintain a level of professional scepticism. The IS auditor should not be satisfied with less than persuasive audit evidence based on a belief that management and those charged with governance are honest and have integrity. The IS auditor and the engagement team should discuss the organisation's susceptibility to irregularities and illegal acts as part of the planning process and throughout the duration of the audit.

S9 Irregularities and Illegal Acts cont.

20 To evaluate the risk of material irregularities and illegal acts existence, the IS auditor should consider the use of:

- His/her previous knowledge and experience with the organisation (including his/her experience about the honesty and integrity of management and those charged with governance)
- Information obtained making inquiries of management
- Management representations and internal control sign-offs
- Other reliable information obtained during the course of the audit
- Management's assessment of the risk of irregularities and illegal acts, and its process for identifying and responding to these risks

21 The following guidance should be referred to for further information on irregularities and illegal acts:

- IS Auditing Guideline G5, Audit Charter
- COBIT Framework, control objective DS3, DS5, DS9, DS11 and PO6
- Sarbanes-Oxley Act of 2002
- Foreign Corrupt Practices Act 1977

Operative Date

22 This ISACA Standard is effective for all information systems audits beginning on or after 1 September 2005.

S10 IT Governance

Introduction

01 ISACA standards contain basic principles and essential procedures identified in bold type, which are mandatory, together with related guidance.

02 The purpose of this ISACA standard is to establish and provide guidance on IT governance areas that the IS auditor needs to consider during the audit process.

Standard

03 The IS auditor should review and assess whether the IS function aligns with the organisation's mission, vision, values, objectives and strategies.

04 The IS auditor should review whether the IS function has a clear statement about the performance expected by the business (effectiveness and efficiency) and assess its achievement.

05 The IS auditor should review and assess the effectiveness of IS resource and performance management processes.

06 The IS auditor should review and assess compliance with legal, environmental and information quality, and fiduciary and security requirements.

07 A risk-based approach should be used by the IS auditor to evaluate the IS function.

08 The IS auditor should review and assess the control environment of the organisation.

09 The IS auditor should review and assess the risks that may adversely effect the IS environment.

Additional Guidance

10 The IS auditor should refer to IS Auditing Guideline G18, IT Governance.

11 The IS auditor should review and assess the risks of the IS working environment that support business processes. The IS audit activity should assist the organisation by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems.

12 IT governance can be reviewed by itself or considered in every review carried out of the IS function.

13 The IS auditor should refer to the following guidance for further information on IT governance:

- IS Auditing Guidelines:
  - G5 Audit Charter
  - G6 Materiality Concepts for Auditing Information Systems
  - G12 Organisational Relationship and Independence
  - G13 Use of Risk Assessment in Audit Planning
  - G15 Planning
  - G16 Effect of Third Parties on an Organisation's IT Controls
  - G17 Effect of a Nonaudit Role on the IS Auditor's Independence
- COBIT *Management Guidelines*
- COBIT *Framework*, *Control Objectives*; this standard relates to all control objectives in all COBIT domains.
- *Board Briefing on IT Governance, 2nd Edition*, IT Governance Institute
- *IT Control Objectives for Sarbanes-Oxley*, IT Governance Institute
- US Sarbanes-Oxley Act of 2002 and other specific regulations could be also applicable.

Operative Date

14 This ISACA standard is effective for all information systems audits 1 September 2005.

S11 Use of Risk Assessment in Audit Planning

Introduction

01 ISACA IS Auditing Standards contain the basic principles and essential procedures, identified in bold type, that are mandatory, together with related guidance.

02 The purpose of this standard is to establish standards and provide guidance regarding the use of risk assessment in audit planning.

Standard

03 The IS auditor should use an appropriate risk assessment technique or approach in developing the overall IS audit plan and in determining priorities for the effective allocation of IS audit resources.

04 When planning individual reviews, the IS auditor should identify and assess risks relevant to the area under review.

Commentary

05 Risk assessment is a technique used to examine auditable units in the IS audit universe and select areas for review to include in the IS annual plan that have the greatest risk exposure.

06 An auditable unit is defined as a discrete segment of every organisation and its systems.

07 Determination of the IS audit universe should be based on knowledge of the organisation's IT strategic plan, its operations and discussions with responsible management.

08 Risk assessment exercises to facilitate the development of the IS audit plan should be carried out and documented at least on an annual basis. Organisational strategic plans, objectives and the enterprise risk management framework should be considered as part of the risk assessment exercise.

09 The use of risk assessment in the selection of audit projects allows the IS auditor to quantify and justify the amount of IS audit resources needed to complete the IS audit plan or a particular review. Also, the IS auditor can prioritise scheduled reviews based on perceptions of risk and contribute towards the documentation of risk management frameworks.

10 An IS auditor should carry out a preliminary assessment of the risks relevant to the area under review. IS audit engagement objectives for each specific review should reflect the results of such a risk assessment.

11 Following the completion of the review, the IS auditor should ensure that the organisation's enterprise risk management framework or risk register is updated, if one has been developed, to reflect findings and recommendations of the review and subsequent activity.

12 The IS auditor should refer to IS auditing guideline G13 Use of Risk Assessment in Audit Planning and the IS auditing procedure P1 IS Risk Assessment Measurement.

Operative Date

13 This standard is effective for IS audits beginning on or after 1 November 2005.

S12 Audit Materiality

Introduction

01 ISACA standards contain the basic principles and essential procedures identified in bold type, which are mandatory, together with related guidance.

02 The purpose of this IS auditing standard is to establish and provide guidance on the concept of audit materiality and its relationship with audit risk.

Standard

03 The IS auditor should consider audit materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures.

04 While planning for audit, the IS auditor should consider potential weakness or absence of controls and whether such weakness or absence of control could result into significant deficiency or a material weakness in the information system.

05 The IS auditor should consider the cumulative effect of minor control deficiencies or weaknesses and absence of controls to translate into significant deficiency or material weakness in the information system.

06 The report of the IS auditor should disclose ineffective controls or absence of controls and the significance of the control deficiencies and possibility of these weaknesses resulting in a significant deficiency or material weakness.

Additional Guidance

07 Audit risk is the risk of the IS auditor reaching an incorrect conclusion based upon audit findings. The IS auditor should also be aware of the three components of audit risk, namely, inherent risk, control risk and detection risk. Refer to *G13, Use of Risk Assessment in Audit Planning*, for more detailed discussion on risks.

08 While planning and performing the audit, the IS auditor should attempt to reduce audit risk to an acceptably low level and meet the audit objectives. This is achieved by appropriate assessment of IS and related controls.

09 Weakness in control is considered "material" if the absence of the control results in failure to provide reasonable assurance that the control objective will be met.

10 A weakness classified as material implies:

- Controls are not in place and/or controls are not in use and/or controls are inadequate.
- It warrants escalation.

11 A material weakness is a significant deficiency or a combination of significant deficiencies that results in more than a remote likelihood of an undesirable event(s) not being prevented or detected

12 There is an inverse relationship between materiality and level of audit risk acceptable to the IS auditor, i.e., the higher the materiality level, the lower the acceptability of the audit risk, and vice versa. This enables the IS auditor to determine the nature, timing and extent of audit procedures. For instance, when planning for a specific audit procedure, the IS auditor determines the materiality is lower, thereby increasing the audit risk. The IS auditor would then want to compensate by either extending the test of controls (reduce assessment of control risk) or extending the substantive testing procedures (reduce assessment of detection risk).

13 In determining whether a control deficiency or combination of control deficiency is a significant deficiency or a material weakness, the IS auditor should evaluate the effect of compensating controls and whether such compensating controls are effective.

14 The IS auditor's assessment of materiality and audit risk may vary from time to time, depending upon the circumstances and the changing environment.

15 The IS auditor should refer to IS Auditing Guideline *G6 Materiality Concepts for Auditing Information Systems.*

16 Refer to the following guidance for further information on audit materiality:

- IS Auditing Guidelines:
  - *G2 Audit Evidence Requirement*
  - *G5 Audit Charter*
  - *G8 Audit Documentation*
  - *G9 Audit Considerations for Irregularities*
  - *G13 Use of Risk Assessment in Audit Planning*
- COBIT 4.0, IT Governance Institute, 2005
- *IT Control Objectives for Sarbanes-Oxley*, IT Governance Institute, 2004

Operative Date

17 This ISACA standard is effective for all IS audits beginning on or after 1 July 2006.

S13 Using the Work of Other Experts

Introduction

01 ISACA standards contain the basic principles and essential procedures identified in bold type, which are mandatory, together with related guidance.

02 The purpose of this IS Auditing Standard is to establish and provide guidance to the IS auditor who uses the work of other experts on an audit.

Standards

03 The IS auditor should, where appropriate, consider using the work of other experts for the audit.

04 The IS auditor should assess and be satisfied with the professional qualifications, competencies, relevant experience, resources, independence and quality control processes of other experts, prior to engagement.

05 The IS auditor should assess, review and evaluate the work of other experts as part of the audit and conclude the extent of use and reliance on expert's work.

06 The IS auditor should determine and conclude whether the work of other experts is adequate and complete to enable the IS auditor to conclude on the current audit objectives. Such conclusion should be clearly documented.

07 The IS auditor should apply additional test procedures to gain sufficient and appropriate audit evidence in circumstances where the work of other experts does not provide sufficient and appropriate audit evidence.

08 The IS auditor should provide appropriate audit opinion and include scope limitation where required evidence is not obtained through additional test procedures.

Additional Guidance

09 The IS auditor should consider using the work of other experts in the audit when there are constraints that could impair the audit work to be performed or potential gains in the quality of the audit. Examples of these are the knowledge required by the technical nature of the tasks to be performed, scarce audit resource and time constraints.

10 An "expert" could be an IS auditor from the external accounting firm, a management consultant, an IT expert or expert in the area of the audit who has been appointed by top management or by the IS audit team.

11 An expert could be internal to an organisation or external to an organisation. If an expert is engaged by another part of the organisation, reliance may be placed on the report of the expert. In some cases this may lessen the need for IS audit coverage even though the IS auditor does not have access to supporting documentation and work papers. The IS auditor should be cautious in providing an opinion on such cases.

12 The IS auditor should have access to all work papers, supporting documentation and reports of other experts, where such access does not create legal issues. Where the expert's access to records creates legal issues and hence such access is not available, the IS auditor should appropriately determine and conclude the extent of use and reliance on the expert's work.

13 The IS auditor's views/relevance/comments on adoptability of the expert's report should form a part of the IS auditor's report.

14 The IS auditor should refer to IS Auditing Standard S6 Performance of Audit Work that states the IS auditor should obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives.

15 If the IS auditor does not have the required skills or other competencies to perform the audit, the IS auditor should seek competent assistance from other experts; however, the IS auditor should have good knowledge of the work performed but not be expected to have a knowledge level equivalent to the expert.

16 The IS auditor should refer to IS Auditing Guideline *G1 Using the Work of Other Auditors and Experts*.

17 Refer to the following guidance for further information on using the work of other auditors and experts:

- IS Auditing Guidelines:
  - *G5 Audit Charter*
  - *G8 Audit Documentation*
  - *G2 Audit Evidence Requirement*
  - *G10 Audit Sampling*
  - *G13 Use of Risk Assessment in Audit Planning*
- COBIT 4.0, IT Governance Institute, 2005
- *IT Control Objectives for Sarbanes-Oxley*, IT Governance Institute, 2004

Operative Date

18 This ISACA standard is effective for all IS audits beginning 1 July 2006.

S14 Audit Evidence

Introduction

01 ISACA standards contain the basic principles and essential procedures, identified in bold type, that are mandatory, together with related guidance.

02 The purpose of this standard is to establish standards and provide guidance on what constitutes audit evidence, and the quality and quantity of audit evidence to be obtained by the IS auditor.

Standard

03 The IS auditor should obtain sufficient and appropriate audit evidence to draw reasonable conclusions on which to base the audit results.

04 The IS auditor should evaluate the sufficiency of audit evidence obtained during the audit.

Commentary

Appropriate Evidence

05 Audit evidence:

- Includes the procedures as performed by the auditor
- Includes the results of procedures performed by the IS auditor
- Includes source documents (in either electronic or paper format), records and corroborating information used to support the audit
- Includes findings and results of the audit work
- Demonstrates that the work was performed and complies with applicable laws, regulations and policies

06 When obtaining audit evidence from a test of controls, the IS auditor should consider the completeness of the audit evidence to support the assessed level of control risk.

07 Audit evidence should be appropriately identified, cross-referenced and catalogued.

08 Properties such as the source, nature (e.g., written, oral, visual, electronic) and authenticity (e.g., digital and manual signatures, stamps) of the audit evidence should be considered when evaluating its reliability.

Reliable Evidence

09 In general terms, audit evidence reliability is greater when it is:

- In written form, rather than oral expressions
- Obtained from independent sources
- Obtained by the IS auditor rather than from the entity being audited
- Certified by an independent party
- Kept by an independent party

10 The IS auditor should consider the most cost-effective means of gathering the necessary evidence to satisfy the objectives and risks of the audit. However, the difficulty or cost is not a valid basis for omitting a necessary process.

11 Procedures used to gather audit evidence vary depending on the subject matter being audited (i.e., its nature, timing of the audit, professional judgement). The IS auditor should select the most appropriate procedure for the audit objective.

12 The IS auditor can obtain the audit evidence by:

- Inspection
- Observation
- Inquiry and confirmation
- Reperformance
- Recalculation
- Computation
- Analytical procedures
- Other generally accepted methods

13 The IS auditor should consider the source and nature of any information obtained to evaluate its reliability and further verification requirements.

Sufficient Evidence

14 The evidence can be considered sufficient if it supports all the material questions to the audit objective and scope.

15 Audit evidence should be objective and sufficient to enable a qualified independent party to reperform the tests and obtain the same results. The evidence should be commensurate with the materiality of the item and the risks involved.

16 Sufficiency is a measure of the quantity of audit evidence, while appropriateness is the measure of the quality of the audit evidence, and they are interrelated. In this context, when information obtained from the organisation is used by the IS auditor to perform audit procedures, the IS auditor should also place due emphasis on the accuracy and completeness of the information.

17 In those situations where the IS auditor believes sufficient audit evidence cannot be obtained, the IS auditor should disclose this fact in a manner consistent with the communication of the audit results.

S14 Audit Evidence cont.

Protection and Retention

18 Audit evidence should be secured against unauthorised access and modification.

19 Audit evidence should be retained after completion of the audit work as long as necessary to comply with all applicable laws, regulations and policies.

Reference

20 Refer to the following guidance for further information on audit evidence:

- IS Auditing Standard *S6 Performance of Audit Work*
- IS Auditing Guideline *G2 Audit Evidence Requirement*
- IS Auditing Guideline *G8 Audit Documentation*
- CobiT control objectives *ME2 Monitor and evaluate internal control* and *ME3 Ensure regulatory compliance.*

Operative Date

21 This standard is effective for information system audits beginning 1 July 2006.

S15 IT Controls

Introduction

01 ISACA standards contain the basic, mandatory principles and essential procedures, identified in bold type (black lettering), together with related guidance.
02 The purpose of this ISACA standard is to establish standards and provide guidance regarding IT controls.

Standard

03 The IS auditor should evaluate and monitor IT controls that are an integral part of the internal control environment of the organisation.
04 The IS auditor should assist management by providing advice regarding the design, implementation, operation and improvement of IT controls.

Commentary

05 Management is accountable for the internal control environment of an organisation including IT controls. An internal control environment provides the discipline, framework and structure for the achievement of the primary objective of the system of internal control.
06 CobiT defines control as 'the policies, procedures, practices and organisational structures, designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected'. Also, CobiT defines a control objective as 'a statement of the desired result or purpose to be achieved by implementing control procedures in a particular process'.
07 IT controls are comprised of general IT controls, which include pervasive IT controls, detailed IT controls and application controls, and refer to controls over the acquisition, implementation, delivery and support of IT systems and services.
08 General IT controls are controls that minimise risk to the overall functioning of the organisation's IT systems and infrastructure and to a broad set of automated solutions (applications).
09 Application controls are a set of controls embedded within applications.
10 Pervasive IT controls are general IT controls that are designed to manage and monitor the IT environment and, therefore, affect all IT-related activities. They are a subset of general controls, being those general IT controls that focus on the management and monitoring of IT.
11 Detailed IT controls are made up of application controls plus those general IT controls not included in pervasive IT controls.
12 The IS auditor should use an appropriate risk assessment technique or approach in developing the overall IS audit plan and in determining priorities for the effective allocation of IS audit resources to provide assurance regarding the state of IT control processes. Control processes are the policies, procedures and activities that are part of a control environment, designed to ensure that risks are contained within the risk tolerances established by the risk management process.
13 The IS auditor should consider the use of data analysis techniques including the use of continuous assurance, which allows IS auditors to monitor system reliability on a continuous basis and to gather selective audit evidence through the computer when reviewing IT controls.
14 When organisations use third parties, they can become a key component in an organisation's controls and its achievement of related control objectives. The IS auditor should evaluate the role that the third party performs in relation to the IT environment, related controls and IT control objectives.
15 The following ISACA and IT Governance Institute® (ITGI™) guidance should be referred to for further information regarding IT controls:

- Guideline G3 Use of Computer-assisted Audit Techniques (CAATs)
- Guideline G11 Effect of Pervasive IS Controls
- Guideline G13 Using Risk Assessment in Audit Planning
- Guideline G15 Planning
- Guideline G16 Effect of Third Parties on an Organisation's IT Controls
- Guideline G20 Reporting
- Guideline G36 Biometric Controls
- Guideline G38 Access Controls
- CobiT framework and control objectives

Operative Date

16 This ISACA standard is effective for IS audits beginning 1 February 2008.

S16 E-Commerce

Introduction

01 ISACA standards contain the basic, mandatory principles and essential procedures, identified in bold type (black lettering), together with related guidance.
02 The purpose of this ISACA standard is to establish standards and provide guidance regarding the review of e-commerce environments.

Standard

03 The IS auditor should evaluate applicable controls and assess risk when reviewing e-commerce environments to ensure that e-commerce transactions are properly controlled.

Commentary

04 E-commerce is defined as the processes by which organisations conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology. Therefore, it includes business-to-business (B2B) and business-to-consumer (B2C) e-commerce models.
05 The IS auditor should use an appropriate risk assessment technique or approach in developing the overall IS audit plan; it should include coverage of e-commerce environments.
06 The IS auditor should consider the use of data analysis techniques including the use of continuous assurance, which allows IS auditors to monitor system reliability on a continuous basis and to gather selective audit evidence through the computer when reviewing e-commerce activities.
07 The level of skills and knowledge required to understand the control and risk management implications of e-commerce varies with the complexity of the organisation's e-commerce activities.
08 The IS auditor should understand the nature and criticality of the business process supported by the e-commerce application prior to commencing the audit so that the results may be evaluated in a proper context.
09 The following guidance should be referred to for further information regarding e-commerce:

- Guideline G21 Enterprise Resource Planning (ERP) Systems Review
- Guideline G22 Business-to-consumer (B2C) E-commerce Review
- Guideline G24 Internet Banking
- Guideline G25 Review of Virtual Private Networks (VPN)
- Guideline G33 General Considerations on the Use of the Internet
- Procedure P6 Firewalls
- COBIT framework and control objectives

Operative Date

10 This ISACA standard is effective for IS audits beginning 1 February 2008.

IT Audit and Assurance Guidelines

Alpha list of IT Audit and Assurance Guidelines

Access Controls G38
Application Systems Review G14
Audit Charter G5
Audit Considerations for Irregularities and Illegal Acts G9
Audit Documentation G8
Audit Evidence Requirement G2
Audit Sampling G10
Biometric Controls G36
Business Continuity Plan (BCP) Review From IT Perspective G32
Business Process Reengineering (BPR) Project Reviews G26
Business-to-consumer (B2C) E-commerce Review G22
Competence G30
Computer Forensics G28
Configuration Management Process G37
Due Professional Care G7
Effect of Nonaudit Role on the IT Audit and Assurance Professional's Independence G17
Effect of Pervasive IS Controls G11
Effect of Third Parties on an Enterprise's IT Controls G16
Enterprise Resource Planning (ERP) Systems Review G21
Follow-up Activities G35
General Considerations on the Use of the Internet G33
Internet Banking G24
IT Governance G18
IT Organisation G39
Materiality Concepts for Auditing Information Systems G6
Mobile Computing G27
Organisational Relationship and Independence G12
Outsourcing of IS Activities to Other Organisations G4
Planning G15
Post-implementation Review G29
Privacy G31
Reporting G20
Responsibility, Authority and Accountability G34
Review of Security Management Practices G40
Review of Virtual Private Networks G25
System Development Life Cycle (SDLC) Review G23
Use of Computer Assisted Audit Techniques (CAATs) G3
Use of Risk Assessment in Audit Planning G13
Using the Work of Other Experts G1

IT Audit and Assurance Guidelines

G1 Using the Work of Other Experts

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S13 Using the Work of Other Experts states 'The IS auditor should, where appropriate, consider using the work of other experts for the audit'.

1.1.2 Standard S6 Performance of Audit Work states 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.2 Linkage to COBIT

1.2.1 ME2.5 states that the IS auditor should 'Obtain, as needed, further assurance of the completeness and effectiveness of internal controls through third-party reviews. Such reviews may be conducted by the corporate compliance function or, at management's request, by internal audit or commissioned to external auditors and consultants or certification bodies. Qualifications of individuals performing the audit, e.g., CISA® certification, must be ensured.'

1.3 Need for Guideline

1.3.1 The interdependency of customers' and suppliers' processing and the outsourcing of non-core activities mean that an IS auditor (internal or external) will often find that parts of the environment being audited are controlled and audited by other independent functions or organisations. This guideline sets out how the IS auditor should comply with the above standard in these circumstances. Compliance with this guideline is not mandatory, but the IS auditor should be prepared to justify deviation from it.

1.3.2 IS auditors should consider using the work of other experts in the audit when there are constraints that could impair the audit work to be performed or potential gains in the quality of the audit. Examples of these are the knowledge required by the technical nature of the tasks to be performed, scarce audit resources and limited knowledge of specific areas of audit. An 'expert' could be an IS auditor from the external accounting firm, a management consultant, an IT expert or expert in the area of the audit who has been appointed by top management or by the IS audit team. An expert could be internal or external to an organisation as long as independence and objectivity is maintained.

2. AUDIT CHARTER

2.1 Rights of Access to the Work of Other Experts

2.1.1 The IS auditor should verify that, where the work of other experts is relevant to the IS audit objectives, the audit charter or engagement letter specifies the IS auditor's right of access to this work.

3. PLANNING

3.1 Planning Considerations

3.1.1 When the IS auditor does not have the required skills or other competencies to perform the audit, the IS auditor should seek competent assistance from other experts; however, the IS auditor should have good knowledge of the work performed but not be expected to have a knowledge level equivalent to the experts.

3.1.2 When an IS audit involves using the work of other experts, the IS auditor should consider their activities and their effect on the IS audit objectives whilst planning the IS audit work. The planning process should include

- Assessing the independence and objectivity of the other experts
- Assessing their professional competence and qualifications
- Obtaining an understanding of their scope of work, approach, timing and quality control processes, including assessing if they exercised due care in creating working papers and retaining evidence of their work
- Determining the level of review required

3.2 Independence and Objectivity

3.2.1 The processes for selection and appointment, the organisational status, the reporting line and the effect of their recommendations on management practices are indicators of the independence and objectivity of other experts.

3.3 Professional Competence

3.3.1 The qualifications, experience, resources and credentials of other experts should all be taken into account in assessing professional competence.

3.4 Scope of Work and Approach

3.4.1 Scope of work and approach ordinarily will be evidenced by the other expert's written audit charter, terms of reference or letter of engagement.

3.5 Level of Review Required

3.5.1 The nature, timing and extent of audit evidence required will depend upon the significance and scope of the other expert's work. The IS auditor's planning process should identify the level of review that is required to provide sufficient reliable, relevant and useful audit evidence to achieve the overall IS audit objectives effectively. The IS auditor should review the other expert's final report, audit programme(s) and audit work papers. The IS auditor should also consider whether supplemental testing of the other expert's work is required.

4. PERFORMANCE OF AUDIT WORK

4.1 Review of Other Expert's Work Papers

4.1.1 The IS auditor should have access to all work papers created by the expert, supporting documentation and reports of other experts, where such access does not create legal issues.

4.1.2 Where the expert's access to records creates legal issues and, hence, such access is not available, the IS auditor should appropriately determine and conclude the extent of use and reliance on the expert's work.

4.1.3 In reviewing other expert's work papers, the IS auditor should perform sufficient audit work to confirm that the other expert's work was appropriately planned, supervised, documented and reviewed, to consider the appropriateness, sufficiency of the audit evidence provided by them, and to determine the extent of use and reliance on the expert's work. Compliance with relevant professional standards should also be assessed. The IS auditor should assess whether the work of other experts is adequate and complete to enable the IS auditor to conclude on the current audit objectives and document such conclusion.

4.1.4 Based on the assessment of the work of other experts' work papers, the IS auditor should apply additional test procedures to gain sufficient and appropriate audit evidence in circumstances where the work of other experts does not provide sufficient and appropriate audit evidence.

4.1.5 If additional test procedures performed do not provide sufficient and appropriate audit evidence, the IS auditor should provide appropriate audit conclusion and include scope limitation where required.

4.2 Review of Other Expert's Report(s)

4.2.1 The IS auditor should perform sufficient reviews of the other expert's final report(s) to confirm that the scope specified in the audit charter, terms of reference or letter of engagement has been met; that any significant assumptions used by the other experts have been identified; and that the findings and conclusions reported have been agreed upon by management.

4.2.2 It may be appropriate for management to provide their own report on the audited entities, in recognition of their primary responsibility for systems of internal control. In this case, the IS auditor should consider management's and the expert's reports together.

4.2.3 The IS auditor should assess the usefulness and appropriateness of reports issued by the other experts, and should consider any significant findings reported by the other experts. It is the IS auditor's responsibility to assess the effect of the other expert's findings and conclusions on the overall audit objective, and to verify that any additional work required to meet the overall audit objective is completed

4.2.4 If an expert is engaged by another part of the organisation, reliance may be placed on the report of the expert. In some cases this may lessen the need for IS audit coverage even though the IS auditor does not have access to supporting documentation and work papers. The IS auditor should be cautious in providing an opinion on such cases.

4.2.5 The IS auditor's views/comments on the adoptability and relevance of the expert's report should form a part of the IS auditor's report if the expert's report is utilised in forming the IS auditor's opinion.

5. FOLLOW-UP ACTIVITIES

5.1 Implementation of Recommendations

5.1.1 Where appropriate, the IS auditor should consider the extent to which management has implemented any recommendations of other experts. This should include assessing if management has committed to remediation of issues identified by other experts within appropriate time frames and the current status of remediation.

6. EFFECTIVE DATE

6.1 This guideline is effective for all IS audits beginning on or after 1 June 1998. The guideline has been reviewed and updated and is effective 1 March 2008.

G2 Audit Evidence Requirement

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.1.2 Standard S9 Irregularities and Illegal Acts states 'The IS auditor should obtain sufficient and appropriate evidence to determine whether management or others within the organization have knowledge of actual, suspected or alleged irregularities and illegal acts'.

1.1.3 Standard S13 Using the Work of Other Experts states 'The IS auditor should provide appropriate audit opinion and include scope limitation where required evidence is not obtained through additional test procedures'.

1.1.4 Standard S14 Audit Evidence states 'The IS auditor should obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the audit results. The IS auditor should evaluate the sufficiency of audit evidence obtained during the audit'.

1.1.5 Procedure P7 Irregularities and Illegal Acts states "Although the IS auditor has no explicit responsibility to detect or prevent irregularities, the IS auditor should assess the level of risk that irregularities could occur. The result of the risk assessment and other procedures performed during planning should be used to determine the nature, extent and timing of the procedures performed during the engagement'.

1.2 Linkage to COBIT

1.2.1 ME2.3 *Control exceptions* states 'Record information regarding all control exceptions and ensure that it leads to analysis of the underlying cause and to corrective action. Management should decide which exceptions should be communicated to the individual responsible for the function and which exceptions should be escalated. Management is also responsible to inform affected parties'.

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to guide the IS auditor to obtain sufficient and appropriate audit evidence and draw reasonable conclusions on which to base the audit results.

1.3.2 This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

2. PLANNING

2.1 Types of Audit Evidence

2.1.1 For a description of appropriate, reliable and sufficient evidence, refer to the commentary section in standard S14.

2.1.2 When planning the IS audit work, the IS auditor should take into account the type of audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability. Amongst the things to be considered are the independence and qualifications of the provider of the audit evidence. For example, corroborative audit evidence from an independent third party can be more reliable than audit evidence from the organisation being audited. Physical audit evidence is generally more reliable than the representations of an individual.

2.1.3 The IS auditor should also consider whether testing of controls has been completed and attested to by an independent third party and whether any reliance can be placed on that testing.

2.1.4 The various types of audit evidence that the IS auditor should consider using include:

- Observed processes and existence of physical items
- Documentary audit evidence
- Representations
- Analysis

2.1.5 Observed processes and existence of physical items can include observations of activities, property and IS functions, such as:

- An inventory of media in an offsite storage location
- A computer room security system in operation

2.1.6 Documentary audit evidence, recorded on paper or other media, can include:

- Results of data extractions
- Records of transactions
- Program listings
- Invoices
- Activity and control logs
- System development documentation

2.1.7 Representations of those being audited can be audit evidence, such as:

- Written policies and procedures
- System flowcharts
- Written or oral statements

2.1.8.1 The results of analysing information through comparisons, simulations, calculations and reasoning can also be used as audit evidence. Examples include:

- Benchmarking IS performance against other organisations or past periods
- Comparison of error rates between applications, transactions and users

2.2 Availability of Audit Evidence

2.2.1 The IS auditor should consider the time during which information exists or is available in determining the nature, timing, extent of substantive testing and, if applicable, compliance testing. For example, audit evidence processed by electronic data interchange (EDI), document image processing (DIP) and dynamic systems such as spreadsheets may not be retrievable after a specified period of time if changes to the files are not controlled or the files are not backed up. Documentation availability could also be impacted by company document retention policies.

2.3 Selection of Audit Evidence

2.3.1 The IS auditor should plan to use the most appropriate, reliable and sufficient audit evidence attainable and consistent with the importance of the audit objective and the time and effort involved in obtaining the audit evidence.

2.3.2 Where audit evidence obtained in the form of oral representations is critical to the audit opinion or conclusion, the IS auditor should consider obtaining documentary confirmation of the representations, either on paper or other media. The auditor should also consider alternative evidence to corroborate these representations to ensure their reliability.

3. PERFORMANCE OF AUDIT WORK

3.1 Nature of Audit Evidence

3.1.1 Audit evidence should be sufficient, reliable, relevant and useful to form an opinion or support the IS auditor's findings and conclusions. If, in the IS auditor's judgement, the audit evidence obtained does not meet these criteria, the IS auditor should obtain additional audit evidence. For example, a program listing may not be adequate audit evidence until other audit evidence has been gathered to verify that it represents the actual program used in the production process.

3.2 Gathering Audit Evidence

3.2.1 Procedures used to gather audit evidence vary depending on the information system being audited. The IS auditor should select the most appropriate, reliable and sufficient procedure for the audit objective. The following procedures should be considered:

- Inquiry
- Observation
- Inspection
- Confirmation
- Reperformance
- Monitoring

3.2.2 The above can be applied through the use of manual audit procedures, computer-assisted audit techniques, or a combination of both. For example:

- A system which uses manual control totals to balance data entry operations might provide audit evidence that the control procedure is in place by way of an appropriately reconciled and annotated report. The IS auditor should obtain audit evidence by reviewing and testing this report.
- Detailed transaction records may only be available in machine-readable format requiring the IS auditor to obtain audit evidence using computer-assisted audit techniques. The auditor should ensure that the version or type(s) of computer-assisted audit techniques (CAATs) to be used are updated and/or fully compatible with the format(s) structured for the detailed transaction records in question.

3.2.3 If there is a possibility that the gathered evidence will become part of a legal proceeding, the IS auditor should consult with the appropriate legal counsel to determine whether there are any special requirements that will impact the way evidence needs to be gathered, presented and disclosed.

3.3 Audit Documentation

3.3.1 Audit evidence gathered by the IS auditor should be appropriately documented and organised to support the IS auditor's findings and conclusions.

3.3.2 For a discussion on protection and retention of evidence, refer to the commentary section in standard S14.

4. REPORTING

4.1 Restriction of Scope

4.1.1 In those situations where the IS auditor believes sufficient audit evidence cannot be obtained, the IS auditor should disclose this fact in a manner consistent with the communication of the audit results.

5. EFFECTIVE DATE

5.1 This guideline is effective for all information systems audits beginning on or after 1 December 1998. The guideline has been reviewed and updated effective 1 May 2008.

.

G3 Use of Computer Assisted Audit Techniques (CAATs)

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by the appropriate analysis and interpretation of this evidence'.

1.1.2 Standard S5 Planning states 'The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards'.

1.1.3 Standard S3 Professional Ethics and Standards states 'The IS auditor should exercise due professional care, including observance of applicable professional auditing standards'.

1.1.4 Standard S7 Reporting states 'The IS auditor should have sufficient and appropriate audit evidence to support the results reported'.

1.1.5 Standard S14 Audit Evidence states 'The IS auditor should obtain sufficient and appropriate audit evidence to draw reasonable conclusions on which to base the audit results'.

1.2 Linkage to Guidelines

1.2.1 Guideline G2 Audit Evidence Requirement provides guidance to the IS auditor regarding the type and sufficiency of audit evidence used in IS auditing.

1.2.2 Guideline G10 Audit Sampling provides guidance to the IS auditor regarding the design and selection of an audit sample and evaluation of sample results.

1.3 Linkage to COBIT

1.3.1 ME2 *Monitor and evaluate internal control* satisfies the business requirement for IT of protecting the achievement of IT objectives and complying with IT-related laws and regulations by focusing on monitoring the internal control processes for IT-related activities and identifying improvement actions.

1.3.2 DS5 *Ensure systems security* satisfies the business requirement for IT of maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents by focusing on defining IT security policies, procedures and standards, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents.

1.4 Need for Guideline

1.4.1 As entities increase the use of information systems to record, transact and process data, the need for the IS auditor to utilise IS tools to adequately assess risk becomes an integral part of audit coverage. The use of computer-assisted audit techniques (CAATs) serves as an important tool for the IS auditor to evaluate the control environment in an efficient and effective manner. The use of CAATs can lead to increased audit coverage, more thorough and consistent analysis of data, and reduction in risk.

1.4.2 CAATs include many types of tools and techniques, such as generalised audit software, customised queries or scripts, utility software, software tracing and mapping, and audit expert systems.

1.4.3 CAATs may be used in performing various audit procedures including:

- Tests of details of transactions and balances
- Analytical review procedures
- Compliance tests of IS general controls
- Compliance tests of IS application controls
- Penetration testing

1.4.4 CAATs may produce a large proportion of the audit evidence developed on IS audits and, as a result, the IS auditor should carefully plan for and exhibit due professional care in the use of CAATs.

1.4.5 This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

1.4.6 This guidance should be applied in using CAATs regardless of whether the auditor concerned is an IS auditor.

2. PLANNING

2.1 Decision Factors for Using CAATs

2.1.1 When planning the audit, the IS auditor should consider an appropriate combination of manual techniques and CAATs. In determining whether to use CAATs, the factors to be considered include:

- Computer knowledge, expertise, and experience of the IS auditor
- Availability of suitable CAATs and IS facilities
- Efficiency and effectiveness of using CAATs over manual techniques
- Time constraints
- Integrity of the information system and IT environment
- Level of audit risk

2.2 CAATs Planning Steps

2.2.1 The major steps to be undertaken by the IS auditor in preparing for the application of the selected CAATs include the following:

- Set the audit objectives of the CAATs, which may be included in the terms of reference for the exercise.

- Determine the accessibility and availability of the organisation's IS facilities, programs/systems and data.
- Clearly understand composition of data to be processed including quantity, type, format and layout.
- Define the procedures to be undertaken (e.g., statistical sampling, recalculation, confirmation).
- Define output requirements.
- Determine resource requirements, i.e., personnel, CAATs, processing environment (the organisation's IS facilities or audit IS facilities).
- Obtain access to the organisation's IS facilities, programs/systems and data, including file definitions.
- Document CAATs to be used, including objectives, high-level flowcharts and run instructions.

2.3 Arrangements with the Auditee

2.3.1 Adequate time may be needed from data owners or users to properly design the CAAT and interpret the data. In addition, the auditee should understand the purpose, scope, timing and goals of the CAATs. Setting clear expectations at the outset of the CAAT should be communicated.

2.3.2 Data files, such as detailed transaction files, are often only retained for a short period of time; therefore, the IS auditor should make arrangements for the retention of the data covering the appropriate audit time frame.

2.3.3 Access to the organisation's IS facilities, programs/systems and data should be arranged well in advance of the needed time period to minimise the effect on the organisation's production environment, if possible.

2.3.4 The IS auditor should assess the effect that changes to the production programs/systems may have on the use of CAATs. In doing so, the IS auditor should consider the effect of these changes on the integrity and usefulness of CAATs, as well as the integrity of the programs/systems and data used by the IS auditor.

2.4 Testing the CAATs

2.4.1 It is critical that the IS auditor obtain reasonable assurance of the integrity, reliability, usefulness and security of the CAATs through appropriate planning, design, testing, processing and review of documentation. This should be done before reliance is placed on CAATs. The nature, timing and extent of testing is dependent on the commercial availability and stability of the CAATs. Custom CAATs should receive additional review and testing to ensure CAATs are operating as expected.

2.5 Security of Data and CAATs

2.5.1 Where CAATs are used to extract information for data analysis, the IS auditor should verify the integrity of the information system and IT environment from which the data are extracted.

2.5.2 CAATs can be used to extract sensitive program/system information and production data that should be kept confidential. The IS auditor should clearly understand company data classification and data handling policies to properly safeguard the program/system information and production data with an appropriate level of confidentiality and security. In doing so, the IS auditor should consider the level of confidentiality and security required by the organisation owning the data and any relevant legislation, and should consult others, such as legal counsel and management, as necessary.

2.5.3 The IS auditor should use and document the results of appropriate procedures to provide for the ongoing integrity, reliability, usefulness and security of the CAATs. For example, this should include a review of program maintenance and program change controls over embedded audit software to determine that only authorised changes have been made to the CAATs.

2.5.4 When CAATs reside in an environment not under the control of the IS auditor, an appropriate level of control should be in effect to identify changes to the CAATs. When CAATs are changed, the IS auditor should obtain assurance of their integrity, reliability, usefulness and security through appropriate planning, design, testing, processing and review of documentation before reliance is placed on the CAATs.

3. PERFORMANCE OF AUDIT WORK

3.1 Gathering Audit Evidence

3.1.1 The use of CAATs should be controlled by the IS auditor to provide reasonable assurance that the audit objectives and the detailed specifications of the CAATs have been met. The IS auditor should:

- Perform a reconciliation of control totals if appropriate
- Review output for reasonableness
- Perform a review of the logic, parameters or other characteristics of the CAATs
- Review the organisation's general IS controls, which may contribute to the integrity of the CAATs (e.g., program change controls and access to system, program, and/or data files)

3.1.2 When using test data, the IS auditor should be aware that test data only point out the potential for erroneous processing; this technique does not evaluate actual production data. The IS auditor should also be aware that test data analysis can be extremely complex and time consuming, depending on the number of transactions processed, the number of programs tested and the complexity of the programs/systems. Before using test data the IS auditor should verify that the test data will not permanently affect the live system.

3.2 Generalised Audit Software

3.2.1 When using generalised audit software to access the production data, the IS auditor should take appropriate steps to protect the integrity of the organisation's data. With embedded audit software, the IS auditor should be involved in system design and techniques should be developed and maintained within the organisation's application programs/systems.

3.3 Utility Software

3.3.1 When using utility software, the IS auditor should confirm that no unplanned interventions have taken place during processing and that the utility software has been obtained from the appropriate system library. The IS auditor should also take appropriate steps to protect the integrity of the organisation's system and files since these utilities can easily damage the system and its files.

3.4 Customised Queries or Scripts

3.4.1 Customised queries or scripts allow the IS auditor to specifically target desired information for analysis. Customised scripts are highly useful for environments where other CAATs are not available but usually require specific technical skill sets to create them. Therefore, the IS auditor should obtain assurance of their integrity, reliability, usefulness and security through appropriate planning, design and testing before reliance is placed on CAATs, and ensure that proper source data are used and that output from scripts and queries are in the proper format. Customised query and script code should be maintained in a secure location to prevent unauthorised changes from occurring.

3.5 Application Software Tracing and Mapping

3.5.1 When using application software tracing and mapping, the IS auditor should confirm that the source code being evaluated has generated the object program currently being used in production. The IS auditor should be aware that application software tracing and mapping only points out the potential for erroneous processing; it does not evaluate actual production data.

3.6 Audit Expert Systems

3.6.1 Audit expert systems are specialised tools that can be used to analyse the flow of data, through the processing logic of the application software, and document the logic, paths, control conditions and processing sequences. When using audit expert systems, the IS auditor should be thoroughly knowledgeable of the operations of the system to confirm that the decision paths followed are appropriate to the given audit environment/situation.

3.7 Continuous Monitoring and Assurance

3.7.1 Continuous assurance is an uninterrupted monitoring approach that allows management and IS auditors to monitor controls on a continuous basis and to gather selective audit evidence through the computer. It is a process that can be used to provide immediate (or nearly so) reporting by IS auditors and lends itself to use in high-risk, high-volume environments. In the current audit model (used by both internal and external auditors), a period of time passes between the completion of fieldwork and issuance of the related audit report. In many instances, the impact of this delay in issuance makes the information contained in the report less useful or beneficial to the user. This is a result of the aging of the information contained in the report that can be affected by such issues as auditee corrections to identified deficiencies, further deterioration to the control environment (or related auditee data) resulting from identified control weaknesses or deficiencies.

3.7.2 Continuous assurance is therefore designed to enable IS auditors to report on subject matter within a much shorter time frame than under the current model. Theoretically, in some environments it should be possible to shorten the reporting time frame to provide almost instantaneous or truly continuous assurance.

3.7.3 By definition, continuous assurance requires a higher degree of reliance on an auditee's information systems than traditional auditing requires. This is a result of the need to rely upon system-generated information vs. externally produced information as the basis for audit testing. Hence, auditors need to make judgements on both the quality of the auditee's systems as well as the information produced by the system itself. Systems that are of lower quality, or produce less-reliable information, (and require a higher degree of manual intervention) are less conducive to continuous assurance than those that are of high quality and produce reliable information.

3.7.4 Environments that are of a higher quality and produce reliable information are better suited to reporting periods of a short to continuous duration. Environments that are of a lower quality or produce less-reliable information should use longer reporting periods to compensate for the period of time that must pass for users to review and approve or correct information processed by the system.

4. CAATs DOCUMENTATION

4.1 Workpapers

4.1.1 The step-by-step CAATs process should be sufficiently documented to provide adequate audit evidence.

4.1.2 Specifically, the audit workpapers should contain sufficient documentation to describe the CAATs application, including the details set out in the following sections.

4.2 Planning

4.2.1 Documentation should include:

- CAATs objectives
- CAATs to be used
- Controls to be exercised
- Staffing and timing

4.3 Execution

4.3.1 Documentation should include:

- CAATs preparation and testing procedures and controls
- Details of the tests performed by the CAATs

- Details of inputs (e.g., data used, file layouts), testing periods, processing (e.g., CAATs high-level flowcharts, logic) and outputs (e.g., log files, reports)
- Listing of relevant parameters or source code

4.4 Audit Evidence

4.4.1 Documentation should include:

- Output produced
- Description of the audit analysis work performed on the output
- Audit findings
- Audit conclusions
- Audit recommendations

4.4.2 Data and files used should be stored in a secure location. In addition, temporary confidential data used as part of the audit should be properly disposed in accordance with corporate data handling procedures

5. REPORTING

5.1 Description of CAATs

5.1.1 The objectives, scope and methodology section of the report should contain a clear description of the CAATs used. This description should not be overly detailed, but it should provide a good overview for the reader.

5.1.2 The description of CAATs used should also be included in the body of the report, where the specific finding relating to the use of CAATs is discussed.

5.1.3 If the description of the CAATs used is applicable to several findings, or is too detailed, it should be discussed briefly in the objectives, scope and methodology section of the report, and the reader should be referred to an appendix with a more detailed description.

6. EFFECTIVE DATE

6.1 This guideline is effective for all IS audits beginning on or after 1 December 1998. The guideline has been reviewed and updated effective 1 March 2008.

G4 Outsourcing of IS Activities to Other Organisations

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S1 Audit Charter states 'The purpose, responsibility, authority and accountability of the information systems audit function should be appropriately documented in an audit charter or engagement letter'.

1.1.2 Standard S5 Planning states 'The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards'.

1.1.3 Standard S6 Performance of Audit Work states 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.2 Linkage to Guidelines

1.2.1 Guideline G16 sets out how the IS auditor should comply with the ISACA IS Auditing Standards and COBIT when assessing the effect a third party has on an organisation's IS controls and related control objectives.

1.3 Linkage to COBIT

1.3.1 DS2 *Manage third-party services* states that the IS auditor should establish what controls the service user has put in place to address the business requirement to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements.

1.4 Need for Guideline

1.4.1 An organisation (the service user) may partially or fully delegate some or all of its IS activities to an external provider of such services (the service provider). The provider could either be onsite using the service user's systems or offsite using its own systems. IS activities that could be outsourced include IS functions such as data centre operations, security, and application system development and maintenance.

1.4.2 The responsibility for confirming compliance with contracts, agreements and regulations remains with the service user.

1.4.3 The rights to audit are often unclear. The responsibility for auditing compliance is also often not clear. The purpose of this guideline is to set out how the IS auditor should comply with standards S1, S5 and S6 in this situation.

1.4.4 This guideline provides guidance in applying IS Auditing Standards. The IS auditor should consider it in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

2. AUDIT CHARTER

2.1 Responsibility, Authority and Accountability

2.1.1 Where any aspect of the IS function has been outsourced to a service provider, these services should be included in the scope of the audit charter.

2.1.2 The audit charter should explicitly include the right of the IS auditor to:

- Review the agreement between the service user and the service provider (pre- or post-effect)
- Carry out such audit work as is considered necessary regarding the outsourced function
- Report findings, conclusions and recommendations to service user management

3. PLANNING

3.1 Fact Finding

3.1.1 The IS auditor should obtain an understanding of the nature, timing and extent of the outsourced services.

3.1.2 The risks associated with the outsourced services should be identified and assessed.

3.1.3 The IS auditor should assess the extent to which the service user's controls provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

3.1.4 The IS auditor should obtain an understanding of which controls are the responsibility of the service provider (or additional subcontracted third parties) and which controls will remain the responsibility of the service user.

3.1.5 The IS auditor should determine the extent to which the outsource agreement provides for the audit of the service provider and consider whether this provision is adequate. This includes assessing the potential reliance on any IS audit work carried out by either the service provider's internal auditors or an independent third party contracted by the service provider.

3.2 Planning

3.2.1 The IS auditor should consider obtaining appropriate expert legal advice when reviewing the contract and service level agreement (SLA) during the planning phase for the extent and any stipulations regarding the right to audit the service provider.

3.2.2 The IS auditor should evaluate any previous audit report prepared for the service provider and plan the IS audit work to address the audit objectives relevant to the service provider's environment, taking into account the information obtained during planning.

3.2.3 The IS auditor should consider what type of outsourcing has been used and what impact it will have on the audit approach:

- Labor outsourcing (common offshore model):
  - Only the labor is outsourced. The service user's internal controls and business processes remain the same. The service provider relies completely on the service user's IT environment to deliver the service.
  - The IS auditor should plan on testing the service user's existing IT controls as well as any additional controls that support that SLA.

- Labor and systems outsourcing (common onshore model):
  - The service provider uses its own IT environment to deliver the service (e.g., payroll outsourcing).
  - The IS auditor should consider whether the service provider is able to provide any documentation of controls testing performed by qualified independent third parties (e.g., SAS70 Type II report) and whether the objectives covered in the testing are applicable to the IS auditor's audit objectives

3.2.4 **The audit objectives should be agreed upon with the service user management before being communicated to the service provider. Any changes requested by the service provider should be agreed with the service user management.**

3.2.5 **The IS auditor should consider the international certifications or frameworks and also International Organization on Standardization requirements that would apply to outsourcing, while deciding the scope and objectives of the work. Based on that, the IS auditor should decide the extent to which international certifications obtained by the service organisation can be relied upon.**

3.2.6 **The IS auditor should plan the IS audit work to comply with applicable professional audit standards, as if the audit were performed in the service user's own environment.**

4. PERFORMANCE OF AUDIT WORK

4.1 Audit Evidence Requirement

4.1.1 The audit should be performed as if the service was being provided in the service user's own IS environment.

4.2 The Agreement With the Service Provider

4.2.1 The IS auditor should consider such things as:

- Existence of a formal agreement between the service provider and the service user
- Inclusion in the outsourcing agreement of a clause that explicitly states that the service provider is obligated to meet all legal requirements applying to its activities and comply with acts and regulations pertaining to the functions it undertakes on behalf of the service user
- Specific and enforceable stipulations in the outsourcing agreement that activities performed by the service provider are subject to controls and audits as if they were performed by the service user itself
- Inclusion of audit access rights in the agreement with the service provider including both the internal audit staff from the service user and any third parties conducting audits of the service user
- Inclusion of provisions requiring the service provider to monitor compliance with the SLA and proactively report any incidents or failures of controls
- Existence of SLAs with performance monitoring procedures
- Adherence to the service user's security policies
- Adequacy of the service provider's fidelity insurance arrangements
- Adequacy of the service provider's personnel policies and procedures, including segregation of duties between key tasks
- Adequacy of the service provider's policies and procedures for subcontracting tasks to additional third parties and monitoring of SLA performance by those providers
- Adequacy of service provider's ability to continue operations in the event of a disaster

4.3 Management of Outsourced Services

4.3.1 The IS auditor should verify that:

- Business processes to produce the information used to monitor compliance with the SLAs are appropriately controlled. The service user should have either accepted the standard service level compliance information available from the service provider or added additional reporting requirements that have been agreed to by the service provider.
- Where SLAs are not being met, the service user has sought remedy and corrective actions have been considered to achieve the agreed-to service level
- The service user has the capacity and competence to follow up and review the services provided

4.4 Restrictions on Scope

4.4.1 Where the service provider proves unwilling to co-operate with the IS auditor, the IS auditor should report the matter to the service user's management. This may also include operations that have been subcontracted by the service provider to additional third parties without a right-to-audit provision in the contract.

5. REPORTING

5.1 Issuing and Agreeing the Report

5.1.1 The IS auditor should provide a report in an appropriate form to the intended service user recipients upon the completion of the audit work.

5.1.2 The IS auditor should consider discussing the report with the service provider prior to release, but the IS auditor should not be responsible for issuing the final report to the service provider. If the service provider is to receive a copy, this should ordinarily come from the service user's management.

5.1.3 The report should specify any restrictions on distribution that the IS auditor or service user management have agreed to impose. For example, the service provider should not be able to provide a copy of the report to other users of their service without the permission of the IS auditor's organisation and, where appropriate, the service user. The IS auditor should also consider including a statement excluding liability to third parties.

5.2 Reporting Restrictions on Scope

5.2.1 The audit report should clearly identify a restriction on scope where audit access rights are denied and should explain the effect of this restriction with respect to the audit.

6. FOLLOW-UP ACTIVITIES

6.1 Effect of Previous Audits

6.1.1 As if the audit had been performed in the service user's own environment, the IS auditor should request appropriate information from both the service user and the service provider on previous relevant findings, conclusions and recommendations. The IS auditor should determine whether appropriate corrective actions have been implemented by the service provider in a timely manner.

7. EFFECTIVE DATE

7.1 This guideline is effective for all IS audits beginning on or after 1 September 1999. The guideline has been reviewed and updated effective 1 May 2008.

G5 Audit Charter

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S1 Audit Charter states 'The responsibility, authority and accountability of the information systems audit function or information audit assignments should be appropriately documented in an audit charter or engagement letter'.

1.2 Linkage to COBIT

1.2.1 ME 4.7 *Independent assurance* states '…Provide the board with timely independent assurance about the compliance of IT with its policies, standards and procedures, as well as with generally accepted practices'.

1.2.2 ME 2.5 *Assurance of internal control* states 'Obtain, as needed, further assurance of the completeness and effectiveness on internal controls through third-party reviews'.

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to assist the IS auditor to prepare an audit charter to define the responsibility, authority and accountability of the IS audit function. This guideline is aimed primarily at the internal IS audit function; however, aspects could be considered for other circumstances.

1.3.2 This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

2. AUDIT CHARTER

2.1 Mandate

2.1.1 The IS auditor should have a clear mandate to perform the IS audit function. This mandate is ordinarily documented in an audit charter that should be formally accepted. Where an audit charter exists for the audit function as a whole, the IS audit mandate should be incorporated.

2.2 Contents of the Audit Charter

2.2.1 The audit charter should clearly address the four aspects of purpose, responsibility, authority and accountability. Aspects to consider are set out in the following sections.

2.2.2 Purpose:

- Role
- Aims/goals
- Mission statement
- Scope
- Objectives

2.2.3 Responsibility:

- Operating principles
- Independence
- Relationship with external audit
- Auditee requirements
- Critical success factors
- Key performance indicators
- Risk assessment
- Other measures of performance

2.2.4 Authority:

- Right of access to information, personnel, locations and systems relevant to the performance of audits
- Scope or any limitations of scope
- Functions to be audited
- Auditee expectations
- Organisational structure, including reporting lines to board and senior management
- Grading of IS audit staff

2.2.5 Accountability

- Reporting lines to senior management
- Assignment performance appraisals
- Personnel performance appraisals
- Staffing/career development
- Auditee rights
- Independent quality reviews

- Assessment of compliance with standards
- Benchmarking performance and functions
- Assessment of completion of the audit plan
- Comparison of budget to actual costs
- Agreed actions, e.g., penalties when either party fails to carry out their responsibilities

2.3 Communication With Auditees

2.3.1 Effective communication with auditees involves:

- Describing the service, its scope, its availability and timeliness of delivery
- Providing cost estimates or budgets if they are available
- Describing problems and possible resolutions for them
- Providing adequate and readily accessible facilities for effective communication
- Determining the relationship between the service offered and the needs of the auditee

2.3.2 The audit charter forms a sound basis for communication with auditees and should include references to service level agreements for such things as:

- Availability for unplanned work
- Delivery of reports
- Costs
- Response to auditee complaints
- Quality of service
- Review of performance
- Communication with auditees
- Needs assessment
- Control risk self-assessment
- Agreement of terms of reference for audits
- Reporting process
- Agreement of findings

2.4 Quality Assurance Process

2.4.1 The IS auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, assignment performance surveys) to understand auditees' needs and expectations relevant to the IS audit function. These needs should be evaluated against the charter with a view to improving the service or changing the service delivery or audit charter, as necessary.

3. ENGAGEMENT LETTER

3.1 Purpose

3.1.1 Engagement letters are often used for individual assignments or for setting the scope and objectives of a relationship between external IS audit and an organisation.

3.2 Content

3.2.1 The engagement letter should clearly address the three aspects of responsibility, authority and accountability. Aspects to consider are set out in the following paragraphs.

3.2.2 Responsibility

- Scope
- Objectives
- Independence
- Risk assessment
- Specific auditee requirements
- Deliverables

3.2.3 Authority

- Right of access to information, personnel, locations and systems relevant to the performance of the assignment
- Scope or any limitations of scope
- Evidence of agreement to the terms and conditions of the engagement

3.2.4 Accountability

- Intended recipients of reports
- Auditee rights
- Quality reviews
- Agreed completion dates
- Agreed budgets/fees if available

4. EFFECTIVE DATE

4.1 This guideline is effective for all IS audits beginning on or after 1 September 1999. The guideline has been reviewed and updated effective 1 February 2008.

G6 Materiality Concepts for Auditing Information

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S5 Planning states, 'The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards'.

1.1.2 Standard S10 IT Governance, states 'The IS auditor should review and assess compliance with legal, environmental, information quality, fiduciary and security requirements'.

1.1.3 Standard S12 Audit Materiality, states 'The IS auditor should consider audit materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures. While planning for audit, the IS auditor should consider potential weakness or absence of controls and whether such weakness or absence of controls could result into significant deficiency or a material weakness in the information system. The IS auditor should consider the cumulative effect of minor control deficiencies or weaknesses and the absence of controls to translate into significant deficiency or material weakness in the information system'.

1.1.4 Standard S19 Irregularities and Illegal Acts, states 'If the IS auditor has identified a material irregularity or illegal act involving management or employees who have significant roles in internal control, or obtains information that a material irregularity or illegal act may exist, the IS auditor should communicate these matters to the appropriate level of management in a timely manner'.

1.2 Linkage to COBIT

1.2.1. PO5 *Manage the IT investment* 'satisfies the business requirement for IT of continuously and demonstrably improving IT's cost-efficiency and its contribution to business profitability with integrated and standardised services that satisfy end-user expectations by focusing on effective and efficient IT investment and portfolio decisions, and by setting and tracking IT budgets in line with IT strategy and investment decisions'.

1.2.2 AI1 *Identify automated solutions* 'satisfies the business requirement for IT of translating business functional and control requirements into an effective and efficient design of automated solutions by focusing on identifying technically feasible and cost-effective solutions'.

1.2.3 DS10 *Manage problems* 'satisfies the business requirement for IT of ensuring end users' satisfaction with service offerings and service levels; reducing solution and service delivery defects and rework by focusing on recording, tracking and resolving operational problems; investigating the root cause of all significant problems; and defining solutions for identified operations problems'.

1.2.4 DS13 *Manage operations* 'satisfies the business requirement for IT of maintaining data integrity and ensuring IT infrastructure can resist and recover from errors and failures by focusing on meeting operational service levels for scheduled data processing, protecting sensitive output, and monitoring and maintaining infrastructure'.

1.2.5 ME4 *Provide IT governance* 'satisfies the business requirement for IT of integrating IT governance with corporate governance objectives; complying with laws and regulations by focusing on preparing board reports on IT strategy, performance and risks; and responding to governance requirements in line with board directions'.

1.2.6 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the materiality concept of auditing information systems by the IS auditor, the processes in COBIT most likely to be relevant, selected and adapted are classified as primary and secondary as follows. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.7 Secondary references:

- PO8 *Manage quality*
- PO9 *Assess and manage IT risks*
- AI2 *Acquire and maintain application software*
- AI3 *Acquire and maintain technology infrastructure*
- AI4 *Enable operation and use*
- AI5 *Procure IT resources*
- AI6 *Manage changes*
- DS3 *Manage performance and capacity*
- DS5 *Ensure systems security*
- DS9 *Manage the configuration*
- ME1 *Monitor and evaluate IT performance*
- ME2 *Monitor and evaluate internal control*

1.2.8 The information criteria most relevant to audit materiality are:

- Primary: Confidentiality, integrity, compliance, reliability
- Secondary: Effectiveness, efficiency, availability

2. NEED FOR GUIDELINE

2.1 IS vs. Financial Audits

2.1.1 Unlike financial auditors, IS auditors require a different yardstick to measure materiality. Financial auditors ordinarily measure materiality in monetary terms, since what they audit is also measured and reported in monetary terms. IS auditors ordinarily perform audits of non-financial items, e.g., physical access controls, logical access controls, program change controls, and

systems for personnel management, manufacturing control, design, quality control, password generation, credit card production and patient care. Therefore, IS auditors may need guidance on how materiality should be assessed to plan their audits effectively, how to focus their effort on high-risk areas and how to assess the severity of any errors or weaknesses found.

2.1.2 This guideline provides guidance in applying IS auditing standards on audit materiality. The IS auditor should consider it in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

3. PLANNING

3.1 Assessing Materiality

3.1.1 The assessment of what is material is a matter of professional judgement and includes consideration of the effect and/or the potential effect on the organisation's ability to meet its business objectives in the event of errors, omissions, irregularities and illegal acts that may arise as a result of control weaknesses in the area being audited.

3.1.2 While assessing materiality, the IS auditor should consider:

- The aggregate level of error acceptable to management, the IS auditor, appropriate regulatory agencies and other stakeholders
- The potential for the cumulative effect of small errors or weaknesses to become material

3.1.3 To meet the audit objectives, the IS auditor should identify the relevant control objectives and, based on risk tolerance rate, determine what should be examined. With respect to a specific control objective, a material control is a control or group of controls without which control procedures do not provide reasonable assurance that the control objective will be met.

3.1.4 Where the IS audit objective relates to systems or operations that process financial transactions, the financial auditor's measure of materiality should be considered while conducting the IS audit.

3.1.5 The IS auditor should determine establishment of roles and responsibilities as well as a classification of information assets in terms of confidentiality, availability and integrity; access control rules on privileges management; and classification of information based upon degree of criticality and risk of exposure. Assessment should include verification of:

- Information stored
- IS hardware
- IS architecture and software
- IS network infrastructure
- IS operations
- Development and test environment

3.1.6 The IS auditor should determine whether any IT general deficiency could potentially become material. The significance of such deficient IT general controls should be evaluated in relation to their effect on application controls, i.e., whether the associated application controls are also ineffective. If the application deficiency is caused by the IT general control, then they are material. For example, if an application-based tax calculation is materially wrong and was caused by poor change controls to tax tables, then the application-based control (calculation) and the general control (changes) are materially weak.

3.1.7 The IS auditor should evaluate an IT general control's deficiency in relation to its effect on application controls and when aggregated against other control deficiencies. For example, a management decision not to correct an IT general control deficiency and its associated reflection on the control environment could become material when aggregated with other control deficiencies affecting the control environment.

3.1.8 The IS auditor should also note that failure to remediate a deficiency could become material.

3.1.9 The IS auditor should consider obtaining sign-off from appropriate stakeholders acknowledging they have disclosed existing material weakness that they are aware of in the organisation.

3.1.10 The following are examples of measures that should be considered to assess materiality:

- Criticality of the business processes supported by the system or operation
- Criticality of the information databases supported by the system or operation
- Number and type of application developed
- Number of users who use the information systems
- Number of managers and directors who work with the information systems classified by privileges
- Criticality of the network communications supported by the system or operation
- Cost of the system or operation (hardware, software, staff, third-party services, overheads or a combination of these)
- Potential cost of errors (possibly in terms of lost sales, warranty claims, irrecoverable development costs, cost of publicity required for warnings, rectification costs, health and safety costs, unnecessarily high costs of production, high wastage, etc.)
- Cost of loss of critical and vital information in terms of money and time to reproduce
- Effectiveness of countermeasures

- Number of accesses/transactions/inquiries processed per period
- Nature, timing and extent of reports prepared and files maintained
- Nature and quantities of materials handled (e.g., where inventory movements are recorded without values)
- Service level agreement requirements and cost of potential penalties
- Penalties for failure to comply with legal, regulatory and contractual requirements
- Penalties for failure to comply with public health and safety requirements

3.1.11 Control failures may potentially lead to monetary loss, competitive position, loss of trust or loss of reputation, apart from damaging the corporate image. The IS auditor should evaluate risks against possible countermeasures.

4. REPORTING

4.1 Identifying Reportable Issues

4.1.1 In determining the findings, conclusions and recommendations to be reported, the IS auditor should consider both the materiality of any errors found and the potential materiality of errors that could arise as a result of control weaknesses.

4.1.2 Where the audit is used by management to obtain a statement of assurance regarding IS controls, an unqualified opinion on the adequacy of controls should mean that the controls in place are in accordance with generally accepted control practices to meet the control objectives, devoid of any material control weakness.

4.1.3 A control weakness should be considered material and, therefore, reportable, if the absence of the control results in failure to provide reasonable assurance that the control objective will be met. If the audit work identifies material control weaknesses, the IS auditor should consider issuing a qualified or adverse opinion on the audit objective.

4.1.4 Depending on the objectives of the audit, the IS auditor should consider reporting to management weaknesses that are not material, particularly when the costs of strengthening the controls are low.

5. EFFECTIVE DATE

5.1 This guideline is effective for all IS audits beginning on or after 1 September 1999. The guideline has been reviewed and updated effective 1 May 2008.

G7 Due Professional Care

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S3 Professional Ethics and Standards, states 'The IS auditor should adhere to the ISACA Code of Professional Ethics in conducting audit assignments'.

1.1.2 Standard S3 Professional Ethics and Standards, states 'The IS auditor should exercise due professional care, including observance of applicable professional auditing standards'.

1.1.3 Standard S2 Independence, states 'In all matters related to the audit, the IS auditor should be independent of the auditee in both attitude and appearance'.

1.1.4 Standard S4 Professional Competence, states 'The IS auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment, and he/she should maintain professional competence through appropriate continuing professional education and training'.

1.1.5 The IS auditor should refer to the commentary sections in the above standards for additional guidance.

1.2 Linkage to COBIT

1.2.1 PO6 *Communicate management aims and direction,* satisfies the business requirement for IT of accurate and timely information on the current and future IT services, associated risks and responsibilities by focusing on providing accurate, understandable and approved policies, procedures, guidelines and other documentation to stakeholders embedded in an IT control framework.

1.2.2 PO7 *Manage IT human resources,* satisfies the business requirement for IT of competent and motivated people to create and deliver IT services by focusing on hiring and training personnel, motivating through clear career paths, assigning roles that correspond with skills, establishing a defined review process, creating position descriptions and ensuring awareness of dependency on individuals.

1.2.3 PO9 *Assess and manage IT risks,* satisfies the business requirement for IT of analysing and communicating IT risks and their potential impact on business processes and goals by focusing on development of a risk management framework that is integrated in business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk.

1.2.4 ME3 *Ensure compliance with external requirements,* satisfies the business requirement for IT of ensuring compliance with laws regulations and contractual requirements by focusing on identifying all applicable laws regulations and contracts and the corresponding level of IT compliance and optimising IT processes to reduce the risk of non-compliance.

1.2.5 ME4 *Provide IT governance,* satisfies the business requirement for IT of integrating IT governance with corporate governance objectives and complying with laws, regulations and contracts by focusing on preparing board reports on IT strategy, performance and risks and responding to governance requirements in line with board directions.

1.2.6 Secondary references:

- PO1 *Define a strategic IT plan*
- PO5 *Manage the IT investment*
- PO8 *Manage quality*
- PO10 *Manage projects*
- AI1 *Identify automated solutions*
- AI6 *Manage changes*
- DS3 *Manage performance and capacity*
- DS7 *Educate and train users*
- DS9 *Manage configuration*
- DS10 *Manage problems*

1.2.7 The information criteria most relevant are**:**

- Primary: Reliability, confidentiality, integrity, compliance and efficiency
- Secondary: Effectiveness and availability

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to clarify the term 'due professional care' as it applies to the performance of an audit in compliance with standard S3 of the IS Auditing Standards.

1.3.2 Members and ISACA certification holders are expected to comply with the ISACA Code of Professional Ethics; failure may result in an investigation into the member/certification holder's conduct and ultimately in disciplinary action, if necessary.

1.3.3 The guideline provides guidance in applying IS Auditing Standards and complying with the ISACA Code of Professional Ethics on performance of duties with due diligence and professional care. The IS auditor should consider it in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

2. PERFORMANCE of AUDIT WORK

2.1 Due Professional Care

2.1.1 The standard of due care is the level of diligence that a prudent and competent expert would exercise under a given set of circumstances. Due professional care applies to an individual who professes to exercise a special skill, such as IS auditing. Due professional care requires the individual to exercise that skill to a level commonly possessed by practitioners of that speciality.

2.1.2 Due professional care applies to the exercise of professional judgement in the conduct of work performed. Due professional care implies that the professional approaches matters requiring professional judgement with proper diligence.

2.1.3 Due professional care should extend to every aspect of the audit, including but not restricted to the evaluation of audit risk, accepting audit assignments, formulation of audit objectives, the establishment of the audit scope, planning the audit, conducting the audit, allocation of resources to the audit, selection of audit tests, evaluation of test results, audit documentation, conclusion of audit, reporting and delivery of audit results. In doing this, the IS auditor should determine or evaluate:

- The type, level, skill and competence of audit resources required to meet the audit objectives

- The significance of identified risks and the potential affect of such risks on the audit
- The audit evidence gathered
- The competence, integrity and conclusions of others upon whose work the IS auditor places reliance

2.1.4 The IS auditor should maintain an independent and objective state of mind in all matters related to the conduct of the IT audit assignment. The auditor should appear honest, impartial and unbiased in addressing audit issues and reaching conclusions.

2.1.5 The IS auditor should conduct the audit with diligence while adhering to professional standards and statutory and regulatory requirements. The IS auditor should have a reasonable expectation that the IS audit assignment can be completed in accordance with established IS audit standards and other appropriate professional, regulatory or industry standards, and will result in the IS audit being able to express a professional opinion. The IS auditor should disclose the circumstances of any non-compliance in a manner consistent with the communication of the audit results.

2.1.6 The IS auditor should have satisfactory assurance that management understands its obligations and responsibilities in providing appropriate, relevant and timely information required in the performance of the audit assignment and ensure the co-operation of relevant personnel during the audit.

2.1.7 The IS auditor should serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and should not engage in acts discreditable to the profession.

2.1.8 The IS auditor should maintain the privacy and confidentiality of information obtained in the course of his/her duties unless disclosure is required by legal authority. Such information should not be used for personal benefit or released to inappropriate parties.

2.1.9 The IS auditor should exercise due professional care while informing appropriate parties of the results of work performed.

2.1.10 The intended recipients of the audit reports have an appropriate expectation that the IS auditor has exercised due professional care throughout the course of the audit. The IS auditor should not accept an assignment unless adequate skills, knowledge and other resources are available to complete the work in a manner expected of a professional**.**

3. EFFECTIVE DATE

3.1 This guideline is effective for all IS audits beginning on or after 1 September 1999. The guideline has been reviewed and updated effective 1 March 2008.

G8 Audit Documentation

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S5 Planning, states 'The IS auditor document an audit plan that lists the audit detailing the nature and objectives, timing and extent, objectives and resources required'.

1.1.2 Standard S6 Performance of Audit Work, states 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence. The audit process should be documented, describing the audit work performed and the audit evidence that supports the IS auditor's findings and conclusions'.

1.1.3 Standard S7 Reporting, states 'The IS auditor should provide a report, in an appropriate form, upon the completion of the audit. The audit report should state the scope, objectives, period of coverage, and the nature, timing and extent of the audit work performed. The report should state the findings, conclusions, recommendations, and any reservations, qualifications or limitations that the IS auditor has with respect to the audit. When issued, the IS auditor's report should be signed, dated and distributed according to the terms of the audit charter or engagement letter'.

1.1.4 Standard S12 Audit Materiality, states 'The report of the IS auditor should disclose ineffective controls or absence of controls and the significance of the control deficiencies and possibility of these weaknesses resulting in a significant deficiency or material weakness'.

1.1.5 Standard S13 Using the Work of Other Experts, states 'The IS auditor should determine whether the work of other experts is adequate and complete to enable the IS auditor to conclude on the current audit objectives. Such conclusion should be clearly documented'.

1.2 Linkage to COBIT

1.2.1 PO1 *Define a strategic IT plan,* satisfies the business requirement for IT of sustaining or extending the business strategy and governance requirements whilst being transparent about benefits, costs and risks by focusing on incorporating IT and business management in the translation of business requirements into service offerings and the development of strategies to deliver these services in a transparent and effective manner.

1.2.2 PO8 *Manage quality,* satisfies the business requirement for IT of continuous and measurable improvement of the quality of IT services delivered by focusing on the definition of a quality management system (QMS), ongoing performance monitoring against predefined objectives and implementation of a programme for continuous improvement of IT services.

1.2.3 AI6 *Manage changes,* satisfies the business requirement for IT of responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework by focusing on controlling impact assessment, authorisation and implementation of all changes to the IT infrastructure, applications and technical solutions, minimising errors due to incomplete request specifications, and halting implementation of unauthorised changes.

1.2.4 DS1 *Define and manage service,* satisfies the business requirement for IT of ensuring the alignment of key IT services with business strategy by focusing on identifying service requirements, agreeing on service levels and monitoring the achievement of service levels.

1.2.5 ME2 *Monitor and evaluate internal control,* satisfies the business requirement for IT of protecting the achievement of IT objectives and complying with IT-related laws and regulations by focusing on monitoring the internal control processes for IT-related activities and identifying improvement actions.

1.2.6 ME3 *Ensure regulatory compliance,* satisfies the business requirement for IT of compliance with laws and regulations by focusing on identifying all applicable laws and regulations and the corresponding level of IT compliance and optimising IT processes to reduce the risk of non-compliance.

1.2.7 The information criteria most relevant are:

- Primary: Reliability, availability, efficiency and integrity
- Secondary: Effectiveness and confidentiality

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to describe the documentation that the IS auditor should prepare and retain to support the audit.

1.3.2 This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

2. PLANNING AND PERFORMANCE

2.1 Documentation Contents

2.1.1 IS audit documentation is the record of the audit work performed and the audit evidence supporting the IS auditor's findings, conclusions and recommendations. Audit documentation should be complete, clear, structured, indexed, and easy to use and understand by the reviewer. Potential uses of documentation include, but are not limited to:

- Demonstration of the extent to which the IS auditor has complied with the IS Auditing Standards
- Demonstration of audit performance to meet requirements as per the audit charter
- Assistance with planning, performance and review of audits
- Facilitation of third-party reviews
- Evaluation of the IS auditing function's QA programme
- Support in circumstances such as insurance claims, fraud cases, disputes and lawsuits
- Assistance with professional development of staff

2.1.2 Documentation should include, at a minimum, a record of:

- Review of previous audit documentation

- The planning and preparation of the audit scope and objectives. IS auditors must have an understanding of the industry, business domain, business process, product, vendor support and overall environment under review.
- Minutes of management review meetings, audit committee meetings and other audit-related meetings
- The audit programme and audit procedures that will satisfy the audit objectives
- The audit steps performed and audit evidence gathered to evaluate the strengths and weakness of controls
- The audit findings, conclusions and recommendations
- Any report issued as a result of the audit work
- Supervisory review

2.1.3 The extent of the IS auditor's documentation depends on the needs for a particular audit and should include such things as:

- The IS auditor's understanding of the areas to be audited and its environment.
- The IS auditor's understanding of the information processing systems and the internal control environment including the:
  - Control environment
  - Control procedures
  - Detection risk assessment
  - Control risk assessment
  - Equate total risk
- The author and source of the audit documentation and the date of its completion
- Methods used to assess adequacy of control, existence of control weakness or lack of controls, and identify compensating controls
- Audit evidence, the source of the audit documentation and the date of completion, including:
  - Compliance tests, which are based on test policies, procedures and segregation duties
  - Substantive tests, which are based on analytic procedures, detailed test accounts balances and other substantive audit procedures
- Acknowledgement from appropriate person of receipt of audit report and findings
- Auditee's response to recommendations
- Version control, especially where documentation is in electronic media

2.1.4 Documentation should include appropriate information required by law, government regulations or applicable professional standards.

2.1.5 Documentation should be submitted to the audit committee for its review and approval.

3. DOCUMENTATION

3.1 Custody, Retention and Retrieval

3.1.1 Policies and procedures should be in effect to verify and ensure appropriate custody and retention of the documentation that supports audit findings and conclusions for a period sufficient to satisfy legal, professional and organisational requirements.

3.1.2 Documentation should be organised, stored and secured in a manner appropriate for the media on which it is retained and should continue to be readily retrievable for a time sufficient to satisfy the policies and procedures defined above.

4. EFFECTIVE DATE

4.1. This revised guideline is effective for all IS audits beginning on or after 1 September 1999. The guideline has been reviewed and updated effective 1 March 2008.

G9 Audit Considerations for Irregularities and Illegal Acts

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S3 Professional Ethics and Standards states: 'The IS auditor should exercise due professional care, including observance of applicable professional auditing standards'.

1.1.2 Standard S5 Planning states: 'The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards'.

1.1.3 Standard S6 Performance of Audit Work states: 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.1.4 Standard S7 Reporting states: 'The IS auditor should provide a report, in an appropriate form, upon the completion of the audit. The audit report should state the scope, objectives, period of coverage, and the nature, timing and extent of the audit work performed. The report should state the findings, conclusions and recommendations and any reservations or qualifications or limitations in scope that the IS auditor has with respect to the audit'.

1.1.5 Standard S9 Irregularities and Illegal Acts elaborates on requirements and considerations by IS auditors regarding irregularities and illegal acts.

1.2 Linkage to CobiT

1.2.1 Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT's control objectives and associated management practices. To meet the audit considerations of IS auditors for irregularities and illegal acts, the processes in CobiT most likely to be relevant, selected and adapted are classified here as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.2 The primary CobiT references are:

- PO5 *Manage the IT investment*
- PO7 *Manage IT human resources*
- PO9 *Assess and manage IT risks*
- PO10 *Manage projects*
- AI1 *Identify automated solutions*
- AI5 *Procure IT resources*
- ME2 *Monitor and evaluate internal controls*
- ME3 *Ensure regulatory compliance*
- ME4 *Provide IT governance*

1.2.3 The secondary CobiT references are:

- PO3 *Determine technological direction*
- PO4 *Define the IT processes, organisation and relationships*
- PO8 *Manage quality*
- DS7 *Educate and train users*
- DS10 *Manage problems*
- ME1 *Monitor and evaluate IT performance*

1.2.4 The most relevant CobiT information criteria are:

- Primary: Compliance, confidentiality, integrity and availability
- Secondary: Reliability, efficiency and effectiveness

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to provide guidance to IS auditors to deal with irregular or illegal activities they may come across during the performance of audit assignments.

1.3.2 Standard S9 Irregularities and Illegal Acts elaborates on requirements and considerations by IS auditors for irregularities and illegal acts. This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the previously identified standards, use professional judgement in its application and be prepared to justify any departure.

2. DEFINITIONS

2.1 Non-fraudulent Irregular Activities

2.1.1 Not all irregularities should be considered fraudulent activities. The determination of fraudulent activities depends on the legal definition of fraud in the jurisdiction pertaining to the audit. Irregularities include, but are not limited to, deliberate circumvention of controls with the intent to conceal the perpetuation of fraud, unauthorised use of assets or services, and abetting or helping to conceal these types of activities. Non-fraudulent irregularities may include:

- Intentional violations of established management policy
- Intentional violations of regulatory requirements
- Deliberate misstatements or omissions of information concerning the area under audit or the organisation as a whole
- Gross negligence
- Unintentional illegal acts

2.2 Irregularities and Illegal Acts

2.2.1 Irregularities and illegal acts may include activities such as, but not limited to:

- Fraud, which is any act involving the use of deception to obtain illegal advantage
- Acts that involve non-compliance with laws and regulations, including the failure of IT systems to meet applicable laws and regulations
- Acts that involve non-compliance with the organisation's agreements and contracts with third parties, such as banks, suppliers, vendors, service providers and stakeholders
- Manipulation, falsification, forgery or alteration of records or documents (whether in electronic or paper form)
- Suppression or omission of the effects of transactions from records or documents (whether in electronic or paper form)
- Inappropriate or deliberate leakage of confidential information
- Recording of transactions in financial or other records (whether in electronic or paper form) that lack substance and are known to be false
- Misappropriation and misuse of IS and non-IS assets
- Acts whether intentional or unintentional that violate intellectual property (IP), such as copyright, trademark or patents
- Granting unauthorised access to information and systems
- Errors in financial or other records that arise due to unauthorised access to data and systems

2.2.2 The determination of whether a particular act is illegal generally would be based on the advice of an informed expert qualified to practice law or may have to await final determination by a court of law. The IS auditor should be concerned primarily with the effect or potential effect of the irregular action, irrespective of whether the act is suspected or proven as illegal.

3. RESPONSIBILITIES

3.1 Responsibilities of Management

3.1.1 It is primarily management's responsibility to prevent and detect irregularities and illegal acts.

3.1.2 Management typically use the following means to obtain reasonable assurance that irregularities and illegal acts are prevented or detected in a timely manner:

- Designing, implementing and maintaining internal control systems to prevent and detect irregularities or illegal acts. Internal controls include transaction review and approval and management review procedures.
- Polices and procedures governing employee conduct
- Compliance validation and monitoring procedures
- Designing, implementing and maintaining suitable systems for the reporting, recording and management of incidents relating to irregularities or illegal acts

3.1.3 Management should disclose to the IS auditor its knowledge of any irregularities or illegal acts and areas affected, whether alleged, suspected or proven, and the action, if any, taken by management.

3.1.4 Where an act of irregularity or illegal nature is alleged, suspected or detected, management should aid the process of investigation and inquiry.

3.2 Responsibilities of IS Auditors

3.2.1 The IS auditor should consider defining in the audit charter or letter of engagement the responsibilities of management and audit with respect to preventing, detecting and reporting irregularities, so that these are clearly understood for all audit work. Where these responsibilities are already documented in the organisation's policy or similar document, the audit charter should include a statement to that effect.

3.2.2 The IS auditor should understand that control mechanisms do not completely eliminate the possibility of irregularities or illegal acts occurring. The IS auditor is responsible for assessing the risk of irregularities or illegal acts occurring, evaluating the impact of identified irregularities, and designing and performing tests that are appropriate for the nature of the audit assignment. The IS auditor can reasonably be expected to detect:

- Irregularities or illegal acts that could have a material effect on either the area under audit or the organisation as a whole
- Weaknesses in internal controls that could result in material irregularities or illegal acts not being prevented or detected

3.2.3 The IS auditor is not professionally responsible for the prevention or detection of irregularities or illegal acts. An audit cannot guarantee that irregularities will be detected. Even when an audit is appropriately planned and performed, irregularities could go undetected, e.g., if there is collusion between employees, collusion between employees and outsiders, or management involvement in the irregularities. The IS auditor should also consider documenting this point in the audit charter or letter of engagement.

3.2.4 Where the IS auditor has specific information about the existence of an irregularity or illegal act, the auditor has an obligation to perform procedures to detect, investigate and report it.

3.2.5 The IS auditor should inform the audit committee (or equivalent) and management when he/she has identified situations where a higher level of risk exists for a potential irregularity or illegal act, even if none is detected.

3.2.6 The IS auditor should be reasonably conversant with the subject to be able to identify risk factors that may contribute to the occurrence of irregular or illegal acts.

3.2.7 IS auditors should ensure that they are independent of the subject during the entire audit assignment.

3.2.8 IS auditors are required to refer to standard S9 Irregularities and Illegal Acts for a detailed discussion on IS auditors' responsibilities.

4. RISK ASSESSMENT

4.1 Planning the Risk Assessment

4.1.1 The IS auditor should assess the risk of occurrence of irregularities or illegal acts connected with the area under audit following the use of the appropriate methodology. In preparing this assessment, the IS auditor should consider factors such as:

- Organisational characteristics, e.g., corporate ethics, organisational structure, adequacy of supervision, compensation and reward structures, the extent of corporate performance pressures, organisation direction

- The history of the organisation, past occurrences of irregularities, and the activities subsequently taken to mitigate or minimise the findings related to irregularities
- Recent changes in management, operations or IS systems and the organisation's current strategic direction
- Impacts resulting from new strategic partnerships
- The types of assets held, or services offered, and their susceptibility to irregularities
- Evaluation of the strength of relevant controls and vulnerabilities to circumvent or bypass established controls
- Applicable regulatory or legal requirements
- Internal policies such as a whistle-blower policy, insider trading policy, and employee and management code of ethics
- Stakeholder relations and financial markets
- Human resources capabilities
- Confidentiality and integrity of market-critical information
- The history of audit findings from previous audits
- The industry and competitive environment in which the organisation operates
- Findings of reviews carried out outside the scope of the audit, such as findings from consultants, quality assurance teams or specific management investigations
- Findings that have arisen during the day-to-day course of business
- Process documentation and a quality management system
- The technical sophistication and complexity of the information system(s) supporting the area under audit
- Existence of in-house developed/maintained application systems, compared with packaged software, for core business systems
- The effect of employee dissatisfaction
- Potential layoffs, outsourcing, divestiture or restructuring
- The existence of assets that are easily susceptible to misappropriation
- Poor organisational financial and/or operational performance
- Management's attitude with regard to ethics
- Irregularities and illegal acts that are common to a particular industry or have occurred in similar organisations

4.1.2 The risk assessment should take into consideration only those factors that are relevant to the organisation and the subject of the engagement, including risk factors relating to:

- Irregularities or illegal acts that affect the financial accounting records
- Irregularities or illegal acts that do not effect the financial records, but affect the organisation
- Other irregularities or illegal acts that relate to the sufficiency of the organisation's controls

4.1.3 As part of the planning process and performance of the risk assessment, the IS auditor should inquire of management with regard to such things as:

- Their understanding regarding the level of risk of irregularities and illegal acts in the organisation
- Whether they have knowledge of irregularities and illegal acts that have or could have occurred against or within the organisation
- How the risk of irregularities or illegal acts is monitored or managed
- What processes are in place to communicate to appropriate stakeholders about the existence of risk of irregularities or illegal acts
- Applicable national and regional laws in the jurisdiction the company operates and extent of co-ordination of the legal department with the risk committee and audit committee

~~5~~. PLANNING OF AUDIT WORK

5.1 Planning the Engagement

5.1.1 While the IS auditor has no explicit responsibility to detect or prevent illegal acts or irregularities, the IS auditor should design the procedures to detect illegal acts or irregularities based on the assessed level of risk that they could occur.

5.1.2 When planning the engagement, the IS auditor should obtain an understanding of such things as:

- A basic understanding of the organisation's operations and objectives
- The internal control environment
- The policies and procedures governing employee conduct
- Compliance validation and monitoring procedures
- The legal and regulatory environment in which the organisation operates
- The mechanism that the organisation uses to obtain, monitor and ensure compliance with the laws and regulations that affect the organisation

5.2 Engagement Procedure

5.2.1 The IS auditor should design procedures for the engagement that take into account the level of risk for irregularities and illegal acts that have been identified.

5.2.2 The results of the risk assessment and other procedures performed during planning should be used to determine the nature, extent and timing of the procedures performed during an engagement.

5.2.3. The IS auditor should inquire of IT and user management (as appropriate) concerning compliance with laws and regulations.

5.2.4. The IS auditor should use the results of the risk assessment, to determine the nature, timing and extent of the testing required to obtain sufficient audit evidence of reasonable assurance that:

- Irregularities that could have a material effect on the area under audit, or on the organisation as a whole, are identified
- Control weaknesses that would fail to prevent or detect material irregularities are identified

- All significant deficiencies in the design or operation of internal controls that could potentially affect the issuer's ability to record, process, summarise and report business data are identified

5.3 Evaluating the Results of Engagement Procedures

5.3.1 The IS auditor should review the results of engagement procedures to determine whether indications of irregularities or illegal acts may have occurred.

5.3.2 When this evaluation is performed, risk factors identified in section 4 should be reviewed against the actual procedures performed to provide reasonable assurance that all identified risks have been addressed.

5.3.3 The evaluation should also include an assessment of the results of the procedures to determine if undocumented risk factors exist.

6. PERFORMANCE OF AUDIT WORK

6.1 Responding to Possible Illegal Acts

6.1.1 During an engagement, indications that the existence of irregularities or illegal acts may come to the attention of the IS auditor. If indications of an illegal act are identified, the IS auditor should consider the potential effect on the subject matter of the engagement, the report and the organisation.

6.1.2 When the IS auditor becomes aware of information concerning a possible illegal act, the IS auditor should consider taking the following steps:

- Obtain an understanding of the nature of the act.
- Understand the circumstances in which it occurred.
- Obtain sufficient supportive information to evaluate the effect of the irregularity or illegal act.
- Perform additional procedures to determine the effect of the irregularity or illegal act and whether additional acts exist.

6.1.3 The IS auditor should work with appropriate personnel in the organisation (such as organisational security personnel), including management (at an appropriate level above those involved, if possible), to determine whether an irregularity or illegal act has occurred and its effect.

6.1.4 When an irregularity involves a member of management, the IS auditor should reconsider the reliability of representations made by management. As stated previously, typically, the IS auditor should work with an appropriate level of management above the one associated with the irregularity or illegal act.

6.1.5 Unless circumstances clearly indicate otherwise, the IS auditor should assume that an irregularity or illegal act is not an isolated occurrence.

6.1.6 The IS auditor should also review applicable portions of the organisation's internal controls to determine why they failed to prevent or detect the occurrence of an irregularity or illegal act.

6.1.7 The IS auditor should reconsider the prior evaluation of the sufficiency, operation and effectiveness of the organisation's internal controls.

6.1.8 When the IS auditor has identified situations where an irregularity or illegal act exists (whether potential or in fact), the IS auditor should modify the procedures performed to confirm or resolve the issue identified during the engagement's performance. The extent of such modifications or additional procedures depends on the IS auditor's judgement as to the:

- Type of irregularity or illegal act that may have occurred
- Perceived risk of its occurrence
- Potential effect on the organisation, including such things as financial effects and the organisation's reputation
- Likelihood of the recurrence of similar irregularities or illegal acts
- Possibility that management may have knowledge of, or be involved with, the irregularity or illegal act
- Actions, if any, that the governing body and/or management is taking
- Possibility that non-compliance with laws and regulations has occurred unintentionally
- Likelihood that a material fine or other sanctions, e.g., the revocation of an essential licence, may be imposed as a result of non-compliance.
- Effect on the public interest that may result from the irregularity

6.2 Effect of Finding Irregularities

6.2.1 If irregularities have been detected, the IS auditor should assess the effect of these activities on the audit objectives and on the reliability of audit evidence collected. In addition, the IS auditor should consider whether to continue the audit when:

- The effect of irregularities appears to be so significant that sufficient, reliable audit evidence cannot be obtained
- Audit evidence suggests that management, or employees who have a significant role in the issuer's internal controls, have participated in or condoned irregularities

6.3 Effect of Finding Indicators of Irregularities

6.3.1 If the audit evidence indicates that irregularities could have occurred, the IS auditor should:

- Recommend to management that the matter be investigated in detail or the appropriate actions taken. If the IS auditor suspects that management is involved in the irregularity, he/she should identify the appropriate responsible figure in the organisation to whom these conclusions should be reported. If reporting internally proves impossible, the IS auditor should consider consulting the audit committee and legal counsel about the advisability and risks of reporting the findings outside the organisation.
- Perform adequate actions to support the audit findings, conclusions and recommendations

6.4 Legal Considerations

6.4.1 If audit evidence indicates that an irregularity could involve an illegal act, the IS auditor should consider seeking legal advice directly or recommending that management seek legal advice. The IS auditor may want to define responsibility for legal costs in the audit charter or letter of engagement.

7. Reporting

7.1 Internal Reporting

7.1.1 The detection of irregularities should be communicated to appropriate persons in the organisation in a timely manner. The notification should be directed to a level of management above that at which the irregularities are suspected to have occurred. In addition, irregularities should be reported to the board of directors, audit committee of the board, or equivalent body, except for matters that are clearly insignificant in terms of both financial effect and indications of control weaknesses. If the IS auditor suspects that all levels of management are involved, then the findings should be confidentially reported to governing bodies of the organisation, such as the board of directors/ governors, trustees or audit committee, according to the local applicable regulations and laws.

7.1.2 The IS auditor should use professional judgement when reporting an irregularity or illegal act. The IS auditor should discuss the findings and the nature, timing and extent of any further procedures to be performed with an appropriate level of management that is at least one level above the persons who appear to be involved. In these circumstances, it is particularly important that the IS auditor maintains independence. In determining the appropriate persons to whom to report an irregularity or illegal act, the IS auditor should consider all relevant circumstances, including the possibility of senior management involvement.

7.1.3 The internal distribution of reports of irregularities should be considered carefully. The occurrence and effect of irregularities is a sensitive issue and reporting them carries its own risks, including**:**

- Further abuse of the control weaknesses as a result of publishing details of them
- Loss of customers, suppliers and investors when disclosure (authorised or unauthorised) occurs outside the organisation
- Loss of key staff and management, including those not involved in the irregularity, as confidence in management and the future of the organisation falls

7.1.4 The IS auditor should consider reporting the irregularity separately from any other audit issues if this would assist in controlling distribution of the report.

7.1.5 The IS auditor's report should include:

- Critical policies and practices adopted by the organisation
- If any deviations from generally accepted standards, management's reason for such deviation and the auditor's opinions on such deviations

7.1.6 The IS auditor should seek to avoid alerting any person who may be implicated or involved in the irregularity or illegal act, to reduce the potential for those individuals to destroy or suppress evidence.

7.2 External Reporting

7.**2.1** External reporting may be a legal or regulatory obligation. The obligation may apply to the management of the organisation, or the individuals involved in detecting the irregularities, or both. Not withstanding an organisation's responsibility to report an illegal act or irregularity, the IS auditor's duty of confidentiality to the organisation precludes reporting any potential or identified irregularities or illegal acts. However, in certain circumstances, the IS auditor may be required to disclose an irregularity or illegal act. These include such things as:

- Compliance with legal or regulatory requirements
- External auditor requests
- Subpoena or court order
- Funding agency or government agency in accordance with requirements for the audits of entities that receive governmental financial assistance

7.2.2 Where external reporting is required, the report should be approved by the appropriate level of audit management prior to external release and should also be reviewed with auditee management in advance, unless the applicable regulations or specific circumstances of the audit prevent this. Examples of specific circumstances that may prevent obtaining auditee management's agreement include:

- Auditee management's active involvement in the irregularity
- Auditee management's passive acquiescence to the irregularity

7.2.3 If auditee management does not agree to the external release of the report, and external reporting is a statutory or a regulatory obligation, then the IS auditor should consider consulting the audit committee and legal counsel about the advisability and risks of reporting the findings outside the organisation. In some jurisdictions, the IS auditor may be protected by qualified privilege. Even in situations where IS auditor's are protected by privilege, IS auditors should seek legal advice and counsel prior to making this type of disclosure to ensure that they are in fact protected by this privilege.

7.2.4 The IS auditor, with the approval of audit management, should submit the report to appropriate regulators on a timely basis. If the organisation fails to disclose a known irregularity or illegal act or requires the IS auditor to suppress these findings, the IS auditor should seek legal advice and counsel.

7.2.5 Where the IS auditor is aware that management is required to report fraudulent activities to an outside organisation, the IS auditor should formally advise management of this responsibility.

7.2.6 If an irregularity has been detected by an IS auditor who is not part of the external audit team, then the IS auditor should consider submitting the report to the external auditors in a timely manner.

7.3 Restriction of Audit Scope

7.3.1 Where the audit scope has been restricted, the IS auditor should include an explanation of the nature and effect of this restriction in the audit report. Such a restriction may occur if:

- The IS auditor has been unable to carry out the further work considered necessary to fulfil the original audit objectives and support the audit conclusions, e.g., because of unreliable audit evidence, lack of resource or restrictions placed on the audit activities by management
- Management has not carried out the investigations recommended by the IS auditor

8 EFFECTIVE DATE

8.1 This guideline is effective for all IS audits beginning on or after 1 March 2000. This guideline has been reviewed and updated, combined with and replaces G19 Irregularities and Illegal Acts, effective 1 September 2008.

G10 Audit Sampling

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states: 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT, applicable to the scope of the particular audit, is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the audit sampling requirement of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.2 ME2 *Monitor and evaluate internal control* satisfies the business requirement for IT of protecting the achievement of IT objectives and complying with IT-related laws, regulations and contracts by focusing on monitoring the internal control processes for IT-related activities and identifying improvement actions.

1.2.3 ME3 *Ensure regulatory compliance* satisfies the business requirement for IT of compliance with laws and regulations by focusing on identifying all applicable laws and regulations and the corresponding level of IT compliance and optimising IT processes to reduce the risk of non-compliance.

1.2.4 The primary references are:

- PO8 *Manage quality*
- PO9 *Assess and manage IT risks*
- AI6 *Manage changes*
- ME2 *Monitor and evaluate internal control*
- ME3 *Ensure regulatory compliance*

1.2.5 The information criteria most relevant are:

- Primary: Effectiveness, integrity, reliability and compliance
- Secondary: Confidentiality, efficiency and availability

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to provide guidance to the IS auditor to design and select an audit sample and evaluate sample results. Appropriate sampling and evaluation will meet the requirements of 'sufficient, reliable, relevant and useful evidence' and 'supported by appropriate analysis'.

1.3.2 The IS auditor should consider selection techniques that result in a statistically based representative sample for performing compliance or substantive testing.

1.3.3 Examples of compliance testing of controls, where sampling could be considered, include user access rights, program change control procedures, procedures documentation, program documentation, follow-up on exceptions, review of logs and software licences audits.

1.3.4 Examples of substantive tests, where sampling could be considered, include reperformance of a complex calculation (e.g., interest) on a sample of accounts, sample of transactions to vouch to supporting documentation, etc.

1.3.5 This guideline provides guidance in applying IS Auditing Standards. The IS auditor should consider it in determining how to achieve implementation of standard S6, use professional judgement in its application and be prepared to justify any departure.

1.3.6 Other useful references on audit sampling include the International Standard on Auditing #530 Audit Sampling and Other Selective Testing Procedures, issued by the International Federation of Accountants (IFAC).

2. PERFORMANCE OF AUDIT WORK

2.1 Audit Sampling

2.1.1 When using either statistical or non-statistical sampling methods, the IS auditor should design and select an audit sample, perform audit procedures, and evaluate sample results to obtain sufficient, reliable, relevant and useful audit evidence.

2.1.2 In forming an audit opinion, IS auditors frequently do not examine all of the information available as it may be impractical and valid conclusions can be reached using audit sampling.

2.1.3 Audit sampling is defined as the application of audit procedures to less than 100 percent of the population to enable the IS auditor to evaluate audit evidence about some characteristic of the items selected to form or assist in forming a conclusion concerning the population.

2.1.4 Statistical sampling involves the use of techniques from which mathematically constructed conclusions regarding the population can be drawn.

2.1.5 Non-statistical sampling is not statistically based, and results should not be extrapolated over the population as the sample is unlikely to be representative of the population.

2.2 Design of the Sample

2.2.1 When designing the size and structure of an audit sample, IS auditors should consider the specific audit objectives, the nature of the population, and the sampling and selection methods.

2.2.2 The IS auditor should consider the need to involve appropriate specialists in the design and analysis of samples.

2.2.3 The sampling unit depends on the purpose of the sample. For compliance testing of controls, attribute sampling is typically used, where the sampling unit is an event or transaction (e.g., a control such as an authorisation on an invoice). For substantive testing, variable or estimation sampling is frequently used where the sampling unit is often monetary.

G10 Audit Sampling cont.

2.2.4 The IS auditor should consider the specific audit objectives to be achieved and the audit procedures that are most likely to achieve those objectives. In addition, when audit sampling is appropriate, consideration should be given to the nature of the audit evidence sought and possible error conditions.

2.2.5 The population is the entire set of data from which the IS auditor wishes to sample to reach a conclusion on the population. Therefore, the population from which the sample is drawn has to be appropriate and verified as complete for the specific audit objective.

2.2.6 To assist in the efficient and effective design of the sample, stratification may be appropriate. Stratification is the process of dividing a population into subpopulations with similar characteristics explicitly defined, so that each sampling unit can belong to only one stratum.

2.2.7 When determining sample size, the IS auditor should consider the sampling risk, the amount of the error that would be acceptable and the extent to which errors are expected.

2.2.8 Sampling risk arises from the possibility that the IS auditor's conclusion may be different from the conclusion that would be reached if the entire population were subjected to the same audit procedure. There are two types of sampling risk:

- The risk of incorrect acceptance—The risk that material misstatement is assessed as unlikely when, in fact, the population is materially misstated
- The risk of incorrect rejection—The risk that material misstatement is assessed as likely when, in fact, the population is not materially misstated

2.2.9 Sample size is affected by the level of sampling risk that the IS auditor is willing to accept. Sampling risk should also be considered in relation to the audit risk model and its components, inherent risk, control risk, and detection risk.

2.2.10 Tolerable error is the maximum error in the population that IS auditors are willing to accept and still conclude that the audit objective has been achieved. For substantive tests, tolerable error is related to the IS auditor's judgement about materiality. In compliance tests, it is the maximum rate of deviation from a prescribed control procedure that the IS auditor is willing to accept.

If the IS auditor expects errors to be present in the population, a larger sample than when no error is expected ordinarily has to be examined to conclude that the actual error in the population is not greater than the planned tolerable error. Smaller sample sizes are justified when the population is expected to be error free. When determining the expected error in a population, the IS auditor should consider such matters as error levels identified in previous audits, changes in the organisation's procedures, and evidence available from an evaluation of the system of internal control and results from analytical review procedures.

2.3.1 Selection of the Sample

2.3.1 There are four commonly used sampling methods. Statistical sampling methods are:

- Random sampling—Ensures that all combinations of sampling units in the population have an equal chance of selection
- Systematic sampling—Involves selecting sampling units using a fixed interval between selections, the first interval having a random start. Examples include Monetary Unit Sampling or Value Weighted selection where each individual monetary value (e.g., $1) in the population is given an equal chance of selection. As the individual monetary unit cannot ordinarily be examined separately, the item which includes that monetary unit is selected for examination. This method systematically weights the selection in favour of the larger amounts but still gives every monetary value an equal opportunity for selection. Another example includes selecting every 'nth sampling unit

Nonstatistical sampling methods are:

- Haphazard sampling—The IS auditor selects the sample without following a structured technique, while avoiding any conscious bias or predictability. However, analysis of a haphazard sample should not be relied upon to form a conclusion on the population
- Judgmental sampling—The IS auditor places a bias on the sample (e.g., all sampling units over a certain value, all for a specific type of exception, all negatives, all new users). It should be noted that a judgemental sample is not statistically based and results should not be extrapolated over the population as the sample is unlikely to be representative of the population.

2.3.2 The IS auditor should select sample items in such a way that the sample is expected to be representative of the population regarding the characteristics being tested, i.e., using statistical sampling methods. To maintain audit independence, the IS auditor should ensure that the population is complete and control the selection of the sample.

2.3.3 For a sample to be representative of the population, all sampling units in the population should have an equal or known probability of being selected, i.e., statistical sampling methods.

2.3.4 There are two commonly used selection methods: selection on records and selection on quantitative fields (e.g., monetary units). For selection on records, common methods are:

- Random sample (statistical sample)
- Haphazard sample (non-statistical)
- Judgemental sample (non-statistical; high probability to lead to a biased conclusion)

For selection on quantitative fields, common methods are:

- Random sample (statistical sample on monetary units)
- Fixed Interval sample (statistical sample using a fixed interval)
- Cell sample (statistical sample using random selection in an interval)

2.4 Documentation

2.4.1 The audit work papers should include sufficient detail to describe clearly the sampling objective and the sampling process used. The work papers should include the source of the population, the sampling method used, sampling parameters (e.g., random start number or method by which random start was obtained, sampling interval), items selected, details of audit tests performed and conclusions reached.

2.5 Evaluation of Sample Results

2.5.1 Having performed, on each sample item, those audit procedures which are appropriate to the particular audit objective, the IS auditor should analyse any possible errors detected in the sample to determine whether they are actually errors and, if appropriate, the nature and cause of the errors. For those that are assessed as errors, the errors should be projected as appropriate to the population, if the sampling method used, is statistically based.

2.5.2 Any possible errors detected in the sample should be reviewed to determine whether they are actually errors. The IS auditor should consider the qualitative aspects of the errors. These include the nature and cause of the error and the possible effect of the error on the other phases of the audit. Errors that are the result of the breakdown of an automated process ordinarily have wider implications for error rates than human error.

2.5.3 When the expected audit evidence regarding a specific sample item cannot be obtained, the IS auditor may be able to obtain sufficient, appropriate audit evidence by performing alternative procedures on the item selected.

2.5.4 The IS auditor should consider projecting the results of the sample to the population with a method of projection consistent with the method used to select the sampling unit. The projection of the sample may involve estimating the probable error in the population and estimating any further error that might not have been detected because of the imprecision of the technique together with the qualitative aspects of any errors found.

2.5.5 The IS auditor should consider whether errors in the population might exceed the tolerable error by comparing the projected population error to the tolerable error, taking into account the results of other audit procedures relevant to the audit objective. When the projected population error exceeds the tolerable error, the IS auditor should reassess the sampling risk and, if that risk is unacceptable, consider extending the audit procedure or performing alternative audit procedures.

3. EFFECTIVE DATE

3.1 This guideline is effective for all IS audits beginning on or after 1 March 2000. The guideline has been reviewed and updated effective 1 August 2008.

G11 Effect of Pervasive IS Controls

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states: 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the audit requirement of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary as follows.

1.2.2 Primary references:

- PO4 *Define IT processes, organisation and relationships*
- AI4 *Enable operation and use*
- AI6 *Manage changes*
- AI7 *Install and accredit solutions and changes*

1.2.3 Secondary references:

- DS3 *Manage performance and change*
- DS5 *Ensure system security*
- ME2 *Monitor and evaluate internal control*

1.2.4 The information criteria most relevant are:

- Primary: Effectiveness, efficiency and integrity
- Secondary: Confidentiality, availability, compliance and reliability

1.3 Need for Guideline

1.3.1 The management and monitoring of any organisation, department or function has an affect on the way in which that organisation, department or function behaves, including the way in which it applies controls. This principle applies as much to the use of IS as it does to a manufacturing organisation, an accounts payable department or a treasury function.

1.3.2 The effectiveness of the detailed IS controls operated within an organisation is limited by the effectiveness of the management and monitoring of the use of information systems in the organisation as a whole. This is often recognised in guidelines for financial audits, where the effect of 'general' controls in the IS environment on 'application' controls in the financial systems is acknowledged.

1.3.3 The IT Governance Institute's COBIT framework can assist the IS auditor in differentiating between:

- The detailed IS controls that are directly relevant to the IS audit scope
- The features of IS management and monitoring that contribute to the assurance and may be obtained by an IS auditor in relation to those detailed IS controls

1.3.4 The general/application control split was designed specifically to apply to audits whose objective is to form an opinion on data processing integrity, system availability to business users and business information confidentiality.

1.3.5 When internal auditors and independent consultants perform IS audits, the audit objective and scope are ordinarily different from those for business processes including financial audits. The systems in use are a combination of manual and computer processes, and the control objectives must be for the entire process, which may be either wider or narrower than business processes including accounting information records. Therefore, the controls framework used for business process audits may not be appropriate for some IS audits.

1.3.6 To form an opinion on the effectiveness of the detailed controls being audited, the IS auditor should consider the need to assess the effectiveness of management and monitoring of information systems, even where such matters are outside the agreed-upon scope for the audit. The outcome of such considerations may range from an extension of the agreed scope to an appropriately qualified report.

1.3.7 The total population of management and monitoring controls is broad, and some of these controls may not be relevant to the specific audit objective. To assess the audit risk and determine the appropriate audit approach, the IS auditor needs a structured method of determining:

- Those management and monitoring controls that are relevant to the audit scope and objectives
- Those management and monitoring controls that should be tested
- The effect of the relevant management and monitoring controls on the audit opinion

This may be achieved using a framework of controls specific to the use of IS and related technology, which may help the IS auditor to focus on the key controls that affect the information systems and operations being audited.

1.3.8 The IS auditor should consider it in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

2. CONTROLS FRAMEWORK

2.1 Overview

2.1.1 COBIT defines control as 'The policies, procedures, practices and organisational structures, designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected'.

G11 Effect of Pervasive IS Controls cont.

For each IS audit, the IS auditor should differentiate between those general controls which affect all information systems and operations (pervasive IS controls) and those general and application controls that operate at a more specific level (detailed IS controls) to focus audit effort on the risk areas relevant to the IS audit objective. The purpose of the controls framework described in this section is to assist the IS auditor in achieving this focus.

2.2 Pervasive IS Controls

2.2.1 The term 'pervasive IS controls' is defined in the ISACA glossary at *www.isaca.org/glossary.* Pervasive IS controls are a subset of general controls; they are those general controls that focus on the management and monitoring of IS.

2.2.2 The effect of pervasive IS controls on the IS auditor's work is not limited to the reliability of application controls in the business process systems. Pervasive IS controls also affect the reliability of the detailed IS controls over, for example:

- Application program development
- System implementation
- Security administration
- Backup procedures

2.2.3 Weak management and monitoring of IS (i.e., weak pervasive IS controls) should alert the IS auditor to the possibility of a high risk that the controls designed to operate at the detailed level may be ineffective.

2.2.4 Pervasive controls are most effectively determined via a risk assessment where crucial processes and controls are identified. For example, depending upon the organisation, the risk assessment may result in rating the controls (i.e., segregation of duties) around the evaluation of program changes from the testing environment into the production processing environment. Specifically, controls that segregate the program development and change environment from the production process environment may be considered pervasive controls. The means and method of accomplishing this control objective ensures that the elevation of new or modified programs is performed by those individuals typically assigned to the production processing environment. Accordingly, pervasive controls are essential to the reliance placed upon other detailed controls.

2.3 Detailed IS Controls

2.3.1 The term detailed IS controls is defined in the ISACA glossary at *www.isaca.org/glossary*. They are made up of application controls plus those general controls not included in pervasive IS controls. In the COBIT framework, detailed IS controls are the controls over the acquisition, implementation, delivery and support of IS systems and services. Examples include controls over:

- Implementation of software packages
- System security parameters
- Disaster recovery planning
- Data input validation
- Exception report production
- User accounts

Application controls are a subset of detailed IS controls. Data input validation, for example, is both a detailed IS control and an application control. AI7 *Install and accredit solutions and changes* is an IS control, but not an application control.

2.3.2 The relationships amongst IS controls are shown in the following outline:

IS Controls

→ General controls
  - Pervasive IS controls
  - Detailed IS controls

→ Application controls

In addition, the IS auditor should consider the effect of non-IS controls on scope and audit procedures.

2.4 Interaction of Pervasive and Detailed IS Controls

2.4.1 Pervasive controls should be analysed based upon the four domains in COBIT:

- Plan and Organise (PO)
- Acquire and Implement (AI)
- Deliver and Support (DS)
- Monitor and Evaluate (ME)

2.4.2 Pervasive controls should be identified from the risks associated with the loss of system availability, data integrity and information confidentiality. For example, controls prohibiting unauthorised and consequential update, which will go undetected, to production data used in either financial or non-financial reporting of a publicly traded company may be construed as a pervasive control from a data-integrity perspective. The remaining parts of 2.4 further illustrate potential pervasive controls in each of the domains.

2.4.3 The effectiveness of the controls in the AI and DS domains is influenced by the effectiveness of the controls operated in the PO and ME domains. Inadequate planning, organisation and monitoring by management imply that controls over acquisition, implementation, and service delivery and support will be ineffective. Conversely, strong planning, organisation and monitoring can identify and correct ineffective controls over acquisition, implementation, and service delivery and support.

2.4.4 For example, detailed IS controls over the COBIT process AI2 *Acquire and maintain application software* include the following COBIT processes:

- PO1 *Define a strategic IT plan*
- PO8 *Manage quality*

- PO10 *Manage projects*
- ME1 *Monitor and evaluate IT performance*

2.4.5 An audit of an application system acquisition should include the identification of the effect of the IS strategy, the project management approach, quality management and the approach to monitoring. Where, for example, project management is inadequate, the IS auditor should consider:

- Planning additional work to provide assurance that the specific project being audited is being effectively managed
- Reporting weaknesses in pervasive IS controls to management

2.4.6 A further example is that effective detailed IS controls over the COBIT process DS5 *Ensure systems security* are affected by the adequacy of pervasive IS controls over processes including the following COBIT processes:

- PO4 *Define the IT processes, organisation and relationships*
- PO6 *Communicate management aims and direction*
- PO9 *Assess and manage IT risks*
- ME1 *Monitor and evaluate IT performance*

2.4.7 An audit of the adequacy of security parameters in a system should include consideration of management's security policies (PO6), allocation of security responsibilities (PO4), risk assessment procedures (PO9) and procedures for monitoring compliance with its security policies (ME1). Even where the parameters do not comply with the IS auditor's view of best practice, they may be evaluated as adequate in light of the risks identified by management and the management policies that direct how such a level of risk should be addressed. Any audit recommendations for improvement, as well as the detailed parameters themselves, should then be directed to risk management.

3. PLANNING

3.1 Approach to Relevant Pervasive IS Controls

3.1.1 The IS Auditing Guideline G15 Planning states that the IS auditor should perform a preliminary assessment of control over the function being audited. A risk assessment is essential in identifying and evaluating relevant pervasive IS controls. The testing of pervasive IS controls may take place on a different cycle to the specific IS audit being performed, since, by their nature, they cover many different aspects of IS usage. The IS auditor should, therefore, consider whether any previous audit work in this area could be relied upon to identify and evaluate these controls.

3.1.2 Where audit work indicates that pervasive IS controls are unsatisfactory, the IS auditor should consider the effect of this finding on the planned approach to achieving the audit objective:

- Strong pervasive IS controls can contribute to the assurance that may be obtained by an IS auditor in relation to detailed IS controls.
- Weak pervasive IS controls may undermine strong detailed IS controls or exacerbate weaknesses at the detailed level.

3.2 Sufficient Audit Procedures

3.2.1 Where pervasive IS controls have a significant potential effect on the audit objective, it is not sufficient to plan to audit only the detailed controls. Where it is not possible or practical to audit the pervasive IS controls, this restriction of scope should be reported.

3.2.2 The IS auditor should plan to test the relevant pervasive IS controls, where this test will contribute to achieving the audit objective.

3.3 Relevant Controls

3.3.1 Relevant pervasive IS controls are those that have an effect on the specific audit objectives for the assignment. For example, where the audit objective is to report on the controls around changes to a specific programme library, pervasive IS controls relating to security policies (PO6) will be relevant, but pervasive IS controls relating to determination of the technological direction (PO3) may not be relevant.

3.3.2 In planning the audit, the IS auditor should identify which of the total population of pervasive IS controls have an effect on the specific audit objectives, and should plan to include these in the audit scope. COBIT's control objectives for the PO and ME domains may help the IS auditor to identify relevant pervasive IS controls.

3.4 Audit Evidence

3.4.1 The IS auditor should plan to obtain audit evidence that relevant controls are operating effectively. Potential tests are outlined in section 4, Performance of Audit Work.

3.5 Approach to Relevant Detailed IS Controls

3.5.1 Where IS audit work indicates that pervasive IS controls are satisfactory, the IS auditor may consider reducing the level of testing planned for detailed IS controls, since the audit evidence of strong pervasive IS controls will contribute to the assurance that may be obtained by an IS auditor in relation to detailed IS controls.

3.5.2 Where IS audit work indicates that pervasive IS controls are not satisfactory, the IS auditor should carry out sufficient testing of detailed IS controls to provide audit evidence that they are working effectively in spite of weaknesses in the relevant pervasive IS controls.

4. PERFORMANCE OFAUDIT WORK

4.1. Testing Pervasive IS Controls

4.1.1 The IS auditor should carry out sufficient testing to provide assurance that relevant pervasive IS controls were operating effectively in the audit period or at a specific point in time. Test procedures that may be appropriate include:

- Observation

- Corroborative inquiries
- Review of relevant documentation (e.g., policies, standards, meeting minutes)
- Reperformance (e.g., using CAATs)

4.1.2 If the testing of the relevant pervasive IS controls indicates that they are satisfactory, the IS auditor should proceed with the planned audit of the detailed IS controls that are directly applicable to the audit objective. The level of such testing may be less than would be appropriate if the pervasive IS controls were not operating satisfactorily.

5. REPORTING

5.1 Pervasive IS Control Weaknesses

5.1.1 Where the IS auditor has identified weaknesses in pervasive IS controls, these should be brought to the attention of management, even where consideration of such areas was not specifically identified in the agreed-upon scope of work.

5.2 Restrictions on Scope

5.2.1 Where pervasive IS controls could have a significant potential effect on the effectiveness of detailed IS controls and the pervasive IS controls have not been audited, the IS auditor should bring this fact to the attention of management in the final report, together with a statement of the potential effect on the audit findings, conclusions and recommendations. For example, when an IS auditor is reporting on an audit of the acquisition of a package solution, but has not seen the organisation's IS strategy, the IS auditor should include in the report a statement that the IS strategy has not been made available or does not exist. Where relevant, the IS auditor should go on to report the potential effect on the audit findings, conclusions and recommendations, e.g., through a statement that it is not possible to say whether the acquisition of the package solution is consistent with the IS strategy and will support the future plans of the business.

6. EFFECTIVE DATE

6.1 This guideline is effective for all IS audits beginning on or after 1 March 2000. The guideline has been reviewed and updated effective 1 August 2008.

G12 Organisational Relationship and Independence

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S2 Independence states: 'In all matters related to the audit, the IS auditor should be independent of the auditee in both attitude and appearance'.

1.1.2 Standard S2 Independence states: 'The IS audit function should be independent of the area or activity being reviewed to permit objective completion of the audit assignment'.

1.1.3 Standard S3 Professional Ethics and Standards states: 'The IS auditor should adhere to the ISACA Code of Professional Ethics'.

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the independence requirement of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary.

1.2.2 PO4 *Define the IT processes, organisation and relationships* satisfies the business requirement for IT of being agile in responding to the business strategy whilst complying with governance requirements and providing defined and competent points of contact by focusing on establishing transparent, flexible and responsive IT organisational structures and defining and implementing IT processes with owners, roles and responsibilities integrated into business and decision processes.

1.2.3 Secondary references:

- ME2 *Monitor and evaluate internal control*
- ME4 *Provide IT governance*

1.2.4 The information criteria most relevant are:

- Primary: Effectiveness and efficiency
- Secondary: Confidentiality, integrity, availability, compliance and reliability

1.3 Need For Guideline

1.3.1 The purpose of this guideline is to expand on the meaning of 'independence' as used in standard S2 and to address the IS auditor's attitude and independence in IS auditing.

1.3.2 This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

2. INDEPENDENCE

2.1 Attitude

2.1.1 IS auditors should seek adherence to applicable codes of professional ethics and auditing standards in all of their work.

2.1.2 As per COBIT, the audit charter should ensure that the independence, authority and accountability of the audit function are maintained and established by appropriate members of the organisation's management team.

3. PLANNING

3.1 Staffing

3.1.1 The IS auditor establishes many relationships with people involved in the audit activity and has the opportunity to explore the innermost aspects of the area being audited, often the whole organisation. The IS auditor's attitude should always be appropriate to this role. Planning should take into account any known relationships.

3.1.2 IS auditors should not participate in an audit if their independence is impaired. For example, independence is impaired if IS auditors have some expectation of financial gain or other personal advantage due to their influence on the results of the audit. However, the IS auditors' independence would not necessarily be impaired as a result of performing an audit of IS where their personal transactions occur in the normal course of business.

3.1.3 At the beginning of the audit, IS auditors may be required to sign a conflict-of-interest statement to declare their independence.

3.2 Prioritised Audit Plan

3.2.1 COBIT process ME4 states: 'Management should provide for independent audit'. To achieve this objective, an audit plan should be established. This plan should verify that regular and independent assurance is obtained regarding the effectiveness, efficiency and economy of security and internal control procedures. Within this plan, management should determine priorities regarding obtaining independent assurance.

4. PERFORMANCE OF AUDIT WORK

4.1 Organisation

4.1.1 IS auditors should be organisationally independent of the area being audited. Independence is impaired if the IS auditors have direct control over the area being audited. The IS auditors' independence can also be impaired if the IS auditors have direct reporting responsibility to those individuals who have direct control over the area being audited. The IS auditors' independence also may be impaired if IS auditors are required, for tracking purposes, to report their time expended in performing the audit, including progress, audit issues, etc., to the IT group responsible for those controls tested and who report the results to senior or executive management. This could be perceived as the IT group project managing the IS auditors and, thus, an impairment of the IS auditors' independence. In addition, IS auditors should take into consideration if independence has been impaired in situations where the scope of work performed is based on requirements of the control process owners for business or regulatory purposes.

4.1.2 Independence should be regularly assessed by the IS auditor and management. This assessment should consider such factors as changes in personal relationships, financial interests, and prior job assignments and responsibilities. IS auditors should consider the use of control self-assessment techniques in this continuous assessment process.

4.1.3 Depending on the assignment, IS auditors can interview persons, analyse organisational processes, gain assistance from the organisation's staff, etc. An IS auditor's attitude and appearance of independence should always be adequate to meet these situations. IS auditors should be aware that the appearance of independence can be influenced by their actions or associations. Perceptions of the IS auditors' independence could affect the acceptance of their work.

4.1.4 If IS auditors become aware that a situation or relationship is perceived to impair their independence, they should inform audit management of the perceived impairment as soon as possible.

4.2 Gathering Information

4.2.1 Amongst the various items needed to obtain an understanding of the organisation being audited, IS auditors, to preserve their independence, should review:

- Organisation policies and procedures relating to the independent assurance process
- Audit charter, mission statement, policies, procedures and standards, prior reports, and audit plans
- The organisational chart

4.3 Controls Evaluation

4.3.1 IS audit plans should define the activities from which IS auditors are required to be independent. IS auditors' independence from these activities should be regularly monitored by senior management, or by the person who determines and approves IS audit plans. This monitoring should include an assessment of the process for assigning individual IS auditors to specific assignments, to verify that this process assures independence and sufficient skills.

4.3.2 Verification of the IS auditors' adherence to applicable professional codes of conduct should always be carried out. In many circumstances, this should be sufficient to provide audit evidence of independence. If there is an indication that an IS auditor's independence has been compromised, a revision of the audit plan should be considered.

5. REPORTING

5.1 Effect on Reporting

5.1.1 In circumstances where the IS auditor's independence is impaired and the IS auditor continues to be associated with the audit, the facts surrounding the issue of the IS auditor's independence should be disclosed to the appropriate management and in the report.

6. EFFECTIVE DATE

6.1 This guideline is effective for all IS audits beginning on or after 1 September 2000. The guideline has been reviewed and updated effective 1 August 2008**.**

G13 Use of Risk Assessment in Audit Planning

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S5 Planning states: 'The IS auditor should plan the IS audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards'.

1.1.2 Standard S6 Performance of Audit Work states: 'During the course of the audit, the IS auditor should obtain sufficient and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.1.3 Paragraph 2.4.1 of IS Auditing Guideline G15 Planning states: 'An assessment of risk should be made to provide reasonable assurance that material items will be covered adequately during the audit work. This assessment should identify areas with relatively high risk of existence of material problems'.

1.2 Linkage to Procedures

1.2.1 This guideline may be used in conjunction with IS Auditing Procedure P1 IS Risk Assessment Measurement.

1.3 Linkage to CobiT

1.3.1 Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT's control objectives and associated management practices. To meet the audit documentation requirement of IS auditors, the processes in CobiT most likely to be relevant, selected and adapted are classified here as primary and secondary.

1.3.2 PO9 Assess *and manage IT risks* satisfies the business requirement for IT of analysing and communicating IT risks and their potential impact on business processes and goals by focusing on development of a risk management framework that is integrated in business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk.

1.3.2 ME2 *Monitor and Evaluate Internal Control* satisfies the business requirement for IT of protecting the achievement of IT objectives and complying with IT-related laws, regulations and contracts by focusing on monitoring the internal control processes for IT-related activities and identifying improvement actions.

1.3.5 Secondary references:

- ME3 *Ensure regulatory compliance*
- ME4 *Provide IT governance*

1.3.6 The information criteria most relevant are:

- Primary: Confidentiality, integrity, availability
- Secondary: Effectiveness, efficiency, compliance and reliability

1.4 Need for Guideline

1.4.1 The level of audit work required to meet a specific audit objective is a subjective decision made by the IS auditor. The risk of reaching an incorrect conclusion based on the audit findings (audit risk) is one aspect of this decision. The other is the risk of errors occurring in the area being audited (error risk). Recommended practices for risk assessment in carrying out financial audits are well documented in auditing standards for financial auditors, but guidance is required on how to apply such techniques to IS audits.

1.4.2 Members of management also bases their decisions on how much control is appropriate upon assessment of the level of risk exposure that they are prepared to accept. For example, the inability to process computer applications for a period of time is an exposure that could result from unexpected and undesirable events (e.g., data centre fire). Exposures can be reduced by the implementation of appropriately designed controls. These controls are ordinarily based upon probabilistic estimation of the occurrence of adverse events and are intended to decrease such probability. For example, a fire alarm does not prevent fires, but it is intended to reduce the extent of fire damage.

1.4.3 This guideline provides guidance in applying IS Auditing Standards. The IS auditor should consider it in determining how to achieve implementation of standards S5 and S6, use professional judgement in its application, and be prepared to justify any departure.

2. PLANNING

2.1 Selection of a Risk Assessment Methodology

2.1.1 There are many risk assessment methodologies available from which the IS auditor may choose. These range from simple classifications of high, medium and low, based on the IS auditor's judgement, to complex and apparently scientific calculations to provide a numeric risk rating. IS auditors should consider the level of complexity and detail appropriate for the organisation being audited.

2.1.2 IS auditors should include, at a minimum, an analysis, within the methodology, of the risks to the enterprise resulting from the loss of and controls supporting system availability, data integrity and business information confidentiality.

2.1.3 All risk assessment methodologies rely on subjective judgements at some point in the process (e.g., for assigning weightings to the various parameters). The IS auditor should identify the subjective decisions required to use a particular methodology and consider whether these judgments can be made and validated to an appropriate level of accuracy.

2.1.4 In deciding which is the most appropriate risk assessment methodology, IS auditors should consider such things as:

- The type of information required to be collected (some systems use financial effects as the only measure—this is not always appropriate for IS audits)
- The cost of software or other licences required to use the methodology
- The extent to which the information required is already available

- The amount of additional information required to be collected before reliable output can be obtained, and the cost of collecting this information (including the time required to be invested in the collection exercise)
- The opinions of other users of the methodology, and their views of how well it has assisted them in improving the efficiency and/or effectiveness of their audits
- The willingness of management to accept the methodology as the means of determining the type and level of audit work carried out

2.1.5 No single risk assessment methodology can be expected to be appropriate in all situations. Conditions affecting audits may change over time. Periodically, the IS auditor should re-evaluate the appropriateness of the chosen risk assessment methodologies.

2.2 Use of Risk Assessment

2.2.1 IS auditors should use the selected risk assessment techniques in developing the overall audit plan and in planning specific audits. Risk assessment, in combination with other audit techniques, should be considered in making planning decisions such as:

- The nature, extent and timing of audit procedures
- The areas or business functions to be audited
- The amount of time and resources to be allocated to an audit

2.2.2 The IS auditor should consider each of the following types of risk to determine their overall level:

- Inherent risk
- Control risk
- Detection risk

2.3 Inherent Risk

2.3.1 Inherent risk is the susceptibility of an audit area to error in a way that could be material, individually or in combination with other errors, assuming that there were no related internal controls. For example, the inherent risk associated with operating system security is ordinarily high, since changes to, or even disclosure of, data or programs through operating system security weaknesses could result in false management information or competitive disadvantage. By contrast, the inherent risk associated with security for a stand-alone PC, when a proper analysis demonstrates it is not used for business-critical purposes, is ordinarily low.

2.3.2 Inherent risk for most IS audit areas is ordinarily high since the potential effects of errors ordinarily spans several business systems and many users.

2.3.3 In assessing the inherent risk, the IS auditor should consider both pervasive and detailed IS controls. This does not apply to circumstances where the IS auditor's assignment is related to pervasive IS controls only.

2.3.4 At the pervasive IS control level, the IS auditor should consider, to the level appropriate for the audit area in question:

- The integrity of IS management and IS management experience and knowledge
- Changes in IS management
- Pressures on IS management that may predispose them to conceal or misstate information (e.g., large business-critical project overruns, hacker activity)
- The nature of the organisation's business and systems (e.g., the plans for e-commerce, the complexity of the systems, the lack of integrated systems)
- Factors affecting the organisation's industry as a whole (e.g., changes in technology, IS staff availability)
- The level of third-party influence on the control of the systems being audited (e.g., because of supply chain integration, outsourced IS processes, joint business ventures, and direct access by customers)
- Findings from and date of previous audits

2.3.5 At the detailed IS control level, the IS auditor should consider, to the level appropriate for the audit area in question:

- The findings from and date of previous audits in this area
- The complexity of the systems involved
- The level of manual intervention required
- The susceptibility to loss or misappropriation of the assets controlled by the system (e.g., inventory, payroll)
- The likelihood of activity peaks at certain times in the audit period
- Activities outside the day-to-day routine of IS processing (e.g., the use of operating system utilities to amend data)
- The integrity, experience and skills of management and staff involved in applying the IS controls

2.4 Control Risk

2.4.1 Control risk is the risk that an error that could occur in an audit area and could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often missed easily, owing to the volume of logged information. The control risk associated with computerised data validation procedures is ordinarily low because the processes are consistently applied.

2.4.2 The IS auditor should assess the control risk as high unless relevant internal controls are:

- Identified
- Evaluated as effective
- Tested and proved to be operating appropriately

2.5 Detection Risk

2.5.1 Detection risk is the risk that the IS auditor's substantive procedures will not detect an error that could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with identifying a lack of disaster recovery plans is ordinarily low, since existence is verified easily.

2.5.2 In determining the level of substantive testing required, IS auditors should consider both:

- The assessment of inherent risk
- The conclusion reached on control risk following compliance testing

2.5.3 The higher the assessment of inherent and control risk the more audit evidence IS auditors should normally obtain from the performance of substantive audit procedures.

3. PERFORMANCE OF AUDIT WORK

3.1 Documentation

3.1.1 IS auditors should consider documenting the risk assessment technique or methodology used for a specific audit. The documentation should ordinarily include:

- A description of the risk assessment methodology used
- The identification of significant exposures and the corresponding risks
- The risks and exposures the audit is intended to address
- The audit evidence used to support the IS auditor's assessment of risk

4. EFFECTIVE DATE

4.1 This guideline is effective for all IS audits beginning on or after 1 September 2000. The guideline has been reviewed and updated effective 1 August 2008.

G14 Application Systems Review

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the G 14 Application Systems Reviews requirements of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.2 Primary IT processes are:

- PO9 *Assess and manage IT risks*
- AI2 *Acquire and maintain application software*
- DS5 *Ensure systems security*
- ME2 *Monitor and evaluate internal control*

1.2.3 Secondary IT processes are:

- PO7 *Manage IT human resources*
- PO8 *Manage quality*
- A16 *Manage changes*
- DS3 *Manage performance and capacity*
- DS10 *Manage problems*
- DS11 *Manage data*

1.2.4 The information criteria most relevant to application system reviews are:

- Primary: Availability, reliability, integrity and confidentiality
- Secondary: Compliance, effectiveness and efficiency

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to describe the recommended practices in performing an application systems review.

1.3.2 The purpose of an application systems review is to identify, document, test and evaluate the controls over an application that are implemented by an organisation to achieve relevant control objectives. These control objectives can be categorised into control objectives over the system and the related data.

2. PLANNING

2.1 Planning Considerations

2.1.1 An integral part of planning is understanding the organisation's IS environment to a sufficient extent for the IS auditor to determine the size and complexity of the systems and the extent of the enterprise's dependence on information systems. The IS auditor should gain an understanding of the enterprise's mission and business objectives, the level and manner in which information technology and information systems are used to support the enterprise, and the risks and exposures associated with the enterprise's objectives and its information systems. Also, an understanding of the organisational structure including roles and responsibilities of key IS staff and the business process owner of the application system should be obtained.

2.1.2 A primary objective of planning is to identify the application-level risks. The relative level of risk influences the level of audit evidence required.

2.1.3 Application-level risks at the system and data level include such things as:

- System availability risks relating to the lack of system operational capability
- System security risks relating to unauthorised access to systems and/or data
- System integrity risks relating to the incomplete, inaccurate, untimely or unauthorised processing of data
- System maintainability risks relating to the inability to update the system when required in a manner that continues to provide for system availability, security and integrity
- Data risks relating to its completeness, integrity, confidentiality, privacy and accuracy

2.1.4 Application controls to address the application-level risks may be in the form of computerized controls built into the system, manually performed controls, or a combination of both. Examples include the computerized matching of documents (purchase order, invoice and goods received report), the checking and signing of a computer generated cheque and the review by senior management of exception reports.

2.1.5 Where the option to place reliance on programmed controls is taken, relevant general IT controls should be considered, as well as controls specifically relevant to the audit objective. General IT controls could be the subject of a separate review, which would include such things as physical controls, system-level security, network management, data backup and contingency planning. Depending on the control objectives of the review, the IS auditor may not need to review general

controls, such as where an application system is being evaluated for acquisition.

2.1.6 Application system reviews can be performed when a package application system is being evaluated for acquisition, before the application system goes into production (pre-implementation) and after the application system has gone into production (post-implementation). Pre-implementation application system review coverage includes the architecture of application-level security, plans for the implementation of security, the adequacy of system and user documentation, and the adequacy of actual or planned user-acceptance testing. Post-implementation review coverage includes application-level security after implementation and system conversion if there has been a transfer of data and master file information from the old to the new system.

2.1.7 The objectives and scope of an application systems review usually form part of the terms of reference. The form and content of the terms of reference may vary but should include:

- The objectives and scope of the review
- IS auditors performing the review
- A statement regarding the independence of the IS auditors from the project
- When the review will commence
- The time frame of the review
- Reporting arrangements
- Closing meeting arrangements
- Objectives should be developed to address the seven COBIT information criteria and then agreed upon by the enterprise. The seven COBIT information criteria are:
  - Effectiveness
  - Efficiency
  - Confidentiality
  - Integrity
  - Availability
  - Compliance
  - Reliability of information

2.1.8 Where the IS auditor has been involved previously in the development, acquisition, implementation or maintenance of an application system and is assigned to an audit engagement, the independence of the IS auditor may be impaired. The IS auditor should refer to appropriate guidelines to deal with such circumstances.

3. PERFORMANCE OF AUDIT WORK

3.1 Documenting the Flow of Transactions

3.1.1 Information gathered should include both the computerized and manual aspects of the system. The focus should be on data input (whether electronic or manual), processing, storage and output that are of significance to the audit objective. The IS auditor may find, depending upon the business processes and the use of technology, that documenting the transaction flow may not be practical. In that event, the IS auditor should prepare a high-level data-flow diagram or narrative and/or utilise system documentation if provided. Consideration should also be given to documenting application interfaces with other systems.

3.1.2 The IS auditor may confirm the documentation by performing procedures such as a walk-through test.

3.2 Identifying and Testing the Application System Controls

3.2.1 Specific controls to mitigate the application risks may be identified and sufficient audit evidence obtained to assure the IS auditor that the controls are operating as intended. This can be accomplished through procedures such as:

- Inquiry and observation
- Review of documentation
- Testing of the application system controls where programmed controls are being tested. The use of computer-assisted audit techniques (CAATs) may be considered.

3.2.2 The nature, timing and extent of testing should be based on the level of risk to the area under review and the audit objectives. In the absence of strong general IT controls, the IS auditor may make an assessment of the effect of this weakness on the reliability of the computerized application controls.

3.2.3 If the IS auditor finds significant weaknesses in the computerized application controls, assurance should be obtained (depending on the audit objective), if possible, from the manually performed processing controls.

3.2.4 The effectiveness of computerized controls is dependent on strong general IT controls. Therefore, if general IT controls are not reviewed, the ability to place reliance on the application controls may be limited severely and the IS auditor should consider alternative procedures.

4. REPORTING

4.1 Weaknesses

4.1.1 Weaknesses identified in the application review either due to an absence of controls or to non-compliance should be brought to the attention of the business process owner and to the IS management responsible for the support of the application.

Where weaknesses identified during the application systems review are considered to be significant or material, the appropriate level of management should be advised to undertake immediate corrective action.

4.1.2 Since effective computerized application controls are dependent on general IT controls, weaknesses in this area should also be reported. In the event that general IT controls were not reviewed, this fact should be included in the report.

4.1.3 The IS auditor should include appropriate recommendations to strengthen controls in the report.

5. EFFECTIVE DATE

5.1 This guideline is effective for all IS audits beginning on or after 1 November 2001. The guideline has been reviewed and updated effective 1 December 2008.

G15 Audit Planning

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S5 Planning states that IT audit and assurance professionals should plan the information systems (IS) audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards. They should develop and document:

- A risk-based audit approach
- An audit plan that details the nature and objectives, timing and extent, objectives, and resources required
- An audit programme and/or plan detailing the nature, timing and extent of the audit procedures required to complete the audit

1.1.2 Standard S11 Use of Risk Assessment in Audit Planning states that IT audit and assurance professionals should:

- Use an appropriate risk assessment technique or approach in developing the overall IT audit plan and in determining priorities for the effective allocation of IT audit resources
- When planning individual reviews, identify and assess risks relevant to the area under review and its relationship to other auditable areas

1.1.3 Standard S12 Audit Materiality states that the IT audit and assurance professionals should consider:

- Audit materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures
- While planning for an audit, potential weaknesses or absences of controls and whether such weaknesses or absences of controls could result in significant deficiency or a material weakness in the information system
- The cumulative effect of minor control deficiencies or weaknesses and absences of controls to translate into significant deficiency or material weakness in the information system

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the planning requirements of IT audit and assurance professionals, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The processes and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.3 Primary IT processes are:

- ME1 *Monitor and evaluate IT performance*
- ME2 *Monitor and evaluate internal control*
- ME3 *Ensure compliance with external requirements*

1.2.4 Secondary IT process is:

- ME4 *Provide IT governance*

1.2.5 The information criteria most relevant are:

- Primary: Effectiveness, efficiency, availability and compliance
- Secondary: Confidentiality, integrity and reliability

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to define the components of the planning process as stated in standard S5 of *ITAF: A Professional Practices Framework for IT Assurance*.

1.3.2 This guideline also provides for planning in the audit process to meet the objectives set by COBIT.

2. PRELIMINARY ENGAGEMENT ACTIVITIES

2.1 Purpose

2.1.1 The purpose of performing these preliminary engagement activities is to help ensure that IT audit and assurance professionals have considered any events or circumstances that may adversely affect their ability to plan and perform the audit engagement and reduce audit risk to an acceptably low level. Performing these preliminary engagement activities helps to ensure the audit engagement plans include that:

- IT audit and assurance professionals maintain the necessary independence and ability to perform the engagement
- There are no issues with management integrity that may affect IT audit and assurance professionals' willingness to continue the engagement
- There is no misunderstanding with the clients as to the terms of the engagement

2.2 Activities

2.2.1 IT audit and assurance professionals should perform procedures regarding the continuance of the client relationship and the specific audit engagement. For continuing audit engagements, such initial procedures often occur shortly after (or in connection with) the completion of the previous audit.

2.2.2 IT audit and assurance professionals should evaluate compliance with ethical requirements, including independence. IT audit and assurance professionals' initial procedures on both clients' continuance and evaluation of ethical requirements (including independence) are performed prior to performing other significant activities for the current audit engagement.

2.2.3 IT audit and assurance professionals should establish an understanding of the terms of the engagement.

G15 Audit Planning cont

3. PLANNING

3.1 Audit Strategy

3.1.1 IT audit and assurance professionals should plan the engagement, so that it will be performed in an effective manner, and establish the overall audit strategy for the audit. Adequate planning helps to ensure that appropriate attention is devoted to important areas of the audit, potential problems are identified and resolved on a timely basis, and the audit engagement is properly organised and managed to be performed in an effective and efficient manner.

3.1.2 A clear project definition is a critical success factor to ensure project effectiveness and efficiency. An audit project should include in the terms of reference such items as:

- Areas to be audited
- Type of work planned
- High-level objectives and scope of the work
- Topics, e.g., budget, resource allocation, schedule dates, type of report, intended audience
- Other general aspects of the work, when applicable

3.1.3 For an internal audit function, a comprehensive risk-based audit plan should be developed/updated, at least annually, for ongoing activities. This high-level plan should act as a framework for audit activities and serve to address responsibilities set by the audit charter.

3.1.4 A plan should normally be prepared for each audit assignment. The plan should document the objectives of the audit.

3.1.5 Each audit project should be referenced either to the general audit plan or state the specific mandate, objectives and other relevant aspects of the work to be performed.

3.1.6 IT audit and assurance professionals should develop an audit plan that takes into consideration the objectives of the auditee relevant to the audit area and the related technology infrastructure. Where appropriate, they should also consider the area under review and its relationship to the enterprise (strategically, financially and/or operationally) and obtain information on the strategic plan, including the IT strategic plan and any other relevant documentation related to the auditee.

3.1.7 IT audit and assurance professionals should have an understanding of the auditee's information architecture and the auditee's technological direction to be able to design a plan appropriate for the present and, where appropriate, future technology of the auditee.

3.2 Knowledge of the Enterprise

3.2.1 Understanding the auditee´s business and the risks it faces is a critical step to developing an effective audit plan focused on the areas most sensitive to fraudulent or inaccurate practices.

3.2.2 Before beginning an audit project, the work of IT audit and assurance professionals should be planned in a manner appropriate for meeting the audit objectives. As a part of the planning process, they should obtain an understanding of the enterprise and its processes. In addition to giving IT audit and assurance professionals an understanding of the enterprise's operations and its IT requirements, this will assist them in determining the significance of the IT resources being reviewed as they relate to the objectives of the enterprise. IT audit and assurance professionals should also establish the scope of the audit work and perform a preliminary assessment of internal control over the function being reviewed.

3.2.3 The extent of the knowledge of the enterprise and its processes required by IT audit and assurance professionals will be determined by the nature of the enterprise and the level of detail at which the audit work is being performed. IT audit and assurance professionals may require specialised knowledge when dealing with unusual or complex operations. A more extensive knowledge of the enterprise and its processes will ordinarily be required when the audit objective involves a wide range of IT functions, rather than when the objectives are for limited functions. For example, a review with the objective of evaluating control over an enterprise's payroll system would ordinarily require a more thorough understanding of the enterprise than a review with the objective of testing controls over a specific programme library system.

3.2.4 IT audit and assurance professionals should gain an understanding of the types of personnel, events, transactions and practices that can have a significant effect on the specific enterprise, function, process or data that is the subject of the auditing project. Knowledge of the enterprise should include the business, financial and inherent risks facing the enterrprise as well as conditions in the enterprise's marketplace and the extent to which the enterprise relies on outsourcing to meet its objectives. IT audit and assurance professionals should use this information in identifying potential problems, formulating the objectives and scope of the work, performing the work, and considering actions of management for which they should be alert.

3.3 Materiality

3.3.1 In the planning process, IT audit and assurance professionals should ordinarily establish levels of planning materiality such that the audit work will be sufficient to meet the audit objectives and will use audit resources efficiently. For example, in the review of an existing system, the IT audit and assurance professional will evaluate materiality of the various components of the system in planning the audit programme for the work to be performed. Both qualitative and quantitative aspects should be considered in determining materiality.

3.4 Risk Assessment

3.4.1 The IT audit and assurance professionals should develop an audit plan for the audit to reduce audit risk to an acceptably level.

3.4.2 A risk assessment should be performed to provide reasonable assurance that all material items will be adequately covered during the audit work. This assessment should identify areas with relatively high probability of material problems.

3.4.3 A risk assessment and prioritisation of identified risks for the area under review and the Enterprise's IT environment should be carried out to the extent necessary.

3.5 Internal Control Evaluation

3.5.1 Audit and assurance projects should include consideration of internal controls either directly as a part of the project objectives or as a basis for reliance upon information being gathered as a part of the project. Where the objective is evaluation of internal controls, IT audit and assurance professionals should consider the extent to which it will be necessary to review such controls. When the objective is to assess the effectiveness of controls over a period of time, the audit plan should include procedures appropriate for meeting the audit objectives, and these procedures should include compliance testing of controls. When the objective is not to assess the effectiveness of controls over a period of time, but rather to identify control procedures at a point in time, compliance testing of controls may be excluded.

3.5.2 When IT audit and assurance professionals evaluate internal controls for the purpose of placing reliance on control procedures in support of information being gathered as part of the audit, they should ordinarily make a preliminary evaluation of the controls and develop the audit plan on the basis of this evaluation. During a review, IT audit and assurance professionals should consider the appropriateness of this evaluation in determining the extent to which controls can be relied upon during testing. For example, in using a computer program to test data files, the IT audit and assurance professional should evaluate controls over program libraries containing programs being used for audit purposes to determine the extent to which the programs are protected from unauthorised modification.

4. CHANGES DURING THE COURSE OF THE AUDIT

4.1 Strategy and Planning

4.1.1 The overall audit strategy and the audit plan should be updated and changed as necessary during the course of the audit.

4.1.2 Planning an audit is a continual and iterative process. As a result of unexpected events, changes in conditions or the audit evidence obtained from the results of audit procedures, the IT audit and assurance professionals may need to modify the overall audit strategy and the resulting planned nature, timing and extent of further audit procedures.

4.1.3 The audit planning should consider the possibility of unexpected events that implicate high risks for the enterprise. Therefore, the audit plan must be able to prioritise such events within the audit and assurance processes in a risk-adequate manner.

5. SUPERVISION

5.1 Engagement Team Members

5.1.1 IT audit and assurance professionals should plan the nature, timing and extent of direction and supervision of engagement team members and review their work. That planning depends on many factors, including the size and complexity of the enterprise, the area of audit, the risks of material misstatement, the capabilities and competence of personnel performing the audit work, and the extent of direction and supervision of engagement team members based on the assessed risk of material misstatement.

6. DOCUMENTATION

6.1 Planning Documentation

6.1.1 The IT audit and assurance professional's work papers should include the audit plan and programme.

6.1.2 The audit plan may be documented on paper or in another appropriate and retrievable form.

6.2 Plan Endorsement

6.2.1 To the extent appropriate, the audit plan, audit programme and any subsequent changes should be approved by audit management.

6.3 Audit Programme

6.3.1 A preliminary programme for review should ordinarily be established by the IT audit and assurance professional before the start of work. This audit programme should be documented in a manner that will permit the IT audit and assurance professional to record completion of the audit work and identify work that remains to be done. As the work progresses, the IT audit and assurance professional should evaluate the adequacy of the programme based on information gathered during the audit. When IT audit and assurance professionals determine that the planned procedures are not sufficient, they should modify the programme accordingly.

6.3.2 **Depending on the audit resources required, the IT audit and assurance professional should include management of the personnel resources required in the audit plan.**

6.3.3 The audit plan should be prepared so that it is in compliance with any appropriate external requirements in addition to the standards as defined in ITAF.

6.3.4 In addition to a listing of the work to be done, the IT audit and assurance professional should, to the extent practicable, prepare a list of personnel and other resources required to complete the work, a schedule for the work, and a budget.

6.3.5 The audit programme and/or plan should be adjusted during the course of the audit to address issues that arise (new risks, incorrect assumptions, or findings from the procedures already performed) during the audit.

7. EFFECTIVE DATE

7.1 This guideline is effective for all IT audits beginning after 1 May 2010.

G16 Effect of Third Parties on an Enterprise's IT Controls

1. BACKGROUND

1.1. Linkage to Standards

1.1.1. Standard S5 Planning states, 'The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable professional auditing standards'.

1.1.2. Standard S6 Performance of Audit Work states, 'During the course of the audit, the IS auditor is to obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.2. Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the responsibility, authority and accountability requirement of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.2 Primary IT processes are:

- PO4 *Define the IT processes, organisation and relationships*
- PO7 *Manage IT human resources*
- AI5 *Procure IT resources*
- DS1 *Manage service levels*
- DS2 *Manage third-party services*
- DS5 *Ensure systems security*
- ME2 *Monitor and evaluate internal control*

1.2.3 Secondary IT processed are:

- PO1 *Define a strategic plan*
- PO2 *Define the information architecture*
- PO8 *Manage quality*
- AI3 *Acquire and maintain technology infrastructure*
- DS12 *Manage the physical environment*
- ME4 *Provide IT governance*

1.2.4 The information criteria most relevant to responsibility, authority and accountability are:

- Primary: Effectiveness, availability, integrity and reliability
- Secondary: Efficiency and confidentiality

1.3 Definitions

1.3.1 Internet service provider (ISP): A third party that provides enterprises with a variety of Internet and Internet-related services

1.3.2 Application or managed service provider (ASP/MSP): A third party that delivers and manages applications and computer services, including security services, to multiple users via the Internet or a private network.

1.3.3 Business service provider (BSP): An ASP that also provides outsourcing of business processes such as payment processing, sales order processing and application development.

1.3.4 In this guideline, ISPs, ASP/MSPs and BSPs are referred to collectively as third parties. Third parties covered under this guideline include any organisation that is separate from the enterprise (such as shared service organisations) whether legally separate or not.

1.4 Guideline Application

1.4.1 When applying this guideline, the IS auditor should consider it in relation to other relevant ISACA guidelines.

1.5 Need for Guideline

1.5.1 This guideline sets out how the IS auditor should comply with the ISACA IS Auditing Standards and COBIT when assessing the effect a third party has on an enterprise's IS controls and related control objectives.

1.5.2 This guideline is not intended to provide guidance on how IS auditor's report on third-party provider controls in accordance with other standard-setting entities.

2. ROLE OF THIRD-PARTY SERVICE PROVIDERS

2.1 Services of Third-party Providers

2.1.1 Enterprises use third-party service providers in a variety of different capacities. These providers often perform important and critical functions for the enterprises and, therefore, usually require access to confidential information, applications and systems.

2.1.2 Third parties provide services such as:

- Business advisory and consulting services
- Connectivity and utility services to the enterprise's partners, suppliers and customers
- Security services
- Providing physical location for hardware (known as co-location)
- Monitoring of system and application access

- Backup and recovery services
- Application development, maintenance and hosting (e.g., enterprise resource planning (ERP) systems, e-commerce systems, web sites)
- Business services such as cash management, credit card services, order processing, call centre services as well as back-office transactional accounting services, such as accounts payable, fixed asset, HR/payroll and/or general ledger accounting/reporting processing

3. EFFECT ON CONTROLS

3.1 Third-party Providers Effect on Controls

3.1.1 When enterprises use third parties, they can become a key component in an enterprise's controls and its achievement of related control objectives.

3.1.2 IS auditors should evaluate the role that the third party performs in relation to the IT environment, related controls and control objectives.

3.1.3 An enterprise that uses third-party providers for limited purposes, such as co-location services, may rely upon these third parties for only limited purposes in achieving its control objectives. However, an enterprise that uses providers for other purposes, such as hosting financial accounting systems and e-commerce systems, utilises the third-party provider's controls wholly or in conjunction with its own controls to achieve its control objectives.

3.1.4 The effectiveness of third-party controls can enhance the ability of an enterprise to achieve its control objectives. Conversely, ineffective third-party controls can weaken the ability of an enterprise to achieve its control objectives. These weaknesses can arise from many sources including:

- Gaps in the control environment arising from the outsourcing of services to the third party
- Poor control design, causing controls to operate ineffectively
- Lack of knowledge and/or inexperience of personnel responsible for control functions
- Over reliance on the third party's controls (when there are no compensating controls within the enterprise)

4. PROCEDURES TO BE PERFORMED BY THE IS AUDITOR

4.1. Obtaining an Understanding

4.1.1 As part of the planning process, IS auditors should obtain and document an understanding of the relationship between the services provided by the third party and the enterprise's control environment. IS auditors should consider reviewing such things as the contract, service level agreements, and policies and procedures between the third party and the enterprise.

4.1.2 IS auditors should document the third party's processes and controls that have a direct effect on the enterprise's processes and control objectives.

4.1.3 IS auditors should thoroughly contemplate and identify risks involved with the process and whether those risks reside with the company and/or the third-party provider.

4.1.4 IS auditors should identify each control, its location in the combined control environment (internal or external), the type of control, its function (preventive, detective or corrective), and the organisation that performs the functions (internal or external) that offset or compensate for those risks.

4.1.5 IS auditors should assess the risk of the services provided by the third party to the enterprise, its controls and control objectives, and determine the significance of third-party controls on the ability of the enterprise to meet its control objectives.

4.2 Confirming the Understanding

4.2.1 IS auditors should confirm their understanding of the control environment.

4.2.2 IS auditors can confirm their understanding of the control environment through a variety of methods including such things as inquiry and observation and process walk-throughs.

4.3 Assessing the Role of Third-party Provider Controls

4.3.1 If the role or effect that the third party has on the enterprise's control objectives is significant, the IS auditor should assess these controls to determine whether they function as described, operate effectively and assist the enterprise in achieving its control objectives. Section 7, Review of Third-party Provider Controls, provides an approach to testing these controls.

5. RISKS ASSOCIATED WITH THIRD-PARTY PROVIDERS

5.1 Effects of Third-party Providers on an Enterprise

5.1.1 Third-party providers can affect an enterprise (including its partners), its processes, controls and control objectives on many different levels. This includes effects arising from such things as:

- The economic viability of the third-party provider
- Third-party provider access to information that is transmitted through their communication systems and applications
- Systems and application availability
- Processing integrity
- Application development and change management processes
- The protection of systems and information assets through backup recovery, contingency planning and redundancy

5.1.2 The lack of controls and/or weakness in their design, operation or effectiveness can lead to such things as:

- Loss of information confidentiality and privacy
- Systems not being available for use when needed
- Unauthorised access and changes to systems, applications or data
- Changes to systems, applications or data occurring that result in system or security failures, loss of data, loss of data integrity, loss of data protection, or system unavailability
- Loss of system resources and/or information assets
- Increased costs incurred by the enterprise as a result of any of the above

5.2 Assessing Identified Control Weaknesses

5.2.1 IS auditors should assess the likelihood (or control risk) that weaknesses in control, design or operation may exist in the IT environment. IS auditors should identify where the control weakness exists.

5.2.2 IS auditors should then assess whether control risk is significant and what effect it has on the control environment.

5.2.3 When weaknesses are identified, IS auditors should also determine if compensating controls exist and to what extent they counter the effect of identified weaknesses (compensating controls may exist at the enterprise, the third-party provider or in both entities). If compensating controls exist, IS auditors should determine if they mitigate the effect of identified control weaknesses.

6. CONTRACTS WITH THIRD-PARTY PROVIDERS

6.1 Roles and Responsibilities

6.1.1 The relationship between the enterprise and a third-party provider should be documented in the form of an executed contract. The contract is a critical element in the relationship between the enterprise and the service provider. These contracts contain many provisions that govern the actions and responsibilities of each party.

6.1.2 IS auditors should review the contract between the enterprise and the third party.

6.1.3 Within the context of this guideline, IS auditors should review the contract (possibly with the assistance of the enterprise's legal counsel) to determine the third party's role and responsibility for assisting the enterprise in achieving its control objectives. Guidance on how to review a contract is outside the scope of this guideline; however, the following list provides examples of issues that should be considered by IS auditors when reviewing the contract:

- Level of service to be provided by the third party (whether to the enterprise, its partners or both)
- Reasonableness of fees charged by the third party
- Responsibilities for design, implementation, performance and monitoring of controls
- Responsibilities for data and application privacy and confidentiality
- Responsibilities for systems, communications, operating system, utility software, data, and application software access controls and administration
- Monitoring of assets and related data and response (enterprise and third party) and reporting procedures (routine and incident)
- Specification of ownership of information assets, including data and domain names
- Specification of ownership of custom programming developed by the third-party provider for the enterprise, including change documentation, source code and escrow agreements
- Provision for systems and data protection, including backup and recovery, contingency planning, and redundancy
- Right to audit clause (including such things as the ability to meet with the third-party provider's internal audit personnel and review their audit work papers and reports)
- Process for negotiation, review and approval of changes to the contract and related documents (such as service level agreements and procedures)

6.1.4 As a minimum, IS auditors should review the contract to determine the extent of responsibility for controls that the third party undertakes on behalf of the enterprise. This process should assess the sufficiency of identified controls and compliance monitoring/reporting, their design, and operating effectiveness.

6.2 Corporate Governance

6.2.1 Even when third-party providers are involved, management is still responsible for the achievement of related control objectives. As part of this responsibility, management should have a process to govern the relationship with and the performance of the third-party provider. IS auditors should identify and review the components of this process. IS auditors should review such things as the process management uses to identify risks associated with the third-party provider, the services provided by the third party and how management governs the relationship between the two entities.

6.2.2 IS auditors' review of the governance process should ascertain such things as whether management reviews the third-party providers against the performance standards or criteria set forth in the contract and any standards specified by regulatory bodies. The governance process should include review of such things as:

- Financial performance of the third-party provider
- Compliance with terms of the contract
- Changes to the control environment mandated by the third party, its auditors and/or regulators
- Results of control reviews performed by others, including the third party's auditors, consultants or others
- Maintaining adequate levels of insurance

G16 Effect of Third Parties on an Enterprise's IT Controls cont.

7. REVIEW OF THIRD-PARTY PROVIDER CONTROLS

7.1 Contractual Limitations

7.1.1 When reviewing third-party provider controls, IS auditors should consider the contractual relationship between the enterprise and the third-party provider and the third-party provider's evaluation and reporting on the controls.

7.1.2 Contractual limitations such as 'right to audit' clauses may preclude IS auditors from reviewing controls at the third-party provider. In these circumstances, IS auditors should assess this limitation of scope on their ability to evaluate the IS control environment.

7.2 Independent Reports

7.2.1 Third-party providers may provide reports from independent sources on their controls. These reports may take the form of service bureau audit reports or other control-based reports. Service auditor's assurance reports are examples of reports issued by independent sources. IS auditors can use these reports as the basis for reliance on controls in the IS control environment.

7.2.2 If the IS auditor decides to use an independent report as the basis for reliance on IS controls at the third-party provider, then the IS auditor should review these reports to determine the following:

- Whether the independent party is qualified. This can include whether the independent party has appropriate professional certification or license, has relevant experience, and is in good standing with applicable professional and regulatory (if applicable) authorities
- Whether the independent party has no relationship with the third-party provider that would impair their independence and objectivity
- The period of coverage of the report
- Whether the report is sufficient (i.e., the report covers the applicable systems and controls and includes tests of areas that an IS auditor would include when performing the work)
- If the testing of the controls is sufficient to enable an IS auditor to rely upon the work of the independent party (i.e., the testing of the controls is sufficient as is the nature, timing and extent of procedures performed)
- If testing exceptions were identified by the independent third party
- Whether the report delineates between the responsibilities of the service provider and the responsibilities of the user enterprise
- Whether the user enterprise has addressed its responsibilities with respect to proper controls

7.2.3 If exceptions exist in testing, IS auditors should determine their impact on control objectives, follow up on whether they have been remediated and assess whether additional testing is required to satisfy the control objective.

7.3 Testing Third-party Controls

7.3.1 If an IS auditor decides to directly review and test controls at the third-party provider, then the IS auditor should do the following:

- Work with management and, as applicable or considered appropriate, internal audit of both enterprises to plan the engagement and set its objectives and scope of review.
- Work with management and, as applicable or considered appropriate, internal audit and staff of both enterprises to determine timing, staffing needs and other issues.
- Address issues such as access to third-party systems and assets and confidentiality.
- Develop an audit programme, budget and engagement plan.
- Validate control objectives.

7.3.2 IS auditors should consider the following areas when setting scope and objectives of the audit:

- Location and environment where third-party services are performed. Remote locations may require special access exceptions that may impact security.
- Size and stability of the third-party provider. The number of employees and size of the company may adversely impact segregation of duties between functions as well as impact appropriateness of access of those employees.
- Housing and handling of data. If the third-party provider is responsible for handling or housing confidential data or assets for multiple clients, privacy, segregation and access controls for employees and customers should be reviewed.

7.3.3 Once the fieldwork has been completed, a conclusion on the operating effectiveness of tested controls should be made. IS auditors should review the effectiveness of the controls within each enterprise and the interplay of controls between the enterprise and the third party.

7.3.4 In most situations, controls overlap between the enterprise and the third-party provider. IS auditors should assess the operating effectiveness of the controls taken together vs. those taken individually.

7.3.5 Situations may also exist where controls for a particular objective in either enterprise may not exist or do not operate effectively. In this situation, IS auditors should assess the effect this weakness has on the overall control environment and on the extent of the procedures.

7.3.6 Situations may also exist where control strengths in one enterprise may be negated partially or completely by control weaknesses in another enterprise. IS auditors are responsible to assess this situation's impact on the overall control environment.

7.4 Internal Auditors of the Third-party Provider

7.4.1 IS auditor's should also consider whether the third-party provider has an internal audit department. The presence of third-party provider internal auditors can enhance the strength of the control environment at the third-party provider.
7.4.2 If an internal audit department exists, IS auditor's should ascertain the extent of their activities with regard to the systems and controls that effect the enterprise.
7.4.3 If possible, IS auditors should review relevant third-party provider internal audit reports.
7.4.4 In situations where it is not possible to review these reports, IS auditors should discuss the scope of these reviews, identify what systems and controls were covered by the reviews, and identify the significant issues and weaknesses.
7.4.5 If the third-party provider is unwilling to grant access to the reports or their internal audit personnel, IS auditors should assess this restriction on the extent of their procedures.
7.4.6 IS auditors should also consider assessing the skills and expertise of the third-party provider's internal audit staff. This can be accomplished through discussions with these individuals and by additional procedures such as reviewing their work plans, work papers and reports.

8. SUBCONTRACTORS OF THIRD PARTIES

8.1 Effect on Controls

8.1.1 IS auditors should determine whether the third party uses subcontractors to provide systems and services.
8.1.2 In situations where subcontractors exist, IS auditors should review the significance of these subcontractors to determine the effect they may have on the primary third party's controls that relate to the enterprise.

8.2 Effect on an Engagement

8.2.1 If the subcontractor does not have a significant effect on the controls relevant to the enterprise, IS auditors should document this in their work papers.
8.2.2 If the subcontractor has a significant effect on the controls relevant to the enterprise, IS auditors should evaluate the processes used by the third party to manage and monitor the relationship with the subcontractor. IS auditors should consider sections 6 and 7 of this guideline when evaluating the third party's controls over its subcontractors.

9. REPORTING

9.1 Weaknesses

9.1.1 The IS auditor's report should indicate that the controls subject to the review extended to controls within the enterprise and those that exist at the third-party organisation. In addition, IS auditors should consider identifying the controls, control weaknesses and compensating controls that exist in each enterprise.
9.1.2 The extent to which conclusions and recommendations are communicated should be documented in the terms of reference. Some third parties may not be willing, or able, to implement recommendations. In these situations, the IS auditor should recommend compensating controls that the enterprise could implement to address control weaknesses at the third-party organisation. In some cases, the enterprise may have to refer back to contract language to determine the appropriate course of action with management if significant issues continue to exist.

10. EFFECTIVE DATE

10.1 This guideline is effective for all IS audits beginning on or after 1 March 2002. The guideline has been reviewed and updated effective 1 March 2009.

G17 Effect of Nonaudit Role on the IT Audit and Assurance Professional's Independence

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S2 Independence states that in all matters related to the audit, the IT audit and assurance professional should be independent of the auditee in both attitude and appearance.

1.1.2 Standard S2 Independence states that the IT audit and assurance function should be sufficiently independent of the area or activity being reviewed to permit objective completion of the audit and assurance assignment.

1.1.3 Standard S3 Professional Ethics and Standards states that the IT audit and assurance professional should exercise due professional care, including observance of applicable professional standards in conducting audit and assurance assignments.

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit and assurance assignment is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the effect of non-audit roles on the IT audit and assurance professional's independence, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.2 Primary IT processes are:

- PO6 *Communicate management aims and direction*
- PO9 *Assess and manage IT risks*
- PO10 *Manage projects*
- DS2 *Manage third-party services*
- DS7 *Educate and train users*
- ME2 *Monitor and evaluate internal controls*
- ME3 *Ensure regulatory compliance*
- ME4 *Provide IT governance*

1.2.3 Secondary IT processes are:

- PO7 *Manage IT human resources*
- DS10 *Manage problems*

1.2.4 The information criteria most relevant are:

- Primary: Reliability, confidentiality, compliance and efficiency
- Secondary: Effectiveness, integrity and availability

1.3 Need For Guideline

1.3.1 In many enterprises, the expectation of management, IT staff and internal audit is that IT audit and assurance professionals may be involved in non-audit activities such as:

- Defining IS strategies relating to areas such as technology, applications and resources
- Evaluation, selection and implementation of technologies
- Evaluation, selection, customisation and implementation of third-party IS applications and solutions
- Design, development and implementation of custom-built IS applications and solutions
- Establishing good practices, policies and procedures relating to various IT functions
- Design, development, testing and implementation of security and control
- Managing IT projects

1.3.2 The non-audit role, in general, involves participation in the IT initiatives and IT project teams in working and/or advisory/consultative capacities on a full-time or part-time basis. IT audit and assurance professionals may fulfil a non-audit role involved in activities such as:

- The full-time temporary assignment or loan of IT audit and assurance staff to the IS project team
- The part-time assignment of an IT audit and assurance staff member as a member of the various project structures, such as the project steering group, project working group, evaluation team, negotiation and contracting team, implementation team, quality assurance team, and trouble shooting team
- Acting as an independent advisor or reviewer on an *ad hoc* basis

1.3.3 Such non-audit roles are an important part of the IT audit and assurance professional's contribution to the education and training of other members of the enterprise. They enable IT audit and assurance professionals to use their expertise and their knowledge of the enterprise to provide a unique and valuable contribution to the efficiency and effectiveness of the enterprise's IT investments. They also provide opportunities to raise the profile of the IT audit and assurance function and to give IT audit and assurance staff valuable practical experience.

1.3.4 Where the IT audit and assurance professional has been involved in a non-audit role in an IS initiative and an audit of that initiative or the related IS function is subsequently/concurrently performed, recommendations and conclusions arising from the audit may be perceived by the recipients as not objective. In this situation, the perception may be that both the independence and the objectivity of the IT audit and assurance professional have been impaired by the non-audit involvement.

1.3.5 The IT audit and assurance professional involved in a non-audit role should evaluate whether this role generates an impairment of independence either in fact or appearance. The IT audit and assurance professional should advise and raise the awareness of the IT decision maker on what to consider when evaluating if a control is adequate. The IT audit and assurance professional performing a non-audit role should not sign off on whether a control is designed effectively.

G17 Effect of Nonaudit Role on the IT Audit and Assurance Professional's Independence cont.

1.3.6 The purpose of this guideline is to provide a framework to enable the IT audit and assurance professional to:

- Establish when the required independence may be, or may appear to be, impaired
- Consider potential alternative approaches to the audit process when the required independence is, or may appear to be, impaired
- Reduce or eliminate the impact of IT audit and assurance professionals on non-audit roles, functions and services
- Determine the disclosure requirements

2. AUDIT CHARTER

2.1 Terms of Non-audit Involvement of IT Audit and Assurance Professionals

2.1.1 The IT audit charter should establish the mandate for the IT audit and assurance professional to be involved in non-audit roles and the broad nature, timing and extent of such roles, to ensure that independence is not impaired with respect to the systems the IT audit and assurance professional may audit. This would avoid the need to obtain specific mandates on a case-by-case basis.

2.1.2 The IT audit and assurance professional should provide reasonable assurance that the terms of reference (TOR) of specific non-audit roles are in conformity with the audit charter. Where there are any deviations, the same should be expressly spelled out in the TOR.

2.1.3 Where the audit charter does not specify the non-audit roles, or where there is no audit charter, IT audit and assurance professionals should report to management and the audit committee, if one exists, the fact of their involvement in non-audit roles. The timing or extent of IT audit and assurance professionals' involvement in IS projects should be subject to individual TOR signed by the function head and approved by the audit committee.

3 TYPES OF NON-AUDIT SERVICES

3.1. Involvements That Do Not Impair Independence

3.1.1 IT audit and assurance professionals providing technical advice based on their technical knowledge and expertise such as participating in commissions, committees, task forces or panels are non-audit involvements that do not impair the IT audit and assurance professionals' independence. However, audit and assurance professionals' independence would be impaired if the extent or nature of the advice resulted in the IT audit and assurance professionals making management decisions or performing management functions.

3.1.2 Non-audit involvements that would not impair independence if supplemental countermeasures are implemented include providing advice on information technology, limited to advising on system design, system installation and system security. The enterprise's board of directors and management, should rely on the IT audit and assurance professionals' work as the primary basis for determining whether to implement a new system, the adequacy of the new system design, the adequacy of major design changes to an existing system, and the adequacy of the system to comply with regulatory or other requirements.

3.2 Involvements That Do Impair Independence

3.2.1 Non-audit roles that impair independence and objectivity include material involvement of the IT audit and assurance professional in the processes of designing, developing, testing, installing, configuring or operating the information systems as well as designing controls for information systems that are material or significant to the subject matter of the audit.

3.2.2 Non-audit roles include serving in a governance role where the IT audit and assurance professional is responsible for either independently or jointly making management decisions or approving policies and standards.

3.2.3 IT audit and assurance professional independence could be impaired when evaluation of information systems implies testing controls of the applications/systems selected by the IT audit and assurance professional while performing a non-audit role.

3.2.4 IT audit and assurance professional independence could be impaired if the extent or nature of the advice resulted in the IT audit and assurance professional making management decisions or performing management functions.

4. INDEPENDENCE

4.1 Relevance of Independence in Non-audit Roles

4.1.1 IT audit and assurance professionals should be independent in all matters related to the audit, unless prohibited by other external standards, there is no requirement for the IT audit and assurance professional either to be, or to be seen to be, independent where the nature of the involvement in the IS initiative is one of a non-audit role.

4.1.2 Although there is no need for the IT audit and assurance professional to be independent when carrying out tasks relating to a non-audit role, objectivity is still a professional requirement. The IT audit and assurance professional should carry out the tasks relating to the non-audit role in an objective and professional manner.

4.1.3 Despite there being no requirement for the IT audit and assurance professional to be independent while playing a non-audit role in an IS initiative, the IT audit and assurance professional should consider whether such a role could be deemed to impair independence if the IT audit and assurance professional is assigned to audit the IS initiative and/or the related function. Where such a conflict is foreseeable (e.g., where an independent audit will be required later and there is only one IT audit and assurance professional with the requisite skills to carry out both the non-audit role and the subsequent audit), the IT audit and assurance professional should discuss the issue with the audit committee or equivalent governance body prior to embarking on the non-audit role.

G17 Effect of Nonaudit Role on the IT Audit and Assurance Professional's Independence cont.

4.1.4 Determining the participation of the IT audit and assurance professional in a non-audit role in an IS initiative and the independent audit of the IS initiative or the related function should be the decision of the audit committee or equivalent governance body. A risk analysis should be performed. Aspects that are likely to influence the decision include:

- Potential alternative resources for either role
- The perception of relative value added by the conflicting activities
- Potential for educating the IS team so that future initiatives could benefit
- Career development opportunities and succession planning for the IT audit and assurance professional
- Level of risk attached to a non-audit role
- Effect on the visibility, profile, image, etc., of the IT audit and assurance function
- Effect of the decision on the requirements of external auditors or regulators, if any
- The provisions of the IT audit charter

4.2 Effect of Non-audit Roles on Subsequent Audits

4.2.1 When an IS initiative or function is being audited as per statutory and/or management requirements, the IT audit and assurance professional should be, and be seen to be, independent of the IS team and its management.

4.2.2 IT audit and assurance professionals should not audit their own work or provide non-audit services in situations in which the non-audit works are significant or material to the subject matter of audits in which they are involved. IT audit and assurance professionals' non-audit involvement in an IS initiative could potentially impair their independence with reference to the audit of the IS initiative and/or the related function. IT audit and assurance professionals should state whether, in their opinion, their independence while carrying out the audit is or is not impaired by their non-audit role. The audit committee or equivalent governance body should be requested to concur with the opinion in writing.

4.2.3 The critical factors that could help determine whether the IT audit and assurance professionals' independence with reference to an audit could be impaired or not by a non-audit role include aspects such as the:

- Nature, timing and extent of the non-audit role in the IS initiative, when an audit of the IT initiative and/or its related function is being considered. The greater the decision powers of the non-audit role, the higher the level of impairment to independence.
- Existence of facts that may be perceived to undermine independence. This includes aspects such as material bonus or penalty relating to the non-audit role.
- Ability as well as the commitment of the IT audit and assurance professional to remain unbiased and impartial while conducting the audit and reporting the weaknesses or errors despite the non-audit role
- Freedom of the IT audit and assurance professional to determine the scope and conduct of the audit despite involvement in a non-audit role
- Disclosure by the IT audit and assurance professional of the non-audit role, the level of involvement in that capacity and the material facts relating to it
- Existence of significant personal relationships (positive or negative) made while in the non-audit role, particularly with those in management positions
- Influence and/or persuasion of the IT audit and assurance professional in the non-audit role, regardless of the decision-making powers of the IT audit and assurance professional
- Criticality (risk rating priority) of information resources that are going to be subjects of audit and already have been subjects of the non-audit role performed by the same person

5. PLANNING

5.1 Effect on Independence

5.1.1 The potential effect of the non-audit role on independence with reference to the likely future/ concurrent audit of the same IS initiative or related function should be evaluated while planning any non-audit roles.

5.1.2 The potential effect of any previous or ongoing non-audit roles of IT audit and assurance professionals in any IS initiative on their independence should be evaluated while planning the audits of any such IT initiatives and or related functions.

5.1.3 The audit committee or equivalent governance body should be informed about the potential impairment of independence as well as any potential appearance of such impairment.

5.1.4 The IT audit and assurance professional should recommend actions or compensating controls that could be taken by the audit management/committee to provide reasonable assurance of independence and objectivity. These could include:

- Assigning additional management and/or staff from within the IT audit and assurance function who did not have any non-audit role in the area being audited, to supplement the IT audit and assurance professional who has/had a non-audit role
- Assigning management and staff from outside the IT audit and assurance function, such as borrowing staff from another function, division, external organisation, etc., to supplement the IT audit and assurance professional who has/had a non-audit role
- Assigning an independent resource, from within the IT audit and assurance function or other sources referenced previously, to carry out a peer review and to act as an independent arbiter during planning, field work and reporting

5.1.5 When the extent of IT audit and assurance professionals' involvement in the non-audit role is very strong, IT audit and assurance professionals should not recommend actions to the audit committee nor should they be directly involved in the review of the subject audit area in which they were already fully involved/participated.

6. PERFORMANCE OF AUDIT WORK

6.1. Monitoring the Conduct of Audit

6.1.1 In the case of an audit where there is potential for impaired independence due to non-audit involvement, IT audit and assurance management should closely monitor the conduct of the audit. Any material indications of the compromise of independence arising out of non-audit involvement should be evaluated critically by IT audit and assurance management and necessary corrective actions should be initiated. In such instances, the audit committee or equivalent governance body should be informed.

6.1.2 In considering whether audits performed by the IT audit and assurance professionals could be significantly or materially affected by the non-audit role, the audit committee or equivalent governance body should evaluate ongoing audits; planned audits; requirements and commitments for audits, which include laws, regulations, rules, contracts and other agreements; and policies or decisions that place responsibilities on the IT audit and assurance professionals due to their involvement in a non-audit role.

6.1.3 Governance bodies should include the allocation of audit resources to non-audit roles, so they can be made aware of potential conflicts in advance and receive assurance from audit management that such conflicts will be minimised and adequately managed.

7. REPORTING

7.1 Disclosure Requirements

7.1.1 Where the independence of IT audit and assurance management and/or staff, with reference to an audit of an IS initiative and/or the related function, could be, or could appear to be, impaired by a non-audit role in the IS initiative, the IT audit and assurance professional should disclose in the audit report sufficient information about the non-audit role as well as the actions taken to provide reasonable assurance of independence and objectivity. This will enable the users of the audit report to understand the likely extent of the impairment, if any, and the measures taken to mitigate the effects of it. Information that IT audit and assurance professionals should consider disclosing includes aspects such as:

- Names and seniority of the IT audit and assurance management and staff involved in the IT initiative in non-audit roles
- Nature, timing and extent of their non-audit involvement in the IS initiative
- Reasons for their involvement in the non-audit role in the IS initiative as well as in the audit of the IS initiative or the related function
- Steps taken to provide assurance that independence and objectivity has not been materially impaired in the course of the audit work and the reporting process
- The fact that the potential impairment of independence has been highlighted to the audit committee or equivalent governance body and their agreement obtained before undertaking the non-audit role
- Existence and extent of the review undertaken to ensure the acceptable level of reliance on the work performed

8. EFFECTIVE DATE

8.1 This guideline has been reviewed and updated, effective 1 May 2010.

G18 IT Governance

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states: "During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by the appropriate analysis and interpretation of this evidence."

1.2 Need for Guideline

1.2.1 The COBIT® *Executive Summary* states: "Organisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management must also optimise the use of available resources including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must establish an adequate system of internal control."

1.2.2 Use of technology in all aspects of economic and social endeavours has created a critical dependency on Information technology to initiate, record, move, and manage all aspects of economic transactions, information and knowledge, creating a critical place for IT governance within enterprise governance.

1.2.3 High profile problems (for example: system failures resulting from virus attacks, loss of trust or systems availability due to web site hacking) experienced by a variety of public and private sector organisations have focused attention on enterprise governance issues. The formal means by which management discharges its responsibility to establish an effective system of internal control over an organisation's operational and financial activities can be subject to public scrutiny and often forms part of the audit scope for both internal and external IS auditors.

1.2.4 The purpose of this guideline is to provide information on how an IS auditor should approach an audit of the IT governance, covering the appropriate organisational position of the IS auditor concerned, issues to consider when planning the audit, and evidence to review when performing the audit. This guideline also provides guidance on reporting lines and content and the follow-up work to be considered.

2. AUDIT CHARTER

2.1 Mandate

2.1.1 IT governance, as one of the domains of the enterprise governance, comprises the body of issues addressed in considering how IT is applied within the enterprise. IT is now intrinsic and pervasive within enterprises, rather than being a separate function marginalised from the rest of the enterprise. How IT is applied within the enterprise will have an immense effect on whether the enterprise will attain its mission, vision, or strategic goals. For this reason, an enterprise needs to evaluate its IT governance, as it is becoming an increasingly important part of the overall enterprise governance. Reporting on IT governance involves auditing at the highest level in the organisation, and may cross divisional, functional or departmental boundaries. The IS auditor should confirm that the terms of reference state the:

- Scope of work, including a clear definition of the functional areas and issues to be covered
- Reporting line to be used where IT governance issues are identified to the highest level of the organisation
- IS auditor's right of access to information

3. INDEPENDENCE

3.1 Organisational Status

3.1.1 The IS auditor should consider whether his or her organisational status is appropriate for the nature of the planned audit. Where this is not considered to be the case, the hiring of an independent third party to manage or perform this audit should be considered by the appropriate level of management.

4. PLANNING

4.1 Fact Finding

4.1.1 The IS auditor should obtain information on the IT governance structure, including the levels responsible for:

- Governing the enterprise
- Setting the enterprise strategic directions
- Assessing performance of the chief executive officer/executive management in implementing enterprise strategies
- Assessing the performance of senior management and subordinates who report on the strategies in operation (including the knowledge, information and technology involved)
- Determining whether the enterprise has developed the skills and IT infrastructure required to meet the strategic goals set for the enterprise
- Assessing the enterprise´s capability to sustain its current operations

4.1.2 The IS auditor should identify and obtain a general understanding of the processes which enable the IT governance structure to perform the functions listed in 4.1.1 including the communication channels used to set goals and objectives to lower levels (top-down) and the information used to monitor its compliance (bottom-up).

4.1.3 The IS auditor should obtain information on the organisation's information systems strategy (whether documented or not), including:

- Long and short range plans to fulfil the organisation's mission and goals
- Long and short range strategy and plans for IT and systems to support those plans
- Approach to setting IT strategy, developing plans and monitoring progress against those plans

- Approach to change control of IT strategy and plans
- IT mission statement and agreed goals and objectives for IT activities
- Assessments of existing IT activities and systems

4.2 IS Audit Objectives

4.2.1 The objectives of an audit of IT governance may be affected by the intended audience's needs and the level of dissemination intended. The IS auditor should consider the following options in establishing the overall objectives of the audit**:**

- Reporting on the system of governance and/or its effectiveness
- Inclusion or exclusion of financial information systems
- Inclusion or exclusion of nonfinancial information systems

4.2.2 The detailed objectives for an IS audit of IT governance will ordinarily depend upon the framework of internal control exercised by top-level management. In the absence of any established framework, the COBIT framework should be used as a minimum basis for setting the detailed objectives.

4.3 Scope of the Audit

4.3.1 The IS auditor should include in the scope of the audit the relevant processes for planning and organising the IT activity and the processes for monitoring that activity.

4.3.2 The scope of the audit should include control systems for the use and protection of the full range of IT resources defined in the COBIT *Framework*. These include:

- Data
- Application systems
- Technology
- Facilities
- People

4.4 Staffing

4.4.1 The IS auditor should provide reasonable assurance that the staff used to perform this review includes persons of appropriate seniority and competence.

5. PERFORMANCE OF AUDIT WORK

5.1 Review of Top-Level Management Activities

5.1.1 IT governance, as part of enterprise governance should be driven by business goals and objectives. The IS auditor should evaluate whether there is a business strategic planning process in place by considering whether:

- There is a clear definition of business vision and mission
- There is a business strategic planning methodology used
- The level of the individuals involved in this process is appropriate
- This planning is periodically updated

5.1.2 In reviewing the IT strategic planning process, the IS auditor should consider whether:

- There is a clear definition of IT mission and vision
- There is a strategic information technology planning methodology in place
- The methodology correlates business goals and objectives to IT business goals and objectives
- This planning process is periodically updated (at least once per year)
- This plan identifies major IT initiatives and resources needed
- The level of the individuals involved in this process is appropriate

5.1.3 In reviewing the IT tactical planning, the IS auditor should consider the project management practices in place, considering:

- The extent of project management methodologies used
- The project management controls applied
- The project management tools used
- The integration of IT and business staff along the various stages of the projects
- Change management methodologies used for large projects, involving significant changes in the organisations

5.1.4 In reviewing the delivery process the IS auditor should consider:

- Operational controls in place (COBIT objectives related to application development)
- The development or modification process
- The project management process (as discussed above in 5.1.3)

5.1.5 Focusing on the application development methodology and practices, and the controls applied over the development process. The IS auditor may include in the review the:

- Application development methodology (considering its quality, for example if it is highly structured and covers all aspects of the system development life cycle and take into consideration special features of the environment such as outsourcing or distributed systems)
- Development metrics used to estimate project size and its progress
- Techniques used to examine testing issues, learning from them and enhancing the methodology and controls for future projects

5.1.6 In reviewing the processes used to administer the current systems portfolio, the IS auditor should consider the coverage of organisational strategic and support areas by the current systems. The IS auditor may include in the review:

- The overall coverage of the policies issued providing the strategic areas defined by the business strategic planning process
- The process followed by top level management to elaborate, communicate, enforce and monitor the policy compliance
- Documented policies on the following that may be appropriate: security, human resources, data ownership, end-user computing, intellectual property, data retention, system acquisition and implementation, outsourcing, independent assurance, continuity planning, insurance and privacy
- The definition of roles and responsibilities of the people involved in the processes under review (for example, data owners, IT management, executive management) and assess whether they are appropriate to support the processes involved in the review
- If the people involved in the processes under review have the skills, experience and resources needed to fulfil their roles
- Whether the appropriate level of involvement of internal audit has been provided (if the organisation has internal audit resources)
- Assessing whether the position in the organisation of IT specialist staff or functions is appropriate to enable the organisation to make the best use of IT to achieve its business objectives
- Assessing whether the organisation and management of IT specialists, and non-specialists with IT responsibilities, is adequate to address the risks to the organisation of error, omissions, irregularities or illegal acts

5.1.7 The IS auditor should consider whether the audit evidence obtained from the above reviews indicates coverage of the appropriate areas. Topics which should be considered are set by COBIT in the IT Governance Management Guideline. This guideline includes the key goal indicators, critical success factors and key performance indicators that drive IT governance to its goals. Examples of the information that should be considered are:

- The existence of an IT mission statement and agreed goals and objectives for IT activities
- Assessment of risks associated with the organisation's use of IT resources, and approach to managing those risks
- IT strategy plans to implement the strategy and monitoring of progress against those plans
- IT budgets and monitoring of variances
- High level policies for IT use and protection and monitoring of compliance with those policies
- Comparison of relevant performance indicators for IT, such as benchmarks from similar organisations, functions, appropriate international standards, maturity models or recognised best practices
- Regular monitoring of performance against agreed performance indicators
- Evidence of periodic reviews of IT by the governance function with action items identified, assigned, resolved, and tracked.
- Evidence of effective and meaningful links between the process described from 5.1.1 (above) to 5.1.5

5.1.8 The IS auditor should consider whether top-level management has initiated the appropriate management activities in relation to IT, and whether these activities are being appropriately monitored.

6. REPORTING

6.1 Addressees

6.1.1 The IS auditor should address reports on IT governance to the audit committee and top-level management.

6.1.2 Where inadequacies in IT governance are identified, these should be reported immediately to the appropriate individual or group defined in the audit charter.

6.2 Contents

6.2.1 In addition to compliance with other ISACA standards on reporting, the audit report on IT governance should include, in accordance with the terms of reference:

- A statement that top-level management is responsible for the organisation's system of internal control
- A statement that a system of internal control can only provide reasonable and not absolute assurance against material
- misstatement or loss
- A description of the key procedures that top-level management has established to provide an effective IT governance system and the related supporting documentation
- Information on any noncompliance with the organisation's policies or any relevant laws and regulations or industry codes of practice for enterprise governance
- Information on any major uncontrolled risks
- Information on any ineffective or inefficient control structures or controls or procedures, together with the IS auditor's recommendations for improvement
- The IS auditor's overall conclusion on the IT governance, as defined in the terms of reference

7. FOLLOW-UP ACTIVITIES

7.1 Timeliness

7.1.1 The effects of any weaknesses in the system of enterprise governance are ordinarily wide-ranging and high-risk. The IS auditor should therefore, where appropriate, carry out sufficient, timely follow-up work to verify that management action to address weaknesses is taken promptly.

8. EFFECTIVE DATE

8.1 This guideline is effective for all information systems audits beginning on or after 1 July 2002.

G20 Reporting

1. BACKGROUND

1.1 Linkage to ISACA Standards

1.1.1. Standard S7 Reporting states 'The IS auditor should provide a report, in an appropriate form, upon the completion of the audit. The report should identify the organisation, the intended recipients and any restrictions on circulation. The report should state the scope, objectives, period of coverage, and the nature, timing and extent of the audit work performed. The report should state the findings, conclusions and recommendations and any reservations, qualifications or limitations in scope that the IS auditor has with respect to the audit'.

1.2 Definitions

1.2.1. Subject matter or area of activity is the specific information subject to the IT audit and assurance professional's report and related procedures. It can include things such as the design or operation of internal controls and compliance with privacy practices or standards or specified laws and regulations.

1.2.2. Attest reporting engagement is an engagement where an IT audit and assurance professional either examines management's assertions regarding a particular subject matter or the subject matter directly. The IT audit and assurance professional's report consists of an opinion on one of the following:

- The subject matter. These reports relate directly to the subject matter itself rather than an assertion. In certain situations management will not be able to make an assertion over the subject of the engagement. An example of this situation is when IT services are outsourced to a third party. Management will not ordinarily be able to make an assertion over the controls for which the third party is responsible. Hence, an IT audit and assurance professional would have to report directly on the subject matter rather than an assertion.
- Management's assertion about the effectiveness of the control procedures
- An examination reporting engagement, where the IT audit and assurance professional issues an opinion on a particular subject matter. These engagements can include reports on controls implemented by management and on their operating effectiveness.

This guideline is directed towards the first type of opinion. If the terms of reference require the latter types of opinion, the reporting requirements may need to be adapted.

1.2.3. Control objectives are the objectives of management that are used as the framework for developing and implementing controls (control procedures).

1.2.4 Controls or control procedures means those policies and procedures implemented to achieve a related control objective.

1.2.5. Control weakness means a deficiency in the design or operation of a control procedure. Control weaknesses potentially can result in risks relevant to the area of activity not being reduced to an acceptable level (relevant risks are those that threaten achievement of the objectives relevant to the area of activity being examined). Control weaknesses can be material when the design or operation of one or more control procedures does not reduce, to a relatively low level, the risk that misstatements caused by illegal acts or irregularities may occur and not be detected by the related control procedures.

1.2.6. Criteria are the standards and benchmarks used to measure and present the subject matter and against which the IT audit and assurance professional evaluates the subject matter. Criteria should be:

- **Objective**—Free from bias
- **Measurable**—Provide for consistent measurement
- **Complete**—Include all relevant factors to reach a conclusion
- **Relevant**—Relate to the subject matter

1.2.7. Direct reporting engagement is an engagement where management does not make a written assertion about the effectiveness of their control procedures and the IT audit and assurance professional provides an opinion, such as the effectiveness of the control procedures, about the subject matter directly.

1.2.8. Internal control structure (internal control) is the dynamic, integrated processes affected by the governing body, management and all other staff, and it is designed to provide reasonable assurance regarding the achievement of the following general objectives:

- Effectiveness, efficiency and economy of operations
- Reliability of management
- Compliance with applicable laws, regulations and internal policies

1.2.9 Management's strategies for achieving these general objectives are affected by the design and operation of the following components:

- Control environment
- Information system
- Control procedures

1.3 Need for Guideline

1.3.1 This guideline sets out how the IT audit and assurance professional should comply with ISACA IT Audit and Assurance Standards and COBIT when reporting on an enterprise's information system controls and related control objectives.

2. INTRODUCTION

2.1. Purpose of This Guideline

2.1.1 The purpose of this guideline is to provide direction to IT audit and assurance professionals engaged to report on whether control procedures for a specified area of activity are effective to either:

- An enterprise's management at the governing body and/or operational level
- A specified third party, for example a regulator or another auditor

2.1.2 The IT audit and assurance professional may be engaged to report on design effectiveness or operating effectiveness.

3. ASSURANCE

3.1 Types of Services

3.1.1 An IT audit and assurance professional may perform any of the following:

- Audit (direct or attest)
- Review (direct or attest)
- Agreed-upon procedures

3.2 Audit and Review

3.2.1 An audit provides a high, but not absolute, level of assurance about the effectiveness of control procedures. This ordinarily is expressed as reasonable assurance in recognition of the fact that absolute assurance is rarely attainable due to such factors as the need for judgement, the use of testing, the inherent limitations of internal control and because much of the evidence available to the IT audit and assurance professional is persuasive rather than conclusive in nature.

3.2.2 A review provides a moderate level of assurance about the effectiveness of control procedures. The level of assurance provided is less than that provided in an audit because the scope of the work is less extensive than that of an audit, and the nature, timing and extent of the procedures performed do not provide sufficient and appropriate audit evidence to enable the IT audit and assurance professional to express a positive opinion. The objective of a review is to enable the IT audit and assurance professional to state whether, on the basis of procedures, anything has come to the threir attention that causes the IT audit and assurance professional to believe that the control procedures were not effective based on identified criteria (expression of negative assurance).

3.2.3 Both audits and reviews of control procedures involve:

- Planning the engagement
- Evaluating the design effectiveness of control procedures
- Testing the operating effectiveness of the control procedures (the nature, timing and extent of testing will vary as between an audit and a review)
- Forming a conclusion about, and reporting on, the design and operating effectiveness of the control procedures based on the identified criteria:
  - The conclusion for an audit is expressed as a positive expression of opinion and provides a high level of assurance.
  - The conclusion for a review is expressed as a statement of negative assurance and provides only a moderate level of assurance.

3.3 Agreed-upon Procedures

3.3.1 An agreed-upon procedures engagement does not result in the expression of any assurance by the IT audit and assurance professional. The IT audit and assurance professional is engaged to carry out specific procedures to meet the information needs of those parties who have agreed to the procedures to be performed. The IT audit and assurance professional issues a report of factual findings to those parties that have agreed to the procedures. The recipients form their own conclusions from this report because the IT audit and assurance professional has not determined the nature, timing and extent of procedures to be able to express any assurance. The report is restricted to those parties (e.g.,, a regulatory body) that have agreed to the procedures to be performed, since others are not aware of the reasons for the procedures and may misinterpret the result.

3.4 Agreed-upon Procedures Reporting

3.4.1 The report on agreed-upon procedures should be in the form of procedures and findings. The report should contain the following elements:

- A title that includes the word independent
- Identification of the specified parties
- Identification of the subject matter (or the written assertion related thereto) and the type of engagement
- Identification of the responsible party
- A statement that the subject matter is the responsibility of the responsible party
- A statement that the procedures performed were those agreed to by the parties identified in the report
- A statement that the sufficiency of the procedures is solely the responsibility of the specified parties and a disclaimer of responsibility for the sufficiency of those procedures
- A list of the procedures performed (or reference thereto) and related findings
- A statement that the IT audit and assurance professional was not engaged in and did not conduct an examination of the subject matter

- A statement that if the IT audit and assurance professional had performed additional procedures, other matters might have come to the IT audit and assurance professional's attention and would have been reported
- A statement of restrictions on the use of the report because it is intended to be used solely by the specified parties

3.5 Engagement Mandate

3.5.1 Where an engagement is to be undertaken to meet a regulatory or similarly imposed requirement, it is important that the IT audit and assurance professional be satisfied that the type of engagement is clear from the relevant legislation or other source of the engagement mandate. If there is any uncertainty, it is recommended that the IT audit and assurance professional and/or appointing party communicate with the relevant regulator or other party responsible for establishing or regulating the requirement and agree with the engagement type and the assurance to be provided.

3.5.2 An IT audit and assurance professional who, before the completion of an engagement, is requested to change the engagement from an audit to a review or agreed-upon procedures engagement needs to consider the appropriateness of doing so and cannot agree to a change where there is no reasonable justification for the change. For example, a change is not appropriate to avoid a modified report.

4. IS AUDIT OPINION

4.1 Limitations

4.1.1 The IT audit and assurance professional's opinion is based on the procedures determined to be necessary for the collection of sufficient and appropriate evidence—that evidence being persuasive rather than conclusive in nature. The assurance provided by an IT audit and assurance professional on the effectiveness of internal controls is, however, restricted because of the nature of internal controls and the inherent limitations of any set of internal controls and their operations. These limitations include:

- Management's usual requirement that the cost of an internal control does not exceed the expected benefits to be derived
- Most internal controls tend to be directed at routine rather than non-routine transactions/events
- The potential for human error due to carelessness, distraction or fatigue, misunderstanding of instructions, and mistakes in judgement
- The possibility of circumvention of internal controls through the collusion of employees with one another or with parties outside the enterprise
- The possibility that a person responsible for exercising an internal control could abuse that responsibility, e.g., a member of management overriding a control procedure
- The possibility that management may not be subject to the same internal controls applicable to other personnel
- The possibility that internal controls may become inadequate due to changes in conditions and that compliance with procedures may deteriorate

4.1.2 Custom, culture and the governance of (corporate and IT) systems may inhibit irregularities by management, but they are not infallible deterrents. An effective control environment may help mitigate the probability of such irregularities. Control environment factors such as an effective governing body, audit committee and internal audit function may constrain improper conduct by management. Alternatively, an ineffective control environment may negate the effectiveness of control procedures within the internal control structure. For example, although an enterprise has adequate IT control procedures relating to compliance with environmental regulations, management may have a strong bias to suppress information about any detected breaches that would reflect adversely on the enterprise's public image. The effectiveness or relevance of internal controls might also be affected by factors such as a change in ownership or control, changes in management or other personnel, or developments in the enterprise's market or industry.

4.2 Subsequent Events

4.2.1 Events sometimes occur, subsequent to the point in time or period of time of the subject matter being tested but prior to the date of the IT audit and assurance professional's report, that have a material affect on the subject matter and that, therefore, require adjustment or disclosure in the presentation of the subject matter or assertion. These occurrences are referred to as subsequent events. In performing an attest engagement, IT audit and assurance professionals should consider information about subsequent events that come to their attention. However, IT audit and assurance professionals have no responsibility to detect subsequent events.

4.2.2 IT audit and assurance professionals should inquire of management as to whether they are aware of any subsequent events, through to the date of IT audit and assurance professional's report, that would have a material effect on the subject matter or assertion.

4.3 Conclusions and Reporting

4.3.1 The IT audit and assurance professional should conclude whether sufficient appropriate evidence has been obtained to support the conclusions in the report. In developing the report, all relevant evidence obtained should be consideered, regardless of whether it appears to corroborate or contradict the subject matter information. Where there is an opinion, it should be supported by the results of the control procedures based on the identified criteria.

4.3.2 An IT audit and assurance professional's report about the effectiveness of control procedures should include the following elements:

- Title

- Addressee
- Description of the scope of the audit, the name of the entity or component of the entity to which the subject matter relates, including:
  - Identification or description of the area of activity
  - Criteria used as a basis for the IS audit and assurance professional's conclusion
  - The point in time or period of time to which the work, evaluation or measure of the subject matter relates
  - A statement that the maintenance of an effective internal control structure, including control procedures for the area of activity, is the responsibility of management
- Where the engagement is an attest engagement, a statement identifying the source of management's representation about the effectiveness of control procedures
- A statement that the IT audit and assurance professional has conducted the engagement to express an opinion on the effectiveness of control procedures
- Identification of the purpose for which the IT audit and assurance professional's report has been prepared and of those entitled to rely on it, and a disclaimer of liability for its use for any other purpose or by any other person
- Description of the criteria or disclosure of the source of the criteria
- Statement that the audit has been conducted in accordance with ISACA IT Audit and Assurance Standards or other applicable professional standards
- Further explanatory details about the variables that affect the assurance provided and other information as appropriate
- Where appropriate, a separate report should include recommendations for corrective action and include management's response
- A paragraph stating that because of the inherent limitations of any internal control, misstatements due to errors or fraud may occur and go undetected. In addition, the paragraph should state that projections of any evaluation of internal control over financial reporting to future periods are subject to the risk that the internal control may become inadequate because of changes in conditions, or that the level of compliance with the policies or procedures may deteriorate. An audit is not designed to detect all weaknesses in control procedures as it is not performed continuously throughout the period and the tests performed on the control procedures are on a sample basis. When the IT audit and assurance professional's opinion is qualified, a paragraph describing the qualification should be included.
- An expression of opinion about whether, in all material respects, the design and operation of control procedures in relation to the area of activity were effective
- IT audit and assurance professional's signature
- IT audit and assurance professional's address
- Date of the IT audit and assurance professional's report. In most instances, the dating of the report is based upon applicable professional standards. In other instances, the date of the report should be based on the conclusion of the fieldwork

4.3.3 In a direct reporting engagement, the IT audit and assurance professional reports directly on the subject matter rather than on an assertion. The report should make reference only to the subject of the engagement and should not contain any reference to management's assertion on the subject matter.

4.3.4 Where the IT audit and assurance professional undertakes a review engagement, the report indicates that the conclusion relates to design and operating effectiveness, and that the IT audit and assurance professional's work in relation to operating effectiveness was limited primarily to inquiries, inspection, observation and minimal testing of the operation of the internal controls. The report includes a statement that an audit has not been performed, that the procedures undertaken provide less assurance than an audit and that an audit opinion is not expressed. The expression of negative assurance states that nothing has come to the IT audit and assurance professional's attention that was a cause to believe the enterprise's control procedures were, in any material respect, ineffective in relation to the area of activity, based on the identified criteria.

4.3.5 During the course of the engagement the IT audit and assurance professional may become aware of control weaknesses. The IT audit and assurance professional should report to an appropriate level of management in a timely manner any identified control weaknesses. The engagement procedures are designed to gather sufficient and appropriate evidence to form a conclusion in accordance with the terms of the engagement. In the absence of a specific requirement in the terms of engagement, the IT audit and assurance professional does not have a responsibility to design procedures to identify matters that may be appropriate to report to management.

5. EFFECTIVE DATE

5.1 This guideline is effective for all IT audits beginning on or after 16 September 2010.

G21 Enterprise Resource Planning Systems Review

1. BACKGROUND

1.1 Linkage to ISACA Standards

1.1.1 ISACA IT Audit and Assurance Standards, as well as certain IT Audit and Assurance Guidelines, have direct relevance to the IT audit and assurance professional's work on enterprise resource planning (ERP) systems or ERP system implementation projects.

1.1.2 For example, in accordance with standard S6 Performance of Audit Work supervision of the performance of ERP-related audit and assurance work by subordinate IT audit and assurance professionals or other staff for the IT audit and assurance professional must be subject to sufficient appropriate supervision by the IT audit and assurance professional.

1.1.3 Further, in those circumstances where the IT audit and assurance professional is requested or required to be involved in non-audit or non-assurance roles associated with the ERP systems or implementation project, in addition to the IT Audit and Assurance Standards and Guidelines related to S2 Independence and G12 Organisational Relationships and Independence, the IT audit and assurance professional should review and appropriately consider the applicability of the ISACA Standards for IS Control Professionals.

1.1.4 If the ERP application will be in scope, ISACA's IT Audit and Assurance Guideline G14 Application System Reviews should be reviewed.

1.1.5 If the IT audit and assurance professional is to be involved from an audit or assurance or a non-audit or non-assurance perspective in the business process re-engineering (BPR) activities associated with the implementation and use of an ERP system, ISACA's IT Audit and Assurance Guideline G26 Business Process Re-engineering should be reviewed.

1.1.6 If any component of the ERP system is outsourced to a third party, ISACA's IT Audit and Assurance Guidelines G4, Outsourcing of IS Activities to Other Organisations and G16 Effect of Third Parties on an Enterprise's IT Controls should be reviewed.

1.1.7 In addition to the pronouncements of ISACA's Professional Standards Committee, its Knowledge Board has or has had a number of projects and deliverables, which are available through the ISACA web site (*www.isaca.org*) and may be of interest to the IT audit and assurance professional, depending on the specific ERP product and other resources being used.

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.2 This guideline has been drafted to avoid limiting its application to a particular brand of ERP. It has also been drafted to cover all aspects of an ERP's use within an enterprise. Therefore, the guideline can be linked to all four COBIT domains, Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

Should a particular audit project be limited by its project charter to one aspect of a particular ERP in a particular business entity then, of course, the applicable COBIT domains and business processes would be correspondingly limited. To illustrate this, the following two examples are provided. These are not intended to be exhaustive and the particular scope of an audit might reasonably alter which processes ought to be included.

Example 1. An Audit/Review of the Planning and Acquisition of an ERP

Plan and Organise:
- PO1 *Define a strategic IT Plan*
- PO2 *Define the information architecture*
- PO3 *Determine the technological direction*
- PO4 *Define the IT processes, organisation and relationships*
- PO5 *Manage the IT investment*
- PO6 *Communicate management aims and direction*
- PO7 *Manage IT human resources*
- PO8 *Manage quality*
- PO9 *Assess and manage IT risks*
- PO10 *Manage projects*

Acquire and Implement:
- AI1 *Identify automated solutions*
- AI2 *Acquire and maintain application software*
- AI3 *Acquire and maintain technology infrastructure*
- AI4 *Enable operation and use*

Monitor and Evaluate:
- ME3 *Ensure compliance with external requirements*

Example 2. An Audit/Review of a Mature ERP System

Plan and Organise:
- PO4 *Define the IT processes, organisation and relationships*
- PO5 *Manage the IT investment*
- PO7 *Manage IT human resources*
- PO8 *Manage quality*
- PO9 *Assess and manage IT risks*

Acquire and Implement:
- AI2 *Acquire and maintain application software*
- AI3 *Acquire and maintain technology infrastructure*
- AI4 *Enable operation and use*
- A/6 *Manage changes*

Deliver and Support:
- DS1 *Define and manage service levels*
- DS2 *Manage third-party services*
- DS3 *Manage performance and capacity*
- DS4 *Ensure continuous service*
- DS5 *Ensure system security*
- DS6 *Identify and allocate costs*
- DS7 *Educate and train users*
- DS8 *Manage service desk and incidents*
- DS9 *Manage the configuration*
- DS10 *Manage problems*
- DS11 *Manage data*
- DS12 *Manage the physical environment*
- DS13 *Manage operations*

Monitor and Evaluate:
- ME1 *Monitor and evaluate IT performance*
- ME2 *Monitor and evaluate internal control*
- ME3 *Ensure compliance with external requirements*

1.3 Need for Guideline

1.3.1 ERP systems, which evolved out of manufacturing resource planning systems for the manufacturing industry, use data from a wide range of business areas to provide cross-departmental management and process information. The term 'ERP' is no longer about just planning, rather it refers to core critical business processes of an enterprise. Despite principal usefulness of the concept, ERP system implementations can fail to deliver expected results if not adequately managed and controlled. Further, there are emerging trends and changing technologies that support expanded use of ERP systems (e.g.,, web-enabled customer interfaces), which will increase the importance of the security and control consideration for ERP.

1.3.2 The audit of an ERP system requires the IT audit and assurance professional to have specific knowledge and an understanding of the complex features and integrated processes built into and required for the successful implementation, use and control of specific vendor products.

1.4 Application of Guideline

1.4.1 When applying this guideline, the IT audit and assurance professional should consider its guidance in relation to other ISACA standards and relevant guidelines. The guideline is written as generic, rather than a product-specific, guidance. The IT audit and assurance professional will need to consider and adapt the guidance depending on the ERP system and other products/procedures being used.

1.4.2 This guideline sets out information and suggests how the IT audit and assurance professional should comply with the ISACA Standards and COBIT when involved in the audit or review of an ERP system or ERP system implementation project.

2. ERP SYSTEMS

2.1 Definitions

2.1.1 ERP is used, first, to denote the planning and management of resources in an enterprise. Second, it denotes a software system that can be used to manage whole business processes, integrating purchasing, inventory, personnel, customer service, shipping, financial management and other aspects of the business. An ERP system typically is based on a common database, various integrated business process application modules and business analysis tools.

2.2 Risks and Control Challenges for Implementation of ERP Systems

2.2.1 ERP systems are implemented to support the operations of an enterprise and, to be successful, must be fully integrated into all the significant processes and procedures that together enable the enterprise to work effectively. Given the integrated nature of ERP systems, they can further add to the enterprise's risks or challenges related to:

- Industry and business environment
- User or management behaviour
- Business processes and procedures
- System functionality
- Application security
- Underlying infrastructure
- Data conversion and integrity
- Ongoing maintenance/business continuity

2.2.2 The risks associated with the implementation and ongoing use of an ERP system cannot be determined or controlled by review of application or technical risks in isolation, but must be considered in conjunction with the business process control objectives of the enterprise being served. The challenge to the IT audit and assurance professional is, therefore, obtaining an understanding of the business and regulatory environment in which the enterprise operates and being skilled in the identification of quantifiable application or technical risks and less quantifiable procedural or behavioral risks.

2.2.3 Typically, in a large enterprise where the quantity of data processed by the ERP system is extremely voluminous, the analysis of patterns and trends proves to be extremely useful in ascertaining the efficiency and effectiveness of operations. Most ERP systems provide opportunities including specific tools for such extraction and analysis. The use of data analysis tools within the ERP system can assist the IT audit and assurance professional throughout the ERP system's life cycle (i.e., pre- and post-implementation).

2.3 BPR and ERP Implementation

2.3.1 BPR and ERP implementation projects can be thought of as being independent initiatives. In theory, each project could exist within an enterprise without the other. In practice, they are often both in process at the same time in an enterprise and are influenced by and dependent on each other in a myriad of complex relationships, often including common design for key business processes. An ERP might be selected to replace an existing system, and the execution of a BPR may be delayed. A BPR might be in place but terminated prior to completion, and an included ERP implementation might continue.

2.3.2 BPR and ERP implementations are often at different stages of their development. A BPR project may be started and several months into the project when it is concluded that an ERP is required to support the new processes, an acquisition project commences. Similarly, a business decision might have been made to acquire a new IT system and choose an ERP system. During the implementation process it may be recognised that the ERP would enable a business reengineering and a BPR initiative's commencement.

2.3.3 The IT audit and assurance professional's primary focus should be with an ERP implementation. However, concurrent BPR may introduce new risks to the implementation process and often change existing risks, e.g.:

- The changes proposed by BPR may require the people affected to behave in a different manner and may engender support, concern and/or even hostility within an enterprise. This may be transferred to the ERP implementation project.
- BPR may drain enterprise resources from the ERP implementation.
- Even if the above two risks have no effect on the ERP implementation, unfamiliarity with new processes introduced by BPR might lead to inadequate process description and suboptimal configuration of the ERP system.
- BPR and ERP may not be well integrated, leaving, at best, suboptimal performance and unnecessary expenses.
- Using ERP as a 'change lever' may distract from BPR. With new, more powerful technology there is a temptation to adopt a process simply because the new technology can do it, rather than because it is the optimum business process.

2.3.4 The common steps when performing BPR, with special attention to those steps where IT can have a strong effect, are as follows:

- **Analysis phase**—The existing processes, the information and the IT systems currently in use are analysed and, the processes that need to be reengineered are identified. As the use of information and IT can be the levers for dramatic changes in the enterprise's processes, the IT audit and assurance professional can provide useful contributions in the early stages of the BPR process.
- **Redesign phase**—The new processes are redesigned, new information or new ways to use existing information are searched, and the blueprint of the new business system is defined. The to-be model of the new workflow, how the new information is to be shared across functional areas of the business and the new IT system specifications, can be areas for IT audit and assurance coverage.
- **Transformation phase**—The migration strategy is developed, and the migration action plan is created and then executed. The transformation of the IT systems, the introduction of new information and new technologies, and the discarding of old information and IT systems can be areas for IT audit and assurance coverage.

2.4 Application and Use of COBIT

2.4.1 COBIT can be applied in many ways while reviewing ERP systems. The relevance of the various control objectives will differ from enterprise to enterprise, as will the needs of the enterprise's control structures. However, a good beginning to applying COBIT during the review would be to address the management IT concerns regarding enterprise packaged solutions (refer to the ISACA publication *Implementing and Continually Improving IT Governance*). The Gartner Group has identified some specific concerns of management regarding ERP systems, including:

- Failure to meet user requirements
- Failure to integrate
- Incompatiblity with technical infrastructure
- Vendor support problems
- Expensive and complex installations

2.4.2 Relevant control objectives that have been identified by ISACA can be used to address the previously mentioned concerns. In addition, the IT audit and assurance professional also could draw up engagement-specific control objectives and engagement-specific audit and assurance procedures for these specific control objectives.

3. ACHIEVING EFFECTIVE COMPLIANCE WITH IS AUDITING STANDARDS

3.1 Introductory Comments

3.1.1 For the IT audit and assurance professional's initial exposure to, or role in, an ERP system or ERP system implementation project, ISACA's IT Audit and Assurance Standards and Guidelines are very relevant and should be considered and appropriately adhered to by the IT audit and assurance professional. The IT audit and assurance professional would be well served to complete a thorough review and analysis of these standards and guidelines within the context of the planned role or work on an ERP system and related initiatives.

3.1.2 For purposes of this guideline, only certain of the more relevant IT Audit and Assurance Guidelines are specifically referenced. ERP systems provide various opportunities for the IT audit and assurance professional andprovide risks for management that need to be addressed with care and planning. The planning stage for an ERP system or implementation review is critical to a successful audit and sign-off.

3.1.3 The audit of an ERP system or implementation calls for a strategically different approach by the IT audit and assurance professional. ERP systems integrate diversified business processes and, accordingly, may be implemented in conjunction with the conduct of a BPR project. As part of this reengineering, critical control procedures, once used to protect the finances and operations of an enterprise, may be changed or eliminated, resulting in entirely new control structures/procedures and related risks.

3.1.4 For ERP systems or implementation projects, the IT audit and assurance professional must also reengineer the way audits are performed. Risks will have undergone a transformation with regard to the intensity, diversity and the means through which they can occur. These risks arise, to some extent, due to the integrated program logic and business process functions inherent in ERP software products. Additionally, many of the legacy controls will no longer be applicable, and as such, the IT audit and assurance professional will need to identify the new control structure.

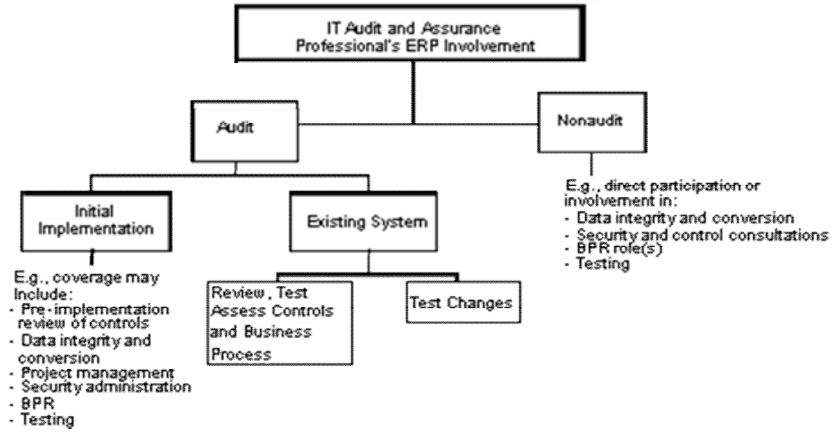
3.1.5 In planning an IT audit of an ERP system, the IT audit and assurance professional should give serious consideration to dividing the audit into sections and auditing the sections sequentially. The audit of a whole ERP system is a considerable undertaking and may strain IT or other audit and assurance resources.

3.2 Audit Charter

3.2.1 The audit charter of the IT audit function may need to be modified as a result of an enterprise's decision to implement an ERP system. For example, BPR considerations associated with effective implementation of an ERP system could require the IT audit and assurance professional's scope of work or relationships with other audit functions (e.g., financial, operational) to be expanded and more closely integrated (e.g., through a joint or collaborative audit and assurance initiative).

3.2.2 The planned scope for audit by the IT audit and assurance professional should be defined in accordance with the IT audit charter.

3.2.3 It is imperative that the enterprise's senior and system management fully understand and support the IT audit and assurance professional's role(s) as it relates to the ERP system or implementation project. The IT Audit and Assurance Guideline G5 Audit Charter, should be reviewed and considered within the context of the ERP system and related initiatives of the enterprise, as shown in the following figure.



3.3 Independence

3.3.1 If the IT audit and assurance professional is to perform or be responsible for non-audit and non-assurance roles associated with the ERP system or an ERP system implementation project, IT Audit and Assurance Guideline G17 Effect of Non-audit Role on the IT Audit and Assurance Professional's Independence should be reviewed and adhered to appropriately.

3.3.2 If the IT audit and assurance professional is to have a non-audit and non-assurance role in an ERP system or related initiatives, the IT audit and assurance professional should also review and appropriately adhere to ISACA's Standards for IS Control Professionals.

3.4 Competence

3.4.1 The IT audit and assurance professional's long-term audit and assurance strategies and plans for an enterprise using ERP systems should include aspects that will support the ongoing development and maintenance of IT audit and the IT audit and assurance professional's competence as it relates to ERP. This would include enhancements to the level of skills and knowledge and continuing professional education (S4).

3.4.2 If an IT audit and assurance professional does not have the required skills to undertake an IT audit of an ERP system or implementation project, the IT audit and assurance professional should consider contracting the audit to a qualified IT audit and assurance professional. It would be appropriate to include in the contract a requirement for knowledge transfer.

3.4.3 Skills for auditing an ERP system implementation can be acquired through ERP audit or product training on the job experience and by participating in ERP areas or audit and assurance groups.

3.4.4 Specific product-related training and experience (i.e., terminology for specific ERP products may be different or mean different things) can be acquired through hands-on use and inquiry or observation. Background interviews or briefing by IT management, technical staff and users responsible for the system can assist the IT audit and assurance professional in understanding the security, control and processing features or risks of the specific ERP system.

3.4.5 The appendix to this guideline provides further guidance on how to address competency gaps.

3.5 Planning

3.5.1 At the outset of an IT audit of an ERP system or ERP system implementation project, the IT audit and assurance professional should invest sufficient time and effort gathering background knowledge and understanding of the enterprise's existing/planned deployment and gaining control of the ERP system and related resources. The IT audit and assurance professional would achieve this through product research, direct inquiry of management and other staff, and document review procedures.

3.5.2 More specifically, the appendix provides a general overview of the elements of, and basic questions on, an ERP system implementation that the IT audit and assurance professional may need to consider.

3.5.3 Although ERP systems and implementations are likely to be more integrated and complex than other business systems that the IT audit and assurance professional may have encountered, they involve many organisational management, environmental, application, control considerations and risks similar to the more traditional systems and implementation projects.

3.5.4 It is of particular note that the areas in which an IT audit and assurance professional might be involved during the audit of an ERP project cover all aspects of an enterprise's operations. The complete audit of an ERP system will, therefore, require a broad skill set that is unlikely to be found in one person or one audit and assurance discipline. It is vitally important that the correct mix of audit and assurance skills are involved in an ERP audit or review. Audit skills and/or resources from financial, operational and regulatory areas may be needed to complement the IT audit and assurance professional's skills.

3.5.5 It is important during planning to consider which, if any, of the ERP processes are extended to the web. With many enterprises extending business over the web via enterprise portals and web-based applications on new mobile computing tools, the IT audit and assurance professional must determine if the ERP system being audited fits into this category (i.e., intranet, extranet or Internet). This will affect the performance of audit and assurance work and may extend the boundaries of the ERP system.

3.5.6 IT audit and assurance professionals should obtain reasonable assurance that management is aware of, and satisfied with, the scope of the audit and assurance work to be performed.

3.6 Performance of Work

3.6.1 The IT audit and assurance professional can use various tools and techniques to audit an ERP environment to address entire populations, flag potential risks and efficiently perform a review. Often the initial design of controls for an ERP system falters over time. Combine this with an evolving environment in which the ERP system not only interfaces to non-ERP systems, but also may serve as a web-enabled environment where the boundaries of the processes extend beyond the ERP system itself, and it becomes apparent that tools and techniques should be considered for:

- **Data mining and analysis**—ERP products ordinarily come with robust audit and assurance-related reports, and where these do not exist, third-party tools may be used to identify and analyse critical data or samples.
- **Separation of duties analysis/authorisation analysis**—Information is not restricted to disparate departmental systems, rather the integrated nature of an ERP system results in a high level of risk around security and access privileges. Business rules can be used to identify cases in which potential security concerns are flagged for review.
- **Workflow/report delivery**—Workflow within ERP systems can be utilised to deliver exception reports to key individuals for analysis and review. Given that the information is available in real time, root-cause analysis is much less complex and corrective business measures can be initiated.
- **Upgrades/control intelligence**—ERP product suppliers continue to invest in research and development leading to new or enhanced functionality, not to mention ongoing corrections to existing functionality. It is vital the enterprise, including the IT audit and assurance professional, remain current on the ERP system's latest functionality, capacity management and control capabilities. Tools exist to stay abreast on the technical control settings that are available within the ERP system, whether it is part of the original implementation or an upgrade.

3.6.2 An audit of an ERP system could provide assurance covering the area of process integrity. Specific matters to consider include the following:

- Identify control objectives for processes being implemented.
- Identify and assess potential business risks and financial risks in the processes being implemented.
- Develop and design the most effective and efficient ways of controlling these risks (which implementers generally do not focus on or do not have the expertise to develop).
- Perform an independent analysis of key business activities, comparing enterprise processes to leading practices and recommending process improvements.
- Provide assurance that the controls within ERP systems are appropriate and effective.
- Review the interfaces feeding into ERP systems from non-ERP systems (including legacy, web based and mobile computing applications).
- Perform audit and assurance tests focusing on business processes and internal controls. Many enterprises reengineer business processes during ERP implementation.
- Review business continuity plans and provide reasonable assurance that they have been tested.

3.6.3 An audit of an ERP could provide assurance covering the area of application security. Specific matters to consider include the following:

- Review standard ERP parameters, including application controls, authorisations and standard security configuration.
- Assess application security to allow processing in an efficient and controlled manner, while protecting valuable data.
- Assess configuration decisions to help provide reasonable assurance of the integrity of business processes and application security.
- Review design documentation for appropriate security and control.
- Assess the security administration process to provide reasonable assurance that the access granted is appropriately identified, evaluated and approved.
- Many business processes may be extended out over the intranet, extranet or Internet. Provide reasonable assurance that security processes appropriately address these risks.

3.6.4 An audit of an ERP system could provide assurance covering the area of infrastructure integrity. Specific matters to consider include the following:

- Identify the potential configuration and security risks for the infrastructure components (i.e., hardware, operating system, database management software, networking hardware, Internet, intranet) supporting the application software package.
- Review the ability of the enterprise's IT infrastructure to support its practices and future operational goals.
- Identify internal system architecture issues that may cause performance, availability or data integrity challenges.
- Review business recovery plans and provide reasonable assurance that they have been tested.

3.6.5 An audit of an ERP system could provide assurance covering the area of implementation integrity. Specific matters to consider include the following:

- Provide reasonable assurance of a smooth transition to the new ERP environment, with minimal effect on employees and without any loss in confidence as to the integrity, security and accuracy of data.
- Identify potential risks connected with the transfer of data from the legacy systems to the new production environment and interfaces with other systems.
- Test and assess the functionality, controls and readiness before go-live.
- Assess data quality.
- Assess data conversion and integrity strategies and control procedures.
- Assess testing plan(s) for completeness and for appropriate security and integrity.
- Confirm that testing has involved the intended user community and that the new ERP owner is satisfied that user acceptance is complete.
- Provide independent review of training for completeness of business process and security considerations.
- Provide post-implementation review of the effectiveness of the control and security environment and the overall management of the implementation process.
- Assess exception reporting.

3.6.6 The auditing of the ERP implementation can be carried out any time in the life cycle of the project by auditing what has been done until that time and what is planned for the future. Ideally the audit would involve review either on a continuous basis or at several points during the project's life cycle. To this end, the IT audit and assurance professional needs an audit and assurance framework that addresses the most critical implementation areas where often major risks are hidden, for instance:

- Project management
- Quality management
- Benefit management
- Risk management
- Change management

3.6.7 Project management consists of four phases:

- **Management planning**—When the project is initiated, a management plan is developed and proposed, the benefits are agreed to, and the project's scope and structure re defined.
- **Project implementation**—Throughout the course of the project, the key project management activities—work planning, resource management, project control, project reporting and communication—are conducted.
- **Project completion**—The project should have a predefined and easily identified end point to which the ERP system moves for live operations following the implementation phase.
- **Derivation of benefit**—After implementation, the management of the project changes in nature and transfers to the business owner who is responsibe for ensuring that the required changes to user behaviour are introduced and benefits are obtained.

3.6.8 The project management of an ERP system does not differ significantly or fundamentally from the management of any other large software project. The same concepts apply in the audit of the management of an ERP system implementation:

- Perform an assessment of executive sponsorship and top management support.
- Perform an independent review and analysis of project management activities.

- Independently assess project planning and control as well as quality assurance.
- Provide management the findings regarding resolution of project issues, including time or budget overruns, functionality gaps, and staffing and skill requirement mismatches, as well as other issues relevant to the management of the project.

3.6.9 Quality management, which should be an integral part of all software projects, should not be concerned solely with the quality of the project deliverables, but should cover all activities and deliverables of the ERP projects, such as project planning, design documentation, specifications, procedures, training materials and implementation plans. The quality assurance, which should be carried out as an independent function inside the project organisation, should not be considered an audit and assurance activity. On the other hand, during the ERP system implementation, it is essential to audit the effectiveness of the quality management and the quality assurance.

3.6.10 The business case and the associated benefit realisation plan are the key focal points for the audit of benefit management. They should identify:

- The business objectives of the project and the expected benefits to be achieved. The benefits (both quantitative and non-quantitative) should be specified clearly in a benefits register. The quantified benefits should be broken down into identifiable and measurable elements.
- The planning for the realisation of the benefits and their correlation with the change management of the business processes
- The control procedures, to provide reasonable assurance of the benefits achievement

3.6.11 A benefit management audit that is conducted before the start of the ERP system implementation has the potential to yield significant benefits for a successful ERP project. A benefit realisation review should be conducted some time after the project is completed (typically 18 months).

3.6.12 Risk management is more than just the management of project risks, it is also the management of the risks that the ERP project may place on the business. The IT audit and assurance professional should be concerned with different types of risk management:

- Risk management relevant to the business processes to be reengineered
- Risk management associated with the project management; the project risks can be either:
  - Inherent, which result from the nature of the project objectives and scope
  - Acquired, which result from the selected methodologies, tools, technique, skills and experience that are applied to the project and to risk management
- Information security management during the system implementation
- Information security management that is planned for after go-live, i.e., during the system operations
- Management of the risks introduced by systems that are external to the ERP project and the risks that the ERP project can cause to third parties. Therefore, the IT audit and assurance professional should have an enterprise approach that transcends a narrow focus on the specific ERP project.

3.6.13 Organisation realignment, communication, project marketing and personnel training are the key activities for successful project management. The IT audit and assurance professional should also evaluate, in addition to the previously mentioned activities, the correlation of change management with the other critical implementation areas, especially benefit management (with regard to the benefits to achieve) and risk management (with regard to the potential resistance to change and the information security that is associated with the authorisation of persons according to their newly defined roles). Benefits derived from an ERP implementation ordinarily require that new processes to be designed into the functionality provided by the application, prior to implementation, and that users change their behaviour to suit the newly designed processes after implementation. Audit of the derivation of business benefit, therefore, will continue after the traditional ERP project has been closed.

3.7 Reporting

3.7.1 The reporting processes for stating audit opinion and/or providing audit comment on an ERP project are not inherently different from any other audit and assurance reporting processes. Some, or all, of the following reporting mechanisms may be appropriate:

- Regular summary reports to ERP project management meetings or steering committee meetings (perhaps as agenda items)
- Maintenance of a project log, tracking audit and assurance issues for clarification or control points for resolution
- Formal reports of audit and assurance opinion and outstanding issues at defined stages in the project life cycle

4. EFFECTIVE DATE

4.1 This guideline is effective for all IT audits beginning 16 September 2010.

G21 Enterprise Resource Planning Systems Review (cont)

APPENDIX

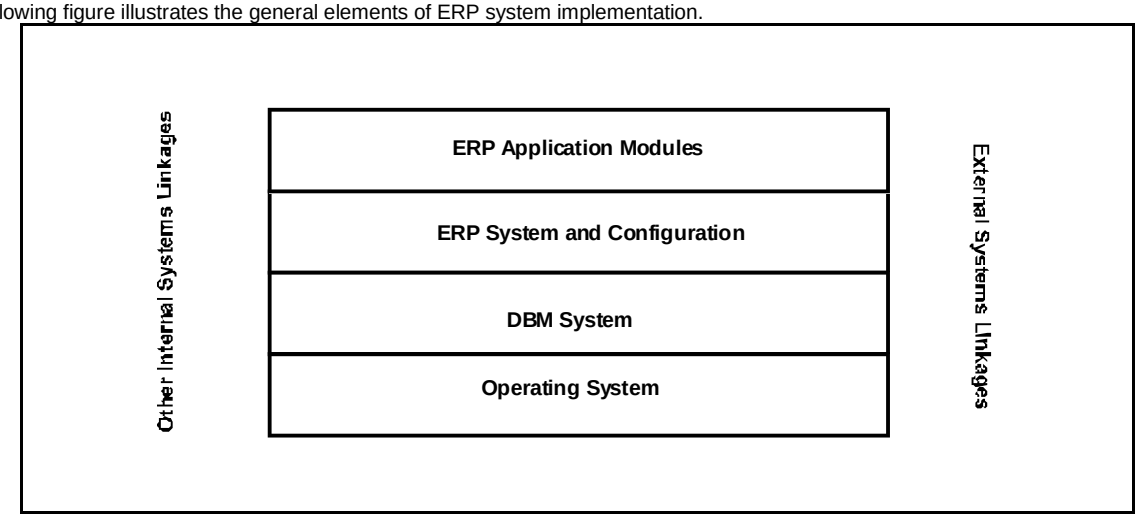
ERP Knowledge and Skill Requirements

	ERP System	Implementation Project
Background knowledge of the IT audit and assurance professional	An understanding of financial and management controls and control risks A thorough understanding of the application of professional IT audit and assurance standards A thorough understanding of IT-related controls and control risks in the following areas: • IT environment • Applications/processing An understanding of client/server architectures An understanding of operating systems and database management systems A general understanding of ERP systems and their design and deployment philosophies, including their effect on the audit trail An understanding of the ERP modules and how they are configured, integrated and deployed An understanding of security and authorisation concepts in an ERP setting	An understanding of project management practices and controls An understanding of project management practices and controls in the area of IT An understanding of IT-related systems development methodologies and standards, including change management An understanding of business process re-engineering principles and application of such
Skills of the IT audit and assurance professional	A seasoned IT audit and assurance professional who is able to focus on the key areas of control risk in an ERP setting An understanding of computer-assisted audit techniques (CAATs) and how to apply them in an ERP setting An ability to recognise where additional skills/expertise (such as financial and regulatory) are required	Experience in the review and assessment of implementation projects
How to acquire skills	Certification as a professional auditor Certification as an IT audit and assurance professional, e.g., a CISA Specialist training courses focusing on both the management and use of ERP systems as well as the audit and assurance of ERP systems ERP learning opportunities especially as part of the end-user community Practical, on-the-job experience Self study, research, Internet, etc.	Specialist training courses focusing on ERP implementation projects and the role of the IT audit and assurance professional in such projects Practical, on-the-job experience Self study, research, Internet, etc.

G21 Enterprise Resource Planning Systems Review (cont)

General Elements of and Questions on ERP System Implementation

The following figure illustrates the general elements of ERP system implementation.



- What ERP product and modules are or will be used?
  - How are or will the modules be interlinked (such as, data flow across the modules)?
- What database management product(s) are or will be used?
  - How is/will the ERP system be configured with the database management system (DBMS)?
- What operating system product(s) are or will be used?
  - How have or will each be configured/implemented and controlled?
- To what level is the ERP system web-enabled?
  - What processes are being extended to the web?
- What interfaces or linkages exist/will exist to non-ERP systems internal or external to the enterprise?
- How have or will each function be controlled?
- To what extent have or will ERP functionality and controlling roles or responsibilities be centralised or decentralised?
- How was or will data integrity be controlled and tested by management during the conversion of data from old or non-ERP systems during the ERP implementation?
- To what extent was or will business processes reengineering take place during the ERP implementation project?
  - If not, why not and when will it take place?
- If so, what changes are implemented and why?
- How do the ERP and BPR projects have agreeing, common process designs?
- What IT hardware and network resources are or will be used, and how will they be configured and managed?
- To what extent are the ERP management and technical support roles and responsibilities integrated or separated from other related IT support (such as, database administration, operations)?
- What will the controls be over the change management processes for:
  - ERP application modules
  - ERP core system
  - DBMS
- What is the operating system?
- What changes will be made to address BPR?
- Other non-ERP system linkages or interfaces
- What are or will be the access security policies and standards, and who will be responsible for ongoing management control and support?
- What processes are being adopted to provide reasonable assurance that acceptance of the ERP system and transfer of ownership to user management is complete?

G22 Business-to-consumer (B2C) E-commerce Review

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.2 Linkage to Guidelines

1.2.1 Guideline G14 Application Systems Review provides guidance.

1.2.2 Guideline G16 Effect of Third Parties on Organisation's IT Controls provides guidance.

1.2.3 Guideline G17 Effect of Nonaudit Roles on the IS Auditor's Independence provides guidance.

1.3 Linkage to COBIT

1.3.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To help meet the business-to-consumer (B2C) e-commerce review requirements of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 For B2C e-commerce and IT-based businesses, all of the IT processes relating to the COBIT domains—Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS) and Monitor and Evaluate (ME) are relevant. Primary IT processes are:

- PO1 *Define a strategic IT plan*
- PO2 *Define the information architecture*
- PO3 *Determine technological direction*
- PO9 *Assess and manage IT risks*
- AI2 *Acquire and maintain application software*
- AI3 *Acquire and maintain technology infrastructure*
- AI4 *Enable operation and use*
- AI6 *Manage changes*
- AI7 *Install and accredit solutions and changes*
- DS1 *Define and manage service levels*
- DS2 *Manage third-party services*
- DS3 *Manage performance and capacity*
- DS4 *Ensure continuous service*
- DS5 *Ensure systems security*
- ME2 *Monitor and evaluate internal control*
- ME3 *Ensure compliance with external requirements*

1.3.3 The information criteria most relevant to a B2C audit are:

- Primary: Availability, compliance, confidentiality, effectiveness and integrity
- Secondary: Efficiency and reliability

1.4 Purpose of the Guideline

1.4.1 This guideline describes the recommended practices in carrying out the review of B2C e-commerce initiatives and applications, so the relevant IS Auditing Standards are complied with during the course of the review.

2. B2C E-COMMERCE

2.1 Definition

2.1.1 The term e-commerce is used by different parties to mean different things. ISACA defines e-commerce as the processes by which organisations conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology. Therefore, it encompasses both business-to-business (B2B) and business-to-consumer (B2C) e-commerce models, but does not include existing non-Internet e-commerce methods that are based on private networks, such as EDI and SWIFTnet.

2.1.2 For the purpose of this guideline, ISACA's definition of e-commerce is used as the basis to arrive at the following definition of B2C e-commerce: B2C e-commerce refers to the processes by which organisations conduct business electronically with their customers and or public at large using the Internet as the enabling technology.

2.2 B2C E-commerce Models

2.2.1 More and more organisations are transforming their businesses using Internet technology in B2C relationships. The extent to which the Internet technology is used in an organisation for B2C relationships depends on the relative Internet maturity of the organisation, its customers, the Internet usage in its geographical market area, the nature of the organisation's products/services

and the relative urgency to which the Internet is used to either achieve competitive advantage or to catch up with the competition. Accordingly, an organisation may be resorting to a B2C e-commerce model, covering one or more of the following broad e-commerce activities:

- Informational (public)—Making information regarding the organisation and its products available on the Internet for whoever wants to access the information
- Customer self-service (informational)—Making information, such as products/services and prices, available on the Internet for the customers of the organisation
- Customer self-service (transactional other than payments)—In addition to making information available on the Internet, accepting customer transactions, such as orders and cancellations, through the Internet, but payments are handled through conventional means
- Customer self-service (payments)—Accepting customer transactions including payments or fund transfers (in the case of banks) through the Internet
- Customer reporting—Providing reports, such as statement of accounts and order status to customers online
- Interactive self-service—Providing interactive responses through e-mails for requests/queries logged through a web site
- Direct selling—Selling products and services directly to prospective buyers through the Internet
- Auctioning—Auctioning the products online

2.3 Special Focus Required in a B2C E-commerce Review

2.3.1 In the case of B2C e-commerce initiatives, the business and the information systems are coupled tightly. Therefore, a review of B2C e-commerce should, in general, address the business risks as well as the IS risks.

2.3.2 COBIT has laid down seven information criteria to be met by information systems. Better compliance with these help to mitigate the IS risks and contribute towards minimising business risks. These are:

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

The relevance of these may be greater in the case of B2C e-commerce, depending on the extent of the broad e-commerce activities (as specified in section 2.2.1) carried out by the organisation. Accordingly, a review of B2C e-commerce should address how COBIT's information criteria are met by the B2C e-commerce application and how the related risks are mitigated.

2.3.3 Being connected to the Internet, B2C e-commerce applications are faced with inherent external threats, such as hackers, viruses and impersonation, which could affect the confidentiality, integrity and availability of the B2C e-commerce application. If the B2C e-commerce application is integrated with back-end systems, there is risk of even those systems becoming affected. In the event of the organisation's B2C e-commerce application being affected by such attacks, the reputation and image of the organisation could be seriously impaired. In this context, the B2C e-commerce reviews should pay significant attention to the adequacy of the protection against such threats.

2.3.4 Non-repudiation of the transaction is an essential requirement of B2C e-commerce. With reference to COBIT's seven information criteria, one of the criteria is integrity. In cases where B2C e-commerce involves transactions and/or payments, authenticity of source and integrity during communication need to be ensured, so there is no subsequent repudiation of the transaction. The review of B2C e-commerce, in such cases, should address the effectiveness of the B2C e-commerce application in ensuring non-repudiation.

2.3.5 B2C e-commerce, in general, involves obtaining details about the customers and prospects using and or transacting through the B2C e-commerce applications. The data protection of such details should be ensured. In other words, the details gathered should be used for the intended purposes only and as per the agreement with the persons providing the information. There are various legal provisions evolving in various countries. In this context, any review of B2C e-commerce should address compliance with the legal provisions of the relevant countries as well as best practices relating to privacy and data protection.

2.3.6 Application audit trails have more significance in the B2C e-commerce environment due to the absence of paper trails for transactions and payments. In this context, the review of B2C e-commerce should address the adequacy of audit trails as well as the processes for reviewing the audit trails. This is important from the point of confirming the authenticity and integrity (including non-repudiation) of the transactions.

2.3.7 As against other channels of business, B2C e-commerce depends largely on the availability of the application and access to the Internet. In this context, there should be appropriate capacity planning processes, redundancies and fallback options as well as disaster recovery procedures in place for both the system and communication link. These should be given due attention while evaluating the availability aspects of the B2C e-commerce application.

2.3.8 Integrity of data between the B2C e-commerce application and the related back-end applications and processes (including manual processes, such as delivery/dispatch and receipt of non-electronic payments) is an important aspect. The adequacy of the automated application and manual controls to ensure such integrity should be an essential part of a B2C e-commerce review.

2.3.9 Where B2C e-commerce involves receiving online payments, there should be appropriate processes to obtain authorisations for the payments and to ensure that the considerations are duly received. In such cases, the appropriateness and adequacy of the controls need to be evaluated as part of the B2C e-commerce review.

2.3.10 Quite often, B2C e-commerce involves use of third-party service providers for various aspects, such as application development and maintenance, and managing the web site and related databases. In such cases, the appropriateness and adequacy of the controls and contractual protection, which ensure appropriate levels of service and the protection of the information relating to the organisation and its customers, needs to be evaluated as part of the B2C e-commerce review.

2.3.11 Data handling, storage, retention and disposal arising from B2C e-commerce activities become a greater concern as most, if not all, data originates and terminates electronically.

2.3.12 Some B2C e-commerce involve use of credit cards and other forms of payment and may be subject to standards set by those providers and processors. Awareness and adherence to those standards is important when enabling B2C e-commerce.

3. CHARTER

3.1 Mandate

3.1.1 Before commencing a review of B2C e-commerce, the IS auditor should provide reasonable assurance of the requisite mandate, by virtue of the IS auditor's position or the required written mandate provided by the organisation, to carry out the envisaged review. In case the review is initiated by the organisation, the IS auditor should also obtain reasonable assurance that the organisation has the appropriate authority to commission the review.

4. INDEPENDENCE

4.1 Professional Objectivity

4.1.1 Before accepting the assignment, the IS auditor should provide reasonable assurance that the IS auditor's interests, if any, in the B2C e-commerce application being reviewed would not in any manner impair the objectivity of the review. In the event of any possible conflict of interests, the same should be communicated explicitly to the organisation, and a written statement of the organisation's awareness of the conflict should be obtained before accepting the assignment.

4.1.2 In case the IS auditor has/had any non-audit roles in the B2C e-commerce application being reviewed, the IS auditor should consider the guideline G17 Effect of Non-audit Roles on the IS Auditor's Independence.

5. COMPETENCE

5.1 Skills and Knowledge

5.1.1 The IS auditor should provide reasonable assurance of the necessary business knowledge to review the B2C e-commerce application. Understanding the business catered to by the B2C e-commerce application is important for evaluating the B2C e-commerce applications/initiatives.

5.1.2 The IS auditor should also provide reasonable assurance of access to the relevant technical skill and knowledge to carry out the review of a B2C e-commerce application. Such reviews would call for technical knowledge to evaluate aspects, including the encryption technologies used, network security architecture and security technologies, such as firewalls, intrusion detection and virus protection. The IS auditor should have adequate knowledge to review these aspects. Where expert inputs are necessary, appropriate inputs should be obtained from external professional resources. The fact that external expert resources would be used should be communicated to the organisation in writing.

6. PLANNING

6.1 High-level Risk Assessment

6.1.1 The IS auditor should gather information regarding the industry in general (since the B2C e-commerce risks would vary from industry to industry), the organisation's B2C e-commerce objectives and policies, its strategy to achieve the objectives, the business processes involved and the underlying flow of information, the scope of the B2C e-commerce system, the extent of usage of the system, and the development process used for building the B2C e-commerce solution. The information gathered should help in carrying out a high-level assessment of the business risks as well as the risks with reference to COBIT's information criteria and the aspects referenced in section 2.3 of this document. This high-level risk assessment will help determine the scope and coverage of the review.

6.2 Scope and Objectives of the Review

6.2.1 The IS auditor, in consultation with the organisation, where appropriate, should define clearly the scope and objectives of the review of the B2C e-commerce. The aspects to be covered by the review should be stated explicitly as part of the scope. The high-level risk assessment referred to in section 6.1.1 would dictate which aspects need to be reviewed and the extent and depth of the review.

6.2.2 For the purpose of the review, the stakeholders in the B2C e-commerce solution should also be identified and agreed upon with the organisation.

6.3 Approach

6.3.1 The IS auditor should formulate the approach, so the scope and objectives of the review can be fulfilled in an objective and professional manner. The approach followed should depend on whether the review is a pre- or a post-implementation review. The approach should be documented appropriately. When and where external expert inputs would be used should also be specified as part of the approach.

6.4 Sign-off for the Plan

6.4.1 Depending on the organisational practices, the IS auditor may obtain the concurrence of the organisation for the plan and approach.

7. PERFORMANCE OF THE B2C E-COMMERCE REVIEW

7.1 General

7.1.1 This section addresses the wide spectrum of aspects to be addressed during the execution of a B2C e-commerce review. For a specific B2C e-commerce review, aspects relevant to the review should be identified from this wide spectrum of aspects depending on the envisaged scope and objectives of the review.

7.1.2 The B2C e-commerce review should be carried out per the defined approach (with refinements as appropriate), so the envisaged objectives of the review are fulfilled.

7.1.3 In general, study of available documentation (i.e., business case, system documentation, contracts, service level agreements, logs), discussions with the stakeholders, use of the B2C e-commerce application and observation should be used appropriately to gather, analyse and interpret the data. Where appropriate, the IS auditor should test the significant processes in the test and/or production environment to verify that the processes are functioning as intended (i.e., test purchases or test ordering using the e-commerce system and test the security mechanisms using penetration testing).

7.1.4 Where necessary and agreed upon with the organisation, external expert inputs could be used suitably in the collection, analysis and interpretation of the data.

7.1.5 The inferences and recommendations should be based on an objective analysis and interpretation of the data.

7.1.6 Appropriate audit trails should be maintained for the data gathered, analysis made, inferences arrived at and corrective actions recommended.

7.2 Evaluating the Business Aspects

7.2.1 The IS auditor should evaluate the e-commerce objectives, strategy and business model critically. The existing and emerging competition should also be considered in evaluating the relative position of the organisation's business. This is essential for evaluating the appropriateness of the objectives and strategies and the effectiveness and efficiency of the B2C e-commerce application in fulfilling these objectives and strategies.

7.2.2 The IS auditor should evaluate whether the B2C e-commerce initiative is a new business by itself, or an additional channel to the existing line of business, and to what extent the success and financial viability of the organisation depends on the B2C e-commerce initiative being reviewed. The greater the dependency on the B2C e-commerce, the higher the effects of the risks should they materialise.

7.2.3 The IS auditor should review the business case to assess whether the costs and benefits of the B2C e-commerce are reflected in an objective manner. Considering the huge and ever-increasing number of Internet users, at times the business potential and volume are projected at levels way beyond what could be achieved pragmatically. If the IS auditor has concerns regarding the underlying assumptions, the same should be clarified with appropriate management.

7.3 Detailed Risk Assessment

7.3.1 The IS auditor should map the key processes relating to the B2C e-commerce application—automated as well as manual processes—in case these are not readily available.

7.3.2 The IS auditor should then assess the likely risks—business and IS risks—pertaining to these processes and their likely effect, and document these along with the aspects that mitigate/could mitigate the risks. The criticality of the residual risk should also be assessed.

7.3.3 Depending on the criticality of the risks, the IS auditor should determine aspects that need to be reviewed further and the depth of the review.

7.3.4 The IS auditor should identify applicable controls to mitigate risks identified. If multiple controls can be identified to mitigate risk, controls can be ranked in order of effectiveness. Primary or 'key' controls should be tested before secondary controls.

7.4 Development Process

7.4.1 The IS auditor should review the appropriateness of the development process followed to determine whether appropriate controls were built into the B2C e-commerce application.

7.4.2 The capabilities of the team developing/maintaining the B2C e-commerce application and the tools being used should be reviewed to assess their adequacy and to verify appropriate controls in the B2C e-commerce application.

7.4.3 In this context, the IS auditor should consider the guideline G23 System Development Life Cycle Reviews to the extent it is appropriate for the review being carried out.

7.5 Change Management Process

7.5.1 Uncontrolled changes to the B2C e-commerce applications could result in unplanned outages and could affect the integrity of data and processing. In this context, the IS auditor should review the appropriateness of the change management process to evaluate its adequacy in ensuring controlled changes to the B2C e-commerce application environment. As part of testing the change management process, the IS auditor should review an adequate number of changes, to verify that the processes are functioning as intended. Adequacy is based on population of changes made within the period and complexity of the change.

7.5.2 The IS auditor should ascertain whether the development, testing, staging and production environments are segregated adequately to minimise the risks arising out of changes. The effects of any inadequacies in this aspect need to be evaluated.

7.6 Content Management Process

7.6.1 The contents appearing in B2C e-commerce web sites—those merely providing information as well as those relating to transactions—should be published through a controlled content management process to ensure appropriateness of language and presentation, correctness of information, and appropriate approvals for the data published, particularly those relating to product and service offering, pricing, contractual obligations, legal terms and conditions, etc.. The IS auditor should understand this process and review its adequacy.

7.6.2 The IS auditor should verify whether adequate audit trails relating to the key contents (i.e., terms, conditions and prices) are maintained and reviewed to verify the integrity and accuracy of the data.

7.6.3 The IS auditor should verify whether the terms and conditions of use of the B2C e-commerce application, as well as the privacy and data protection policies of the organisation, as published on the site, have been vetted by legal experts to confirm that adequate attention has gone into legal compliance and contractual protection.

7.7 Identification and Authentication

7.7.1 Depending on the e-commerce activities permitted by the B2C e-commerce application—particularly where transactions and payments are processed—the user should be identified and authenticated uniquely to ensure non-repudiation and to preserve confidentiality. The IS auditor should evaluate whether the controls/mechanisms/technologies (such as ID and passwords, challenge/response procedure, tokens, digital certificates and digital signatures), deployed regarding identification and authentication, are commensurate with the intended use of the B2C e-commerce application.

7.8 Data Validations and Authorisations

7.8.1 If the B2C e-commerce application accepts data from the users by way of transactions and/or information, the IS auditor should verify whether adequate validations built into the application ensure the appropriateness of the data being entered and that such validations are being performed.

7.8.2 If the B2C e-commerce application accepts electronic payments (such as credit cards), the IS auditor should verify whether there are adequate validation and payment authorisation processes to ensure the authenticity as well as the actual receipt of the payments.

7.9 Communication Controls

7.9.1 In the case of B2C e-commerce applications processing transactions and payments as well as accepting and/or displaying any personal details confidential in nature (such as statement of accounts), the IS auditor should verify whether an appropriate encryption technology/mechanism (such as Secure Socket Layer or IPSec) is being used to encrypt the transmission between the user and the application.

7.9.2 Where appropriate and necessary, the IS auditor should ascertain whether the communication across the network is made secure using a virtual private network (VPN) and related encryption.

7.10 Processing Controls

7.10.1 In the case of B2C e-commerce applications processing transactions and payments, the IS auditor should verify whether there are adequate application controls to ensure the integrity and correctness of the processing.

7.11 Integration With Back-end Processes and Applications

7.11.1 Some of the B2C e-commerce applications require back-end processes for fulfillment of orders, receipt of money and accounting for transactions. While some of this may be handled through detached applications or manual processes, they may call for integration of the B2C e-commerce application with some of the other applications. In such instances, the IS auditor should verify whether there are sufficient controls, including reconciliation processes to ensure integrity of original data across the related applications and processes (including manual processes).

7.12 Data Storage Integrity

7.12.1 Behind any B2C e-commerce application is a database, the integrity and confidentiality of which is crucial. The IS auditor should evaluate the controls over the database to confirm that there are adequate checks and balances to prevent intentional or inadvertent damage, destruction or modification of data. In this context, the IS auditor should review the database access privileges and the access logs.

7.12.2 The IS auditor should also review the controls over the archived data to provide reasonable assurance that the confidentiality and integrity are protected adequately.

7.13 Audit Trails and Their Review

7.13.1 As indicated previously, in the absence of paper trails, the role of automated audit trails is critical in B2C e-commerce applications. The IS auditor should review the adequacy of the audit trails relating to transactions, including payments, changes to critical master data (such as rates, prices and actions) and any changes carried out by staff with system administration privilege.

7.13.2 Mere availability of audit trails would not suffice. There should be processes for reviewing the audit trails to provide reasonable assurance that the actions, as reflected in the audit trails, are valid and duly authorised. In this context, the IS auditor should look for audit evidence that the audit trails are being reviewed and acted upon.

7.14 Protection Against External IS Threats

7.14.1 The IS auditor should evaluate the external IS threats to the B2C e-commerce environment, taking into account the nature of the business of the organisation. The external threats to be addressed should include denial of service, unauthorised access to data and unauthorised use of the computer equipment. These could arise from various sources (such as casual hackers, competitors, alien governments and terrorists). The characteristics of the business of the organisation (such as intensity of competition, market share, nature, timing and extent of technology usage, and innovative/strategic products and/or services) should be used to determine the possible sources of such threats. The likely damage associated with these threats is linked closely to the dependence of the business on the e-commerce processes.

7.14.2 The IS auditor should assess whether the protective measures in place to counter the external threats are commensurate with the level of the assessed risk. In this process, the IS auditor should review the following:

- Technical architecture of the application, including the choice of protocols
- Security architecture of the application
- Virus protection mechanisms

- Firewall implementation, appropriateness of the firewall solution, location of firewall, firewall policies, connections to the firewall and any external connections bypassing the firewall
- Intrusion detection and prevention mechanisms
- Existence of relevant logs as well as their ongoing review by competent staff
- Processes in place, such as penetration and vulnerability testing, to verify the compliance with the envisaged architectures, policies and procedures.

7.15 Compliance With Regulations and Best Practices

7.15.1 The IS auditor should evaluate whether the relevant privacy and data protection requirements imposed by the relevant laws and best practices relating to privacy and data protection are being complied with by the organisation. As indicated previously, the IS auditor should verify whether the privacy and data protection policies and practices are displayed appropriately on the web site.

7.15.2 The IS auditor should evaluate whether the B2C e-commerce activity is subject to other governmental laws and regulations and identify processes and controls to ensure compliance. Appropriate measures should be taken to verify adherence to local and other applicable laws depending on jurisdiction, such as those related to anti-money laundering, taxation and industry regulations/standards such as PCI. The IS auditor should also evaluate whether goods and services sold via B2C activity violate export law. Encryption technology or weapons are examples of goods that may trigger export restrictions.

7.16 Availability of the B2C E-commerce Application and Business Continuity

7.16.1 Since B2C e-commerce depends largely on the availability of the application and access to the Internet, the IS auditor should evaluate whether there are appropriate capacity planning processes, redundancies and fallback options, offsite storage, rotation of media, and disaster recovery procedures in place for both the system and communication link.

7.16.2 Where relevant, the IS auditor should also review the fallback arrangements with reference to automated and other related manual processes to ascertain their appropriateness in ensuring business continuity and fast recovery in the event of any disruptions.

7.17 Effectiveness and Efficiency

7.17.1 The IS auditor should evaluate the effectiveness of the B2C e-commerce application with reference to the intended objectives of the initiative. Certain aspects, such as volume of transactions, value of business, number of customers/prospects/visitors attracted, volume and value of repeat business, and attrition of customers, would help in assessing the effectiveness of the system.

7.17.2 The IS auditor should compare, where relevant, the actual costs and benefits against what was envisaged, to assess whether the B2C e-commerce application is sufficiently cost-efficient. The processing performance, customer feedback and ease of use of the application (as indicated by the use of the system) also help in assessing the efficiency of the B2C e-commerce application.

7.17.3 The IS auditor should ascertain whether there are appropriate mechanisms to monitor the effectiveness and efficiency of B2C e-commerce on an ongoing basis. This should include the processes to detect and report exceptions so as to prevent errors and frauds.

7.18 Third-party Services

7.18.1 Where the B2C e-commerce solution depends on any third-party service providers, such as an Internet service provider (ISP), certificate authority (CA), registration authority (RA) and web-hosting agency, the IS auditor should ascertain whether the security procedures at their ends are appropriate and adequate.

7.18.2 Where such third-party service providers are used, the IS auditor should review the related contracts and service level agreements (SLAs) as well as the SLA reporting, to assess whether the interests of the organisation are being protected adequately.

7.18.3 In this context, the IS auditor should consider whether the guideline G16 Effect of Third Parties on Organisation's IT Controls provides the appropriate guidance.

7.18.4 When third parties are used for certification in B2C, the IS auditor should provide due diligence in reviewing how the information is collected and used for those seals of control (e.g., BetterBusiness, Webtrust).

7.19 Nonrepudiation

7.19.1 Where the B2C e-commerce solution involves processing of transactions and payments, the IS auditor should evaluate the relevant controls referred to previously (sections 7.7, 7.9 and 7.10) with reference to authentication, communication, processing, and ensuring non-repudiation.

8. REPORTING

8.1 Report Content

8.1.1 The report on the B2C e-commerce review should address the following aspects depending on the scope of its coverage:

- The scope, objective, methodology followed and assumptions
- Overall assessment of the solution in terms of key strengths and weaknesses as well as the likely effects of the weaknesses
- Recommendations to overcome the weaknesses and improve the solution
- The extent of compliance with COBIT's information criteria and criteria specific to B2C e-commerce (such as non-repudiation) and the effect of any noncompliance
- Recommendations regarding how the experience could be used to improve similar future solutions or initiatives

8.1.2 The observations and recommendations should be validated with the stakeholders and organisation, as appropriate, before finalising the report.

9. EFFECTIVE DATE

9.1 This guideline is effective for all IS audits beginning on or after 1 August 2003. The guideline has been reviewed and updated effective 1 December 2008.

APPENDIX

References

- ISACA, E-commerce Security Series publications, 2000-2002
- Australian Accounting Research Foundation, Auditing Guidance Statement AGS1056 E-commerce: Audit Risk Assessments and Control Considerations

G23 System Development Life Cycle (SDLC) Reviews

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, "During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

1.1.2 Guideline G14 Application Systems Review provides guidance.

1.1.3 Guideline G17 Effect of Nonaudit Roles on the IS Auditor's Independence provides guidance.

1.1.4 Guideline G20 Reporting provides guidance.

1.2 Linkage to COBIT®

1.2.1 The COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."

1.2.2 The COBIT *Management Guidelines* provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 The *Management Guidelines* provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

1.2.4 The *Management Guidelines* can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.

1.2.6 Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

1.3 Need for Guideline

1.3.1 To support the business operations, organisations implement application systems. The process of defining, acquiring and implementing application systems involves various stages from identifying requirements to actually implementing the application system and generally is referred to as a system development life cycle (SDLC).

1.3.2 This guideline is meant to provide the necessary guidance to IS auditors in carrying out reviews of the SDLC of application systems.

2. SYSTEMS DEVELOPMENT LIFE CYCLE

2.1 Definition

2.1.1 The system development life cycle is the process, involving multiple stages (from establishing the feasibility to carrying out post implementation reviews), used to convert a management need into an application system, which is custom-developed or purchased or is a combination of both.

2.2 Factors Influencing the SDLC

2.2.1 The SDLC for an application system would depend on the chosen acquisition/development mode. Application systems could be acquired/developed through various modes, which include:

- Custom development using internal resources
- Custom development using fully or partly outsourced resources located onsite or offsite (locally or in an offshore location)
- Vendor software packages implemented as-is with no customisation
- Vendor software packages customised to meet the specific requirements

At times, large complex applications may involve a combination of the above.

2.2.2 Some organisations use specific SDLC methodologies and processes, either custom- or vendor-developed. These generally prescribe standard processes for different modes of acquisition with the facility to customise the process design for specific application systems. These may be supported by appropriate tools to manage the SDLC. In such cases, the SDLC would depend on the methodology/tool.

2.2.3 Where an application system is developed instead of being purchased as a package, the SDLC would depend on the development methodology used, such as waterfall development, prototyping, rapid application development, CASE and object-oriented development.

2.3 SDLC Risks

2.3.1 During the SDLC of an application system, various risks could be encountered, which include:

- Adoption of inappropriate SDLC for the application system
- Inadequate controls in the SDLC process
- User requirements and objectives not being met by the application system
- Inadequate stakeholder (including internal audit) involvement
- Lack of management support
- Inadequate project management
- Inappropriate technology and architecture
- Scope variations
- Time over-runs
- Cost over-runs
- Inadequate quality of the application system
- Insufficient attention to security and controls (including validations and audit trails) in the application system
- Performance criteria not being met
- Inappropriate resourcing/staffing model management
- Inadequate staffing skills
- Insufficient documentation
- Inadequate contractual protection
- Inadequate adherence to chosen SDLC and/or development methodologies
- Insufficient attention to interdependencies on other applications and processes
- Inadequate configuration management
- Insufficient planning for data conversion/migration and cutover
- Post cut-over disruption to business

3. PLANNING

3.1 Factors to be Considered in Planning

3.1.1 The IS auditor should consider the following while planning the review of the SDLC of an application system:

- The acquisition/development mode, technology, size, objectives and intended usage of the application system
- Project structure for the acquisition and implementation
- Skill and experience profile of the project team
- The SDLC model chosen
- The formal SDLC methodology and customised process design adopted, if any
- Risks that are likely to effect the SDLC
- Any concerns or issues perceived by appropriate management
- The current SDLC stage
- Any prior review of the earlier SDLC stages of the application system
- Any prior SDLC reviews of similar application systems
- Any other risk assessments/reviews by the IS auditor or others (such as IT) that have a bearing on the proposed review
- The skill and experience level of the IS auditors available and the possibility of getting competent external assistance where necessary

3.2 Terms of Reference

3.2.1 Taking the above into account, the IS auditor should arrive at the terms of reference (TOR) of the planned SDLC review. This should include:

- The objectives of the review
- Scope of the review in terms of SDLC stages to be covered by the review
- Type of review –whether it is a pre-implementation review of the proposed SDLC, a parallel/concurrent review as the SDLC stages are being executed, or a post-implementation review after the SDLC stages in question are completed
- The timeframe of the review—likely start and end dates
- Process for reporting the observations and recommendations
- Process for following up on the agreed actions

3.2.2 The IS auditor should obtain the agreement of the appropriate management for the proposed review of the SDLC of the chosen application system.

4. COMPETENCE

4.1 Skills and Experience

4.1.1 The IS auditors assigned to the SDLC review should have the requisite skills and experience to carry out the review cost-effectively and efficiently. Where specific SDLC methodologies and tools are used, the IS auditors should possess adequate knowledge and experience regarding such methodologies and tools and the associated risks. Similarly, where the application system is being developed instead of being purchased from a vendor, the IS auditor should possess sufficient knowledge and experience regarding the development methodologies and tools being used (such as waterfall development, prototyping, rapid application development, CASE and object-oriented development). If warranted, the IS auditor should seek external resources (subject to applicable policies, procedures and approvals) to complement the internal skill availability.

5. INDEPENDENCE

5.1 Independence

5.1.1 When reviewing the SDLC of application systems, the IS auditor should be, and be seen to be, independent of the project team responsible for acquiring and implementing the application system. Guideline G17, which provides guidance regarding the Effect of Nonaudit Roles on the IS Auditor's Independence, should be considered in this context.

6. PERFORMANCE OF REVIEW WORK

6.1 Types of Reviews

6.1.1 The IS auditor should carry out the review or audit of the SDLC as per the TOR agreed upon with the appropriate management:

- Where the review is a pre-implementation review, the IS auditor should study the proposed SDLC model and the related aspects to assess their appropriateness as well as the potential risks and provide the necessary risk mitigation recommendations to the appropriate management.
- In the case of parallel/concurrent reviews, the IS auditor should review the relevant SDLC stages, as they are happening, to highlight risks/issues and provide necessary risk mitigation recommendations to the appropriate management.
- In the case of post-implementation reviews, the IS auditor should review the relevant SDLC stages after their completion to highlight issues faced and provide recommendations for downstream corrections (if possible) and to serve as a learning tool for the future.

6.2 Aspects to be Reviewed

6.2.1 The IS auditor should study and evaluate the following during the course of the review to assess the risks/issues and their effects. While some of these are relevant for all the SDLC reviews, irrespective of the type of review (pre-implementation, parallel/concurrent or post-implementation), some are relevant for specific types of review alone. The IS auditor should study and evaluate those aspects that are relevant for the objectives and scope of the proposed review, so as to arrive at the appropriate assessment of the risks and issues as well as the recommendations to mitigate their effects, such as:

- Project charter (including the project plan, deliverables and their schedules) and business case (highlighting costs and benefits) for the application system
- Project structure including any working groups, steering groups, and the related roles and responsibilities
- The formal project management methodology adopted, if any (such as PRINCE 2), and the related process of creating the customised design of processes
- The development or application development methodology, such as waterfall development, prototyping, rapid application development, CASE, and object-oriented development, and the associated tools chosen for the application system
- Contracts with suppliers for purchased application systems
- Contracts with suppliers for outsourced services, such as customisation and/or development
- Control processes within the SDLC model—particularly reviews, validations, approvals and sign-offs for the SDLC stages under review
- Structure of the deliverables for the SDLC stages under review
- Minutes of relevant meetings, such as working group and steering group meetings
- Actual deliverables, as well as the audit trails of their reviews and sign-off
- Project reporting, progress tracking (efforts, time and cost) and escalation
- Resource management
- Ongoing risk management
- Quality management/assurance
- Change management
- Performance and problem management including service level agreements (SLAs)
-

- Configuration management
- Data conversion/migration
- Documentation relating to in-project reviews including testing
- In-project and supplier communications
- Reviews, if any, of earlier SDLC stages of the application system
- Earlier SDLC reviews, if any, of similar applications
- Relevant legal, regulatory and policy aspects to be complied with, if any

6.2.2 COBIT defines the high-level control objectives with reference to acquisition of application systems, which includes areas such as Identify Automated Solutions (AI1) and Acquire and Maintain Application Software (AI2). Similarly, there are high-level control objectives regarding Manage Projects (PO10), Manage Quality (PO11) and Ensure System Security (DS5). Within COBIT, these are further expanded into detailed control objectives. As part of the review, the IS auditor should evaluate the extent to which these control objectives (relevant to the SDLC stages under review) are met and the effectiveness of the mechanisms and procedures employed to achieve such objectives.

6.2.3 COBIT also defines seven information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability) to be met by application systems. As part of the review of the SDLC of an application system, the IS auditor also should evaluate how effectively the SDLC processes/stages under review contribute towards the adequate fulfilment of these criteria. Actual evaluation of the compliance of the application system with these criteria would be part of the application system review (refer to guideline G14 Application Systems Review).

7. REPORTING

7.1 IS Auditor's Report

7.1.1 For SDLC reviews of application systems, often, reporting could be performed progressively, as and when risks and issues are identified. These reports should be addressed to the appropriate management for necessary action. A final report listing all issues raised during the review can be issued.

7.1.2 Depending on the type of review, the report should address aspects, such as:

- Appropriateness of the SDLC model and development methodology
- Risks and issues; their causes and effects
- Possible risk mitigation actions within the SDLC stage—under review or in downstream stages. For instance, some of the issues faced during the design stage would call for risk mitigation actions during subsequent stages, such as development and testing.

8. FOLLOW-UP

8.1 Timely Follow-up

8.1.1 For SDLC reviews of application systems, particularly, the pre-implementation and parallel/concurrent reviews, there should be an appropriate follow-up to provide reasonable assurance that the risk mitigation actions are taken in a timely manner. In the case of post-implementation reviews, the follow-up should focus on the timeliness of corrective actions in the downstream stages and in similar future projects.

9. EFFECTIVE DATE

9.1 This guideline is effective for all information systems audits beginning on or after 1 August 2003. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

APPENDIX

COBIT Reference

Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.

In the case of this specific audit area, review of the SDLC, the processes in COBIT likely to be the most relevant are: selected *Plan and Organise* IT processes, all the *Acquire and Implement* IT processes, and selected *Deliver and Support*. Therefore, COBIT guidance for the following processes should be considered relevant when performing the audit:

- PO8—Ensure Compliance with External Requirements
- PO10—Manage Projects
- PO11—Manage Quality
- AI1—Identify Automated Solutions
- AI2—Acquire and Maintain Application Software
- AI3—Acquire and Maintain Technology Infrastructure
- AI4—Develop and Maintain Procedures
- AI5—Install and Accredit Systems

G23 System Development Life Cycle (SDLC) Reviews cont.

- AI6—Manage Changes
- DS1—Define and Manage Service Levels
- DS2—Manage Third-party Services
- DS3—Manage Performance and Capacity
- DS4—Ensure Continuous Service
- DS5—Ensure Systems Security
- DS7—Educate and Train Users

The information criteria most relevant to an SDLC audit are:

- Primary: effectiveness and efficiency
- Secondary: confidentiality, integrity, availability, compliance and reliability

G24 Internet Banking

1. BACKGROUND

1.1 Linkage to ISACA Standards

1.1.1 Standard S2 Independence states, “The IS audit function should be independent of the area or activity being reviewed to permit objective completion of the audit assignment.”

1.1.2 Standard S4 Professional Competence states, “The IS auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment.”

1.1.3 Standard S5 Planning states, "The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards."

1.1.4 Standard S6 Performance of Audit Work states, "During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

1.1.5 Guideline G22 Business-to-consumer E-commerce Reviews provides guidance.

1.1.6 Procedure P3 Intrusion Detection System (IDS) Review provides guidance.

1.1.7 Procedure P2 Digital Signatures and Key Management provides guidance.

1.2 Linkage to COBIT

1.2.1 The COBIT *framework* states, "it is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."

1.2.2 The COBIT *Management Guidelines* provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 The *Management Guidelines* provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

1.2.4 The *Management Guidelines* can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.

1.2.6 Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to describe the recommended practices to carry out the review of Internet banking initiatives, applications and implementations, as well as to help identify and control the risks associated with this activity, so that the relevant IS Auditing Standards are complied with during the course of the review.

2. INTERNET BANKING

2.1 Definition

2.1.1 The term Internet banking refers to the use of the Internet as a remote delivery channel for banking services. Services include the traditional ones, such as opening an account or transferring funds to different accounts, and new banking services, such as electronic online payments (allowing customers to receive and pay bills on a bank’s web site).

2.2 Internet Banking Activities

2.2.1 More and more banks are transforming their businesses by using Internet technology to develop or expand relationships with their customers. The extent to which the Internet is used in a bank depends on the relative maturity of the bank in regard to Internet technology. Banks offer Internet banking in two main ways. An existing bank with physical offices, ordinarily termed a brick-and-mortar bank, can establish a web site and offer Internet banking to its customers as an addition to its traditional delivery channels. An alternative is to establish either a virtual, branchless or Internet-only bank. The computer server or bank database that lies at the heart of a virtual bank may be housed in an office that serves as the legal address of such a bank or at some other location. Virtual banks provide customers with the ability to make deposits and withdrawals via automated teller machines (ATMs) or through other remote delivery channels owned by other institutions. Characteristics of Internet banking include the unprecedented speed of change related to technological and customer service innovation, the ubiquitous and global nature of the Internet, the integration of Internet banking applications with legacy computer systems and the increasing dependence of banks on third parties that provide the necessary information technology. Accordingly, a bank can perform Internet activities in one or more of the following ways:

- Informational—This is the basic level of Internet banking. Typically, the bank has marketing information about the bank's products and services on a stand-alone server. Risks associated with these operations are relatively low, as informational systems typically have no path between the server and the bank's internal network. This level of Internet banking can be provided by the bank or can be outsourced. While the risk to a bank is relatively low, the data on the server or web site may be vulnerable to alteration. Appropriate controls, therefore, must be in place to prevent unauthorised alterations of the data on the bank's server or web site.
- Communicative—This type of Internet banking system allows some interaction between the bank's systems and the customer. The interaction may be limited to electronic mail, account inquiry, loan applications or static file updates (name and address changes). Because these servers ordinarily have a direct path to the bank's internal networks, the operational risk is higher with this configuration than with informational systems. Controls should be in place to prevent, monitor and alert management of any unauthorised attempt to access the bank's internal networks and computer systems. Virus detection and prevention controls are also important in this environment.
- Transactional—This level of Internet banking allows customers to directly execute transactions with financial implications. There are two levels of transactional Internet banking, each with a different risk profile. The basic transactional site only allows a transfer of funds between the accounts of one customer and the bank. The advanced transactional site provides a means for generating payments directly to third parties outside of the bank. This can take the form of bill payments via a bank official check or electronic funds transfer/automated clearing house entries. Many banks are also offering payments from consumer to consumer using either payment method. When the transfers of funds are allowed to a point outside of the bank, the operational risk increases. Unauthorised access in this environment can lead or give rise to fraud. Since a communication path is typically complex and may include passing through several public servers, lines or devices between the customer's and the bank's internal networks, this is the highest risk architecture and must have the strongest controls.

3. REVIEW OF INTERNET BANKING

3.1 Scope

3.1.1 Banking, by its very nature, is a high-risk business. The major risks associated with banking activities are: strategic, reputational, operational (including security—sometimes called transactional—and legal risks), credit, price, foreign exchange, interest rate and liquidity. Internet banking activities do not raise risks that were not already identified in traditional banking, but it increases and modifies some of these traditional risks. The core business and the information technology environment are tightly coupled, thereby influencing the overall risk profile of Internet banking. In particular, from the perspective of the IS auditor, the main issues are strategic, operational and reputational risk, as these are directly related to threats to reliable data flow and are heightened by the rapid introduction and underlying technological complexity of Internet banking. Banks should have a risk management process to enable them to identify, measure, monitor and control their technology risk exposure. Risk management of new technologies has three essential elements:

- Risk management is the responsibility of the board of directors and senior management. They are responsible for developing the bank's business strategy and establishing an effective risk management methodology. They need to possess the knowledge and skills to manage the bank's use of Internet banking and all related risks. The board should make an explicit, informed and documented strategic decision as to whether and how the bank is to provide Internet banking services. The initial decision should include the specific accountabilities, policies and controls to address risks, including those arising in a cross-border context. The board should review, approve and monitor Internet banking technology-related projects that have a significant effect on the bank's risk profile and ensure that adequate controls are identified, planned and implemented.
- Implementing technology is the responsibility of information technology senior management. They should have the skills to effectively evaluate Internet banking technologies and products, and to ensure that they are installed and documented appropriately. If the bank does not have the expertise to fulfil this responsibility internally, it should consider contracting with a vendor who specialises in this type of business or engaging in an alliance with another third party with complementary technologies or expertise.
- Measuring and monitoring risk is the responsibility of operational management. They should have the skills to effectively identify, measure, monitor and control risks associated with Internet banking. The board of directors should receive regular reports on the technologies employed, the risks assumed, and how those risks are managed.

3.1.2 Internal controls over Internet banking systems should be commensurate with the level of risk of the services the bank offers, the level of risk involved in the implementation and the bank's risk tolerance level. The review of internal control in the Internet banking environment must help the IS auditor to provide reasonable assurance that the controls are appropriate and function appropriately. Control objectives for an individual bank's Internet banking technology and products might focus on:

- Consistency of technology planning and strategic goals, including effectiveness, efficiency and economy of operations and compliance with corporate policies and legal requirements
- Data and service availability, including business recovery planning
- Data integrity, including providing for safeguarding of assets, proper authorisation of transactions and reliability of the data flow
- Data confidentiality and privacy standards, including controls over access by both employees and customers
- Reliability of management reporting

3.1.3 To appropriately evaluate the internal controls and their adequacy, the IS auditor should understand the bank's operational environment. COBIT 3rd Edition, published by the IT Governance Institute in 2000, has laid down seven information criteria to be met by information systems:

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

3.1.4 The information criteria listed in section 3.1.3 of this document are relevant in the case of Internet banking. Accordingly, a review of Internet banking should address how the information criteria of COBIT are met by the Internet banking initiative/application/ implementation.

3.1.5 Compared with other forms/channels of banking activities, Internet banking depends greatly on the integrity or trust in the confidentiality of customer data and on the availability of the system. In this context, there should be in place appropriate redundancy and fallback options, as well as disaster recovery procedures. In the case of Internet banking involving payments or funds transfers, nonrepudiation and integrity of the transactions are essential attributes. In such cases, the review of Internet banking should address the effectiveness of the Internet banking system controls in assuring nonrepudiation and integrity. Due attention should be given to them while evaluating the availability of Internet banking solutions, especially if the continuity is based on cross-border processing, because it might infringe a regulation or might run counter to compliance with bank regulations.

3.1.6 It is essential in Internet banking to confirm that any communication, transaction or access request is legitimate. Accordingly, banks should use reliable methods for verifying the identity and authorisation of new customers as well as authenticating the identity and authorisation of established customers seeking to initiate electronic transactions. Customer verification during account origination is important to reduce the risk of theft, fraudulent transactions and money laundering activities. Strong customer identification and authentication processes are particularly important in the cross-border context given the difficulties that may arise from doing business electronically with customers across national and international borders, including the risk of identity impersonation and the difficulty in conducting effective credit checks on potential customers.

3.1.7 Auditability has more significance in the Internet banking environment, because a significant proportion of the transactions take place in paperless environments.

4. INDEPENDENCE

4.1 Professional Objectivity

4.1.1 Before accepting the engagement, the IS auditor should provide reasonable assurance than any interests he/she may have in the Internet bank under review would not in any manner impair the objectivity of the review. In the event of any possible conflicts of interest, these should be explicitly communicated to the bank's management and the written approval of the bank's management should be obtained before accepting the assignment.

5. COMPETENCE

5.1 Skills and Knowledge

5.1.1 The IS auditor should have the necessary technical and operational skills and knowledge to carry out the review of the technology employed and risks associated with Internet banking. The IS auditor should determine whether the technology and products are aligned with the bank's strategic goals. In particular, such reviews would call for bank operations knowledge and associated risks, knowledge of banking laws and regulations together with the technical knowledge necessary to evaluate aspects such as web hosting/web housing technologies, encryption technologies, network security architecture and security technologies, such as firewalls, intrusion detection and virus protection. Where expert advice or expert input is necessary, appropriate use should be made of external professional resources. The fact that external expert resources may be used should be communicated to the bank's management in writing.

6. PLANNING

6.1 High-level Risk Assessment

6.1.1 The IS auditor should gather information regarding the Internet banking objectives of the bank, the strategy used to achieve the objectives, the way that the bank is using Internet technology in the relationships with its customers (either informative, communicative or transactional, as set out in 2.2.1). The information thus gathered should be such that it helps in carrying out a high-level assessment of the banking risks as well as the risks pertaining to the information criteria of COBIT. This high-level risk assessment will help determine the scope and coverage of the review. If the bank has an enterprise risk framework, this can be used.

6.1.2 The IS auditor should follow a risk assessment approach for analysing and evaluating the main potential general and specific threats connected to implementation of Internet banking, the possible manifestations, the potential effect on the bank, the likelihood of occurrences and the possible risk management measures that can be implemented for preventing risks. The following strategic risks should be evaluated:

- The strategic assessment and risk analysis
- Integration within corporate strategic goals
- Selection and management of technological infrastructure
- Comprehensive process for managing outsourcing relationships with third-party providers

6.1.3 The following security risks should be evaluated:

- Customer security practices
- Authentication of customers
- Nonrepudiation and accountability of transactions
- Segregation of duties
- Authorisation controls within systems, databases and applications
- Internal or external fraud
- Data integrity of transactions, databases and records
- Audit trails for transactions
- Confidentiality of data during transmission
- Third-party security risk

6.1.4 The following legal risks should be evaluated:

- Disclosures of information to customers
- Privacy
- Compliance to laws, rules and statements of the regulator or supervisor
- Exposure to foreign jurisdictions

6.1.5 The following reputational risks should be evaluated:

- Service level delivery
- Level of customer care
- Business continuity and contingency planning

6.2 Scope and Objectives of the Review

6.2.1 The IS auditor should, in consultation with the bank management where appropriate, clearly define the scope and objective of the review of Internet banking. The aspects to be covered by the review should be explicitly stated as part of the scope. The nature of the bank's Internet activities and volume of the Internet banking activities (set out in 2.2.1) and the risks associated with them—as identified by the high-level risk assessment—dictate which aspects need to be reviewed as well as the extent and depth of the review.

6.2.2 For the purpose of the review, control objectives should be in accordance with regulations and applicable banking laws. The Internet is borderless, so it is easy for any bank using an Internet-based delivery channel to operate in a multi-state and even multi-country environment. The bank may find itself bound by the laws, regulations and customs of wherever its customers are located rather than just where the bank is physically located. Therefore, the IS auditor should determine the geographic spread of the bank's current and planned customer base. The IS auditor needs to identify how many different jurisdictions have legal and regulatory control over the Internet banking operations and determine how the Internet bank is managing this risk.

6.3 Approach

6.3.1 The IS auditor should formulate the approach in such a way that the scope and objectives of the review could be fulfilled in an objective and professional manner. The approach followed should depend on whether the review is a pre-implementation review or a post-implementation review. The approach should be appropriately documented. If the input or advice of external experts is to be used, this should also be specified as part of the approach.

6.4 Sign-off for the Plan

6.4.1 Depending on the practices of the organisation, it may be appropriate for the IS auditor to obtain the agreement of the bank's management for the review plan and approach.

7. PERFORMANCE OF INTERNET BANKING REVIEW

7.1 Execution

7.1.1 The aspects to be reviewed and the review process should be chosen by taking into account the intended scope and objective of the review as well as the approach defined as part of the planning process.

7.1.2.1 In general, in gathering, analysing and interpreting the Internet banking environment, a study should be made of available documentation, such as bank regulations about Internet banking, Internet law, privacy law, web banking system documentation and use of the Internet banking solution.

7.1.3 To identify any problems relating to the Internet banking area which have been noted previously and which may require follow-up, the IS auditor should review the following documents:

- Previous examination reports
- Follow-up activities
- Work papers from previous examinations
- Internal and external audit reports

7.1.4 The IS auditor should map the key processes—both automated as well as manual—relating to the Internet banking initiative/ system.

7.1.5 The assessment of the core business risks (set out in 6.1) should include a critical evaluation of the Internet banking objectives, strategy and business model.

7.1.6 The IS auditor should then assess the probability that the risks identified pertaining to these processes (business as well as IS risks) will materialise together with their likely effect, and document the risks along with the controls, which mitigate these risks.

7.1.7 As part of the IS risk assessment, external IS threats should be evaluated depending on the nature of products offered by a bank and the external threats to be addressed. These threats include denial of service, unauthorised access to data, unauthorised use of the computer equipment, which could arise from various sources such as casual hackers, competitors, alien governments, terrorists or disgruntled employees.

7.1.8 Depending on the nature of the pre- or post-implementation review, the IS auditor should test the significant processes in the test and or production environment to verify that the processes are functioning as intended. These tests include testing of balance inquiry, testing of bill presentation and payment and testing the security mechanisms using penetration testing.

7.1.9 In post implementation review the IS auditor should obtain, at least, an understanding of network mapping, network routing, systems and network security assessment, and internal and external intrusion.

7.1.10 Since the Internet banking solution is predominantly an information technology solution, it should meet the information criteria established in COBIT, as well as other relevant standards or regulations of the industry. The extent of compliance with the information criteria, standards and/or regulations and the effect of noncompliance should be analysed.

7.2 Aspects to Review

7.2.1 The following organisational aspects should be reviewed for whether:

- Due diligence and risk analysis are performed before the bank conducts Internet banking activities
- Due diligence and risk analysis are performed where cross-border activities are conducted
- Internet banking is consistent with the bank's overall mission, strategic goals and operating plans
- Internet application is compliant with the defined and approved business model
- Internet banking systems and/or services are managed in-house or outsourced to a third-party
- Management and personnel of the organisation display acceptable knowledge and technical skills to manage Internet banking
- Measures to ensure segregation of duties are in place
- Management reports are adequate to appropriately manage Internet banking transaction and payment services activities

7.2.2 The review should include policy aspects such as whether:

- Suitable policies have been defined and implemented regarding the acquisition of customers, the engagement of suppliers, the customers authentication, the privacy of customers/suppliers data, audit trail, the review of usage logs and whether the bank is keeping abreast of legal developments associated with Internet banking
- The bank is providing accurate privacy disclosures associated with its Internet banking product line
- Information is provided on the web site to allow customers to make informed judgment about the identity and regulatory status of the bank before they enter into Internet banking services (name of the bank and the location of its head office, the primary bank supervisory authority, ways to contact to customer service and other relevant information)
- The bank has established policies governing the use of hypertext links such that consumers can clearly distinguish between bank and non-bank products, and that they are informed when leaving the bank's web site
- There are appropriate procedures in place regarding change control, the review of audit trails and the review/analysis of usage logs (firewall logs and other reports)
- There are suitable and adequate procedures in place to ensure the privacy and integrity of the data and to ensure compliance with the applicable laws and regulations as well as best practice

7.2.3 The following planning aspects should be reviewed for whether:

- The planned information systems technology architecture is feasible and will result in safe and sound operations
- There are appropriate incident response plans in place to manage, contain and minimise problems arising from unexpected events, including internal or external attacks

- An "Internet product life cycle" exists and if it is followed both for developing, maintenance and upgrading Internet applications
- Business continuity and contingency plans for critical Internet banking processing and/or delivery systems are in place and regularly tested

7.2.4 The following information systems infrastructure aspects should be reviewed for whether:

- The infrastructure and systems are capable of expansion to accommodate the proposed business plan
- An information security architecture has been defined and is appropriate for the nature of the Internet banking model
- The bank has an adequate process and controls to address physical security for hardware, software and data communications equipment associated with the Internet banking system
- The bank has a sound process which ensures adequate control over the path between the web site and the bank's internal networks or computer systems and whether the internal network is suitably protected from the external environment using appropriate firewall technology
- Databases and data flow are protected from unauthorised/inappropriate access
- There are suitable and adequate procedures in place to ensure the identification of access points and potential areas of vulnerability
- There are appropriate manual balancing controls where automated controls are inadequate
- The record for each customer transaction contains identification of the customer, the transaction number, the type of transaction, the transaction amount and other information of relevance, if it is stored and archived, for control purposes or other business functions such as marketing

7.2.5 The following telecommunication infrastructure aspects should be reviewed for whether:

- The network architecture is appropriate for the nature, timing and extent of the Internet banking operation
- The network protocols used are appropriate for the intended use (for instance, if payments or funds transfers are accepted through the Internet banking system, secure protocols should be used)
- The bank has an effective process to assess the adequacy of physical controls in place to restrict access to firewall servers and components
- Intrusion detection systems and virus control systems/procedures are in place
- There is adequate penetration testing of internal or external networks
- The communication across the network is made secure using virtual private network (VPN) and related encryption techniques where appropriate and necessary
- Adequate and strong encryption algorithms were selected to protect data during communication across the network

7.2.6 The following authentication aspects should be reviewed for whether:

- Control features are in place to validate the identity of prospective customers while they use the Internet to apply for new bank loan and/or deposit accounts
- Control features are built into the systems to ensure the authentication of the existing customer, the integrity of data and the confidentiality of transactions
- Authentication procedures are used to uniquely and positively identify the transacting party using digital certificates and digital signatures where necessary
- Nonrepudiation is ensured for an eventual later business or legal use where transactions are made using the Internet banking system
- The fault tolerance features of the Internet banking system are commensurate with the nature, volume and criticality of its system

7.2.7 The following third-party service provider aspects should be reviewed for whether:

- Due diligence review of the competency and financial viability was conducted prior to entering into any contract with third-party service providers
- The contracts with third-party service providers adequately protect the interests of the bank and the bank's customers, and whether the bank organisation has reviewed vendor contracts to ensure that the responsibilities of each party are appropriately identified and defined
- The bank organisation obtains and reviews internal or external audit reports of third-party service providers, evaluating vendor management processes or specific vendor relationships as they relate to information systems and technology, and whether all outsourced systems and operations are subject to risk management, security and privacy policies that meet the bank's own standards
- The bank organisation has the right to conduct independent reviews and/or audits of security, internal control and business continuity and contingency plans of third-party service providers
- The security procedures of the third parties are appropriate and adequate where the Internet banking solution depends on the any third-party service providers such as Internet service providers (ISP), certification authority (CA), registration authority (RA), web-hosting/housing agency

- Third-party service providers have appropriate business continuity and contingency plans for critical Internet banking processing and/or delivery systems are in place and regularly tested, and whether the bank receives copies of test result reports
- The bank has an adequate process to ensure that software maintained by the vendor is under a software escrow agreement and that the software is confirmed as being current on a regular basis where the bank obtains software products from a vendor
- A third –party's opinion is sought in the pre-implementation phase of Internet applications for evaluating the security architecture solution that will be developed and configured

7.2.8 Where necessary and agreed with the bank, external expert input or advice should be used suitably in the collection, analysis and interpretation of the data.
7.2.9 The inferences and recommendations should be based on an objective analysis and interpretation of the data.
7.2.10 Appropriate audit trails should be maintained and protected for the data gathered, the analysis made and the inferences arrived at, as well as the corrective actions recommended.
7.2.11 Before finalising the report, the observations and recommendations should be validated with the stakeholders, board of directors and the bank's management, as appropriate.

8. REPORTING

8.1 Report Content
8.1.2 The IS auditor should produce regular reports on the technologies employed, the risks assumed, and how those risks are managed. Monitoring system performance is a key success factor. Depending on the scope of its coverage, the report on Internet banking review carried out should address the following, as appropriate:

- The scope, objectives and methodology followed and assumptions
- An overall assessment of the Internet banking processes/systems solution in terms of key strengths and weaknesses as well as the likely effects of weaknesses
- Recommendations to overcome the significant weaknesses and to improve the Internet banking processes/systems solution
- A statement on the extent of compliance with bank regulations or applicable laws, along with the effect of any noncompliance
- A statement on the extent of compliance with the information criteria of CobiT, along with the effect of any noncompliance
- Recommendations regarding how the lessons of the review could be used to improve similar future solutions or initiatives

9. EFFECTIVE DATE

9.1 This guideline is effective for all information systems audits beginning on or after 1 August 2003. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

APPENDIX

CobiT Reference
Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT's information criteria.

In the case of this specific audit area, Review of Internet Banking, the processes in CobiT likely to be the most relevant are: selected *Plan and Organise* IT processes, selected *Acquire and Implement* IT processes, selected *Deliver and Support, and selected Monitor and Evaluate*. Therefore, CobiT guidance for the following processes should be considered relevant when performing the audit:

- PO1—Define a Strategic IT Plan
- PO3—Determine Technological Direction
- PO8—Ensure Compliance with External Requirements
- PO9—Assess Risk
- AI2—Acquire and maintain application software
- AI3—Acquire and maintain technology infrastructure
- AI4—Develop and maintain procedures
- AI5—Install and accredit systems
- AI6—Manage Changes
- DS1—Define and Manage Service Levels
- DS2—Manage Third-party Services
- DS3—Manage performance and capacity
- DS4—Ensure Continuous Service
- DS5—Ensure Systems Security

- DS8—Assist and Advise Customers
- DS10—Manage Problems and Incidents
- DS11—Manage Data
- M1—Monitoring the Process
- M2—Assess Internal Control Adequacy

The information criteria most relevant to an Internet Banking audit are:

- Primary: confidentiality, integrity, availability, compliance and reliability
- Secondary: effectiveness and efficiency

REFERENCES

An Internet Banking Primer, Federal Reserve Bank of Chicago, USA

*Basle Directive N° 82, Risk Management Principles for Electronic Banking***,** Basel Committee on Banking Supervision, May 2001, Switzerland

Basle Directive N° 86, Sound Practices for the Management and Supervision of Operational Risk, Basel Committee on Banking Supervision, May 2001, Switzerland

*Basle Directive N° 91, Risk Management Principles for Electronic Banking***,** Basel Committee on Banking Supervision, July 2002, Switzerland

BIS Papers N° 7. Electronic finance: a new perspective and challenges, Monetary and Economic Department, Bank for International Settlements, November 2001, Switzerland

Cronin, Mary J., *Banking and Finance on the Internet,* John Wiley & Sons, Inc., ISBN 0-471-29219-2, USA

Essinger, James, *The Virtual Banking Revolution,* Thomson Business Press, ISBN 1-86152-343-2, United Kingdom

*Internet Banking Comptroller's Handbook***,** Comptroller of the Currency Administrator of National Banks, October 1999, USA

Furst, Karen, William W. Lang and Daniel E. Nolle, *Internet Banking: Developments and Prospects,* Economic and Policy Analysis Working Paper 2000-9, Office of the Comptroller of the Currency, September 2000, USA

The Internet and the National Bank Charter, Comptroller of the Currency Administrator of National Banks, January 2001, USA

Treatment of material on overseas Internet world wide web sites, accessible in the UK but not intended for investors in the UK, Financial Services Authority, United Kingdom

G25 Review of Virtual Private Networks

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, "During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

1.1.2 GuidelineG16 Effect of Third Parties on an Organisation's IT Controls provides guidance.

1.1.3 GuidelineG17 Effect of Nonaudit Role on the IS Auditor's Independence provides guidance.

1.2 Linkage to COBIT

1.2.1 COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."

1.2.2 COBIT *Management Guidelines* provides a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 *Management Guidelines* provides example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and identify control gaps and strategies for improvement.

1.2.4 *Management Guidelines* can be used to support self-assessment workshops and can also be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.

1.2.6 The COBIT references located in the appendix of this document offer the specific objectives or processes of COBIT to consider when reviewing the area addressed by this guidance.

1.3 Need for Guideline

1.3.1 The purpose of this guideline is to describe the recommended practices in carrying out the review of virtual private network (VPN) implementations so that the relevant IS Auditing Standards are complied with during the course of the review.

2. VIRTUAL PRIVATE NETWORK (VPN)

2.1 Definition

2.1.1 *Virtual Private Networking—New Issues for Network Security*, published by the IT Governance Institute, defines VPN as a: "network of virtual circuits that carries private traffic through public or shared networks such as the Internet or those provided by network service providers (NSPs)." For the purpose of this guideline, this definition of VPN is used.

2.1.2 In the context of VPN, the terms "tunnel" and "tunneling" are often used. The process of encapsulating one type of packet in another packet type so the data can be transferred across paths that otherwise would not transmit the data is called tunneling. The paths the encapsulated packets follow in an Internet VPN are called tunnels.

2.2 VPN Models

2.2.1 There are three common VPN models for deployment. The major differences among the models are in the location of their service end points or tunnel end points, the level of management required, quality of service, and the reliance on direct service provider involvement. The three most common models are:

- Pure provider model
- Hybrid provider model
- End-to-end model

2.2.2 In the pure provider model, most of the VPN functionality is built into the service provider infrastructure and not in the network of the organisation. This model is often deployed over one service provider's network. There is a clear line of distinction between the organisation's network and the service provider's network. Remote access to the organisation's network is typically provided by a dedicated circuit (such as, T1, T3), ATM connections or dedicated frame relay connections. The customer owns and operates the remote access VPN-related equipment and software in the network, while equipment and software inside the service provider's network, from the physical circuit out, is owned and operated by the service provider. The service provider initiates VPN tunnels from edge-to-edge of the network and relies on the private circuits on either end for security. In this model, the provider has a high level of control over the network and is responsible for capacity planning, design, configuration, diagnostics and troubleshooting.

2.2.3 The hybrid provider model involves the networks of both the service provider and the organisation. A VPN tunnel is initiated from inside the provider's network, and the tunnel is terminated at the organisation's network. In this model, the service provider is responsible for the initiation of the VPN tunnels for the remote users after the users are authenticated. When the remote user reaches the organisation's network, a second authentication may be required before being granted access permission to the private network. Users can access the network facilities as if they are directly connected to the enterprise LAN, once they are authenticated.

2.2.4 In the end-to-end model, the service provider serves only as a transport for the VPN data. The service end points or tunneling could be the desktop or a VPN device that serves as a proxy for multiple desktops. Both service end points are outside the service provider's network. This model can be used for remote access or to connect multiple sites.

2.3 VPN Usage

2.3.1 There are various ways to use a VPN, depending upon the model used. The most common are:

- Site-to-site connectivity
- Remote access connectivity
- Extended enterprise extranet connectivity

2.3.2 The site-to-site connectivity provides separate intranets to connect securely, effectively creating one large intranet. Site-to-site VPNs are often used by geographically distributed organisations to create a single logical network.

2.3.3 The remote access connectivity permits mobile employees to access the organisation's intranet, via the Internet, using a secure network communications. This is used in combination with global dial-up, wireless and broadband ISPs. Many organisations use remote access VPNs to provide low-cost network accessibility to their employees.

2.3.4 Extended enterprise extranet connectivity provides connections to networks outside the enterprise. Business, research or marketing partners often use these to speed communications through secured connections. Generally, extranets have stronger controls in place to allow, manage and monitor network-to-network traffic, and the internal network may be protected from the extranet via firewalls.

2.4 VPN Architecture

2.4.1 There are many possible options for installing VPNs. A VPN supplied by a network service provider is one of the most common approaches to connect an organisation to the Internet. The VPN architecture in any organisation could be one or combinations of the following:

- Firewall-based VPNs
- Router-based VPNs
- Remote access-based VPNs
- Hardware (black box)-based VPNs
- Software-based VPNs

2.4.2 The firewall-based VPNs are the most common form of implementation. Since most organisations already use a firewall to connect to the Internet, they need to add encryption software and some kind of authorisation software.

2.4.3 There are two types of router-based VPNs. In one, software is added to the router to allow encryption to occur. With the second type, a third-party vendor-supplied external card must be inserted into the same chassis as the router to off-load the encryption process from the router's CPU to the card.

2.4.4 With remote access-based VPNs, someone from a remote location could create an encrypted packet stream or tunnel to a network device in the organisation.

2.4.5 With hardware (black box)-based VPNs, the vendor offers a black box, or a device with encryption software, to create a VPN tunnel. The black box VPN device is ordinarily behind the firewall or on the side of the firewall to secure the data, but in fact the VPN system may be wholly independent of the firewall.

2.4.6 In software-based VPNs, the software handles the tunneling to another client or encryption of packets. Software is loaded on the client and the server. Traffic starts from a specific client within the organisation and makes a connection to a server located at the remote site. Traffic leaving the client is encrypted or encapsulated, and routed to its destination. The same applies for someone trying to connect to the internal network.

2.5 VPN Configuration/Topology

2.5.1 When configuring the VPN, parameters must be set for key length, authentication servers, connection and idle timeouts, certificate generation and key generation, and distribution mechanisms. There are numerous ways to configure and implement VPN architecture and to place the architecture in a VPN topology. Organisations could use one or combinations of the following most commonly used topologies in a VPN configuration:

- Firewall-to-client
- LAN-to-LAN
- Firewall-to-intranet/extranet
- Hardware and software VPN

2.5.2 Firewall-to-client is the most commonly used topology, and it applies to remote users who dial into an internal network.

2.5.3 LAN-to-LAN is the second most commonly used topology. It extends the firewall-to-client topology to different remote offices and among offices, business partners and suppliers when a VPN tunnel has been created between two sites.

2.5.4 In firewall-to-intranet/extranet topology, intranets are used by employees and extranets are used externally by customers, business partners and suppliers. When remote users try to access servers on the extranet or intranet, a decision must be made as to which server they may access.

2.5.5 Hardware and software VPNs are stand-alone devices designed to implement VPN technology algorithms. A VPN device is ordinarily behind the firewall on the internal network. Data packets flow through the firewall and the VPN device. As the packets pass through these devices, they can be encrypted. Generally in software encryption models like SSL protocol, the special devices (authentication) are not required and the packet flow is encrypted by the software.

2.5.6 VPN technologies and protocols include:

- PPTP (point to point tunneling protocol)
- L2TP (layer 2 tunneling protocol)
- IPSec (Internet protocol security)
- SSL (secure socket layer)

3. RISKS ASSOCIATED WITH VPNs

3.1 Types of Risks

3.1.1 Since VPN is a communication infrastructure for the business that uses third-party services, the risks associated with it could be categorised as:

- Security risk
- Third-party risk
- Business risk
- Implementation risk
- Operating risk

3.2 Security and Legal Risk

3.2.1 The security risks relating to VPNs include:

- Inadequate assessment of security and legal risks arising out of using VPNs
- Insufficient security programs to mitigate risks to information assets arising out of VPNs
- Inadequate protection of data while they are at the point before entering the VPN, or once they arrive at the point on leaving the VPN
- Failure to secure information while unencrypted over a given network path (internal networks before encryption device or external networks after decryption device)
- Lack of implementation that could result in confidentiality, integrity, nonrepudiation and/or availability issues.

3.3 Third-party Risk

3.3.1 The reliance on third-party service providers could result in risks such as:

- Choice of an inappropriate provider
- Inadequate relationship management
- Inadequacies in service level agreements (SLA) and metrics
- Inappropriate governance and management process
- Inadequate measuring and monitoring of SLAs and metrics
- Inadequate backup/redundancy strategy
- Insufficient benchmarking of the relationship and services
- Abuse of access to data on the VPN

3.4 Business Risk

3.4.1 Risks such as the following could lead to nonfulfillment of the management or business expectations:

- Inadequate alignment to business strategy
- Inadequate cost savings
- Failure to achieve security requirements
- Insufficient ease of use
- Failure to address scope and span of user needs
- Loss/degradation of service in other areas of the organisation or process

3.5 Implementation Risk

3.5.1 Risks such as the following could lead to the implementation of an ineffective and inefficient solution:

- Inadequate attention to and investment in up-front design
- Inappropriate selection of the VPN model for organisation
- Inadequate use of the third parties where appropriate
- Insufficient attention to security in design
- Inappropriate recovery processes
- Failure to design service level expectations and measurements
- Inappropriate integration strategy
- Ineffective change, project or implementation management processes
- VPN client risk (same interface accept Internet and VPN traffic)

3.6 Operating Risk

3.6.1 Risks such as the following result in ineffective and inefficient utilisation/operation of the VPN:

- Inadequate resources to operate effectively
- Lack of reliability
- Impairment of quality of service
- Lack of interoperability
- Failure to encapsulate
- Inadequate capacity
- Failure to provide redundancy or back up
- Use of personal devices (home computing) for business purpose (lack of security configurations, antivirus software, personal firewalls)
- Lack of confidentiality on operation parameters or data

4. CHARTER

4.1 Mandate

4.1.1 Before commencing a review of a VPN, the IS auditor should provide reasonable assurance of the requisite mandate by virtue of the IS auditor's position or the required written mandate provided by the organisation to carry out the envisaged review. In case the review is initiated by the organisation, the IS auditor also should obtain reasonable assurance that the organisation has the appropriate authority to commission the review.

5. INDEPENDENCE

5.1 Professional Objectivity

5.1.1 Before accepting the assignment, the IS auditor should provide reasonable assurance that the IS auditor's interests, if any, in the VPN solution being reviewed would not in any manner impair the objectivity of the review. In the event of any possible conflict of interests, the same should be communicated explicitly to the organisation, and a written statement of the organisation's awareness of the conflict should be obtained before accepting the assignment.

5.1.2 In case the IS auditor has/had any nonaudit roles in the VPN being reviewed, the IS auditor should consider the guideline G17 Effect of Nonaudit Roles on the IS Auditor's Independence.

6. COMPETENCE

6.1 Skills and Knowledge

6.1.1 The IS auditor should provide reasonable assurance of the necessary technical knowledge to review the VPN. A clear understanding of the business requirements and the technical aspects of the VPN is necessary while reviewing the VPN implementation in an organisation.

6.1.2 The IS auditor also should provide reasonable assurance of access to the relevant technical skill and knowledge to carry out the review of the VPN. Review of VPN would call for good technical knowledge to evaluate aspects such as the encryption technologies used, network security architecture and security technologies. The IS auditor should have adequate knowledge to review these aspects. Where expert inputs are necessary, appropriate inputs should be obtained from external professional resources. The fact that external expert resources would be used should be communicated to the organisation in writing.

7. PLANNING

7.1 High-level Risk Assessment

7.1.1 The IS auditor should gather information regarding the business and its requirements for the VPN to carry out a high-level risk assessment.

7.1.2 The VPN-related risks referred to in section three above should be considered depending on the stage at which the review is being carried out, such as during design (pre-implementation), implementation or post-implementation.

7.1.3 The relevant COBIT information criteria—effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability—that need to be reviewed and confirmed, should also be identified.

7.1.4 The relevant aspects of the *Control Objectives for Net Centric Technology* (CONCT) should also be considered in this context, since these are extensions of COBIT criteria to network-centric environments such as those supported by VPNs.

7.1.5 This high-level risk assessment will help determine the scope and coverage of the review.

7.2 Scope and Objectives of the Review

7.2.1 The IS auditor, in consultation with the organisation where appropriate, should clearly define the scope and objective of the review of the VPN. The aspects to be covered by the review should be explicitly stated as part of the scope. The high-level risk assessment referred to in section 7.1.1 would dictate which aspects need to be reviewed and the extent and depth of the review.

7.2.2 For the purpose of the review, the stakeholders in the solution also should be identified and agreed upon with the organisation.

7.2.3 Any key concerns of the stakeholders should also be included, as appropriate, in the scope and objectives of the review.

7.2.4 In case the review scope includes third-party providers, the IS auditor must assure the audit clause was included in the contract.

7.3 Approach

7.3.1 The IS auditor should formulate the approach in such a way that the scope and objectives of the review could be fulfilled in an objective and professional manner. The approach followed should depend on whether the review is pre-implementation, at the implementation stage or post-implementation. The approach should be appropriately documented. When and where external expert inputs would be used also should be specified as part of the approach. Any planned use of testing/monitoring tools should also be stated as part of the approach.

7.4 Sign-off for the Plan

7.4.1 Depending on the organisational practices, the IS auditor may obtain the concurrence of the organisation for the plan and approach.

8. PERFORMANCE OF THE VPN REVIEW

8.1 General

8.1.1 This section addresses the wide spectrum of aspects to be addressed during the execution of a VPN review. For a specific VPN review, aspects relevant to the review should be identified from this wide spectrum of aspects depending on the envisaged scope and objectives of the review.

8.1.2 The VPN review should be carried out as per the defined approach (with refinements as appropriate), so the envisaged objectives of the review are fulfilled.

8.1.3 In general, study of available documentation (such as, business case, system documentation, contracts, service level agreements and logs), discussions with the stakeholders and service providers, and observation should be used appropriately in gathering, analysing and interpreting the data. Where appropriate, the IS auditor should test the significant processes/functions in the VPN environment to verify that the processes/functions are performing as intended.

8.1.4 Where necessary and agreed upon with the organisation, external expert inputs could be used suitably in the collection, analysis and interpretation of the data.

8.1.5 The inferences and recommendations should be based on an objective analysis and interpretation of the data.

8.1.6 Appropriate audit trails should be maintained for the data gathered, analysis made, inferences arrived at and corrective actions recommended.

8.2 Pre-implementation Review

8.2.1 The pre-implementation review, carried out before the VPN solution is implemented (during design stage), should address the appropriateness of the:

- Requirements for a VPN solution
- Cost-benefits of the proposed solution
- Proposed VPN technology, such as VPN model, VPN architecture, VPN configuration/topology and VPN usage
- Proposed security architecture and features, including the proposed encryption technologies
- Redundancy and backup facilities planned
- Management approvals
- Proposed project management structures and monitoring mechanisms
- Selection process for the choice of the service provider
- Proposed contract, SLAs and metrics
- Statutory requirements, if any, that need to be fulfilled

8.2.2 To address these aspects the IS auditor should:

- Study the VPN requirements—business as well as technical
- Study the business case (costs and benefits) and the approvals for the same
- Review the VPN design document outlining the technology aspects
- Review whether the proposed solution would conform to one of PPTP, L2TP and IPSec protocols
- Review the proposed security architecture and encryption technology
- Review the tender process, including the technical and commercial evaluation of the alternate proposals and the ultimate choice of the service provider
- Study the proposed project management structure
- Study the proposed contracts, SLA and metrics
- Study the statutory requirements to be fulfilled
- Evaluate the redundancy and backups proposed
- Review the strategy proposed for integrating the VPN with the applications
- Use external experts, where necessary, to evaluate the appropriateness of the technology and security aspects
- Study the proposed training plans
- Study any related audit/review reports
- Evaluate the results of the above with reference to their appropriateness as well as their adequacy to mitigate the risks—security risk, third-party risk, business risk, implementation risk and operating risk
- Evaluate how COBIT and CONCT criteria are being fulfilled
- Highlight the risks and issues arising out of the review for necessary corrective action.

8.3 Implementation Review

8.3.1 The implementation review happens during the implementation, and accordingly, it should address whether the:

- Implementation is progressing per the approved plans and within agreed time frames and costs
- VPN technology—VPN model, VPN architecture, VPN configuration/topology and VPN usage—is implemented as intended
- Security scheme and the encryption technologies used are robust and are as designed
- The planned redundancy and backup facilities are implemented
- The actual contracts, SLAs and metrics address the organisation's requirements
- The statutory requirements, if any, are addressed

8.3.2 To address the above referred aspects the IS auditor should:

- Study the project progress reports and minutes of meetings
- Evaluate the actual implementation of the technologies against the plans and identify the deviations, if any
- Confirm whether the solution is certified to conform to one of PPTP, L2TP and IPSec protocols
- Evaluate the actual security architecture and encryption technology implemented for conformance with the approved design
- Study the actual contracts, SLA and metrics that were agreed upon
- Evaluate the redundancy and backups established
- Review the actual integration of the VPN with the applications
- Use external experts, where necessary, to evaluate the appropriateness of the technology and security aspects actually implemented

- Evaluate the adequacy of the testing and migration processes to assess whether they address all kinds of users and cover such things as capacity, bandwidth, access control and encryption in an appropriate manner
- Evaluate the billing mechanisms being built
- Assess whether the legacy connections are being retired, their billings discontinued and equipments disposed of progressively with the implementation of the VPN
- Study the earlier pre-implementation audit report, if any, and any other related review reports to assess whether the risk mitigation actions recommended earlier are being implemented
- Evaluate the results of the above with reference to their appropriateness as well as their adequacy to mitigate the risks—security risk, third-party risk, business risk, implementation risk and operating risk
- Evaluate how COBIT and CONCT criteria are fulfilled
- Highlight the risks and issues arising out of the review for necessary corrective action

8.4 Post-implementation Review

8.4.1 The post-implementation review occurs after the implementation of the VPN, and hence, it should address whether the:

- Envisaged benefits are being achieved
- One-time costs are as planned and reasonable
- Ongoing billings are reasonable and as agreed
- VPN technology is being used as intended
- VPN and its usage are in conformance with the security policies and procedures including data classification
- Third parties accessing the VPN via extranets have signed the relevant security and confidentiality agreements and are complying with the same
- The users accessing through remote connection and using laptops use necessary security features including personal firewalls, where appropriate
- There are appropriate processes for the management of digital certificates
- The SLAs and metrics, including quality of service (QoS), are measured, monitored and escalated on a regular basis for timely actions
- The data are sufficiently protected at entry and exit points as well as over unencrypted links using appropriate procedures
- Appropriate security tools and processes are in place for such things as virus checking and intrusion detection
- The services and costs are comparable and competitive
- The redundancy and backup facilities are functioning appropriately
- The statutory requirements, if any, are addressed

8.4.2 To address the above referred aspects the IS auditor should:

- Study the project completion report
- Review the VPN technology in actual use for its conformance with the approved design
- Confirm whether the solution is certified to conform to one of PPTP, L2TP and IPSec protocols
- Review the ongoing billings on a sample basis
- Carry out sample checking of compliance with security policies and procedures
- Check the third-party access as well as the agreements signed by third parties regarding extranet access
- Check the remote and laptop access processes as well the laptops for appropriate security settings
- Review the actual SLAs and metrics including QoS and the actual process of monitoring them
- Check the security implementation across the network
- Test the backup and redundant facilities
- Carry out periodic benchmarking to provide reasonable assurance of continued reasonableness of charges and quality of services

- Use external experts, where necessary, to evaluate the appropriateness of the technology and security aspects in place
- Use appropriate tools to test relevant aspects of the VPN solution
- Review the help desk process supporting the VPN
- Evaluate the results of the above with reference to their appropriateness as well as their adequacy to mitigate risks—security risk, third-party risk, business risk, implementation risk and operating risk
- Evaluate how COBIT and CONCT criteria are fulfilled
- Highlight the risks and issues arising out of the review for necessary corrective action

9. REPORTING

9.1 Report Content

9.1.1 The report on the VPN review should address the following aspects depending on the scope of its coverage:

- The scope, objective, methodology followed and assumptions
- Overall assessment of the solution in terms of key strengths and weaknesses as well as the likely effects of the weaknesses
- Recommendations to overcome the significant weaknesses and improve the solution
- The extent of compliance with COBIT's information criteria and CONCT criteria, and the effect of any noncompliance
- Recommendations regarding how the experience could be used to improve similar future solutions or initiatives

9.1.2 The observations and recommendations should be validated with the stakeholders and organisation, as appropriate, before finalising the report.

10. FOLLOW-UP

10.1 Tracking Actions Agreed

10.1.1 The actions agreed at the end of the VPN review should be assigned due dates and tracked for completion. Outstanding issues should be escalated to appropriate management for necessary action.

11. EFFECTIVE DATE

11.1 This guideline is effective for all information systems audits beginning on or after 1 July 2004. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary*.

APPENDIX

COBIT Reference

Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT information criteria.

In a VPN, a communication infrastructure, the following aspects are more relevant:

- PO1—Define a Strategic IT Plan
- PO3—Determine Technological Direction
- PO5—Manage The IT Investment
- PO8—Ensure Compliance With External Requirements
- PO9—Assess Risks
- PO10—Manage Projects
- AI3—Acquire and Maintain Technology Infrastructure
- AI4—Develop and Maintain Procedures
- AI5—Install and Accredit Systems
- AI6—Manage Changes
- DS1—Define and Manage Service Levels
- DS2—Manage Third-party Services
- DS3—Manage Performance and Capacity
- DS4—Ensure Continuous Service
- DS5—Ensure Systems Security

G25 Review of Virtual Private Networks cont.

- DS9—Manage the Configuration
- DS12—Manage Facilities
- DS13—Manage Operations
- M1—Monitor the Processes

The information criteria most relevant to a VPN review are:

- Primary: availability, confidentiality, effectiveness and integrity
- Secondary: efficiency, compliance and reliability

References

Virtual Private Networking—New Issues for Network Security, IT Governance Institute, USA, 2001
Control Objectives for Netcentric Technology (CONCT), *IT Governance Institute, USA, 1999*

G26 Business Process Reengineering (BPR) Project Reviews

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, "During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

1.1.2 Guideline G17 Effect of Nonaudit Role on the IS Auditor's Independence provides guidance.

1.1.3 Guideline G21 ERP Systems Review provides guidance.

1.2 Linkage to CobiT

1.2.1 CobiT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."

1.2.2 CobiT *Management Guidelines* provides a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 *Management Guidelines* provides example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

1.2.4 *Management Guidelines* can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 CobiT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT's information criteria.

1.2.6 A CobiT reference is located in the appendix of this document for the specific objectives or processes of CobiT that should be considered when reviewing the area addressed by this guidance.

1.3 Need for Guideline

1.3.2 Manufacturing and service organisations are taking an increasing interest in business process reengineering (BPR) to support their evolution in a dynamic and rapidly changing business environment. BPR offers an invaluable opportunity to achieve a real breakthrough in business performance, but it also introduces risks, for example in the case of wrong reengineering choices or of inadequate implementation of the devised changes.

1.3.3 Reengineering involves comprehensive changes not simply to business processes but to management and support structures, people and organisation, technology and information systems, and policies and regulations. That means that BPR projects have a strong effect on the control system of the organisations that have implemented the BPR. Specifically, there is an increased risk that essential controls are reengineered out of the process to expedite business transactions. Accordingly, the IS auditor should be cognisant and espouse to management that controls, though they appear in nature to slow the process down, are a necessity to avoid risk that cannot be easily managed or measured in both likelihood or effect.

1.3.4 The purpose of this guideline is to provide IS auditors with the basic reengineering issues as a framework for assessing the key tasks and risks associated with BPR projects with special attention to the IS aspects.

2. BUSINESS PROCESS REENGINEERING PROJECTS

2.1 Definition

2.1.1 Although there is no universally accepted definition of business process reengineering, the definition most often quoted is that offered by Hammer and Champy: The fundamental rethinking and radical redesign of business processes to bring about dramatic improvements in critical, contemporary measures of performance, such as cost, quality, service and speed.[1]

2.1.2 BPR aims to improve business processes by substantially revising their structure and by dramatically changing the way in which the processes are managed and implemented. This ordinarily produces a great effect on the people involved and the working practices and supporting technologies, particularly information technologies.

2.2 BPR Key Results

2.2.1 A BPR project is extremely pervasive. The effect is a substantial modification of all organisation processes and relationships. The main results of a BPR project can therefore be summarised as follows:

- Strategic in concept
- New business priorities based on value and customer requirements (customer driven, output focused) with concentration on process (focus on key business processes) as a means of improving product, service and profitability

[1] Hammer and Champy, *Reengineering the Corporation*, 1993

- New approaches to organising and motivating people inside and outside the enterprise
- New approaches to the use of technology in developing, producing and delivering goods and services
- Redefined roles for suppliers, including outsourcing, joint development, quick response, just-in-time inventory and support
- Redefined roles for clients and customers providing them with more direct and active participation in the enterprise's business processes

2.3 BPR Principles and Activities

2.3.1 Principles help with the innovative thinking necessary to change the process structure. The principles are mainly of value in what is ordinarily the most difficult stage of BPR projects, namely considering the options for changing the process.

2.3.2 The BPR principles suggested by Hammer are as follows:

- Several jobs are combined into one.
- Workers make decisions.
- The steps in a process are performed in a natural order.
- Processes have multiple versions.
- Work is performed where it makes the most sense.
- Checks and controls are reduced (while controls on implementation are critical).
- Reconciliation is minimised.
- A case manager provides a single point of contact.
- Hybrid centralised/decentralised operations are prevalent.

2.3.3 Others , including Carter and Handfield, suggest carrying out the BPR activities in sequence: 1) simplification (which includes elimination of nonvalue-added activities), 2) standardisation, 3) integration, 4) parallelism, 5) variance control, 6) resource allocation, 7) automation. They indicate the BPR process should tackle steps 1 to 7 in a strict sequence. It would, for example, be wrong to attempt automating a process with an IT application without first considering its simplification; not only could simplification make automation redundant but the full benefits of automation may not be realised either. However, there is a danger in restricting the thinking process to a strict sequence. For example, integration of activities requiring different resources into a single activity to be carried out by an individual may sometimes become possible only with automation.

2.3.4 Sometimes a holistic view is the best approach.

2.4 BPR Methodology

2.4.1 Reengineering is inherently highly situational and creative. Basically, there are two distinct approaches to BPR that can be found in the literature.

2.4.2 The methodology originally prescribed by Hammer and Champy is a top-down approach, which suggests that the BPR team should focus on determining how the strategic objectives of the organisation can be met without letting its thinking be constrained by the existing process. The emphasis is on the to-be process, and is consistent with the step-change philosophy that the authors presented.

2.4.3 The more incremental change methodology outlined by Harrington is a bottom-up approach which advocates modeling the existing process to gain understanding of it, and then streamlining it appropriately to meet the strategic objectives. The focus is on changing the as-is process by identifying opportunities for improving it.

2.4.4 In practice, a BPR team will ordinarily need to adopt a mixed approach. If the top-down methodology is used as the basis, there is still a need to understand the current functionality and to define carefully the transition path from the current to the preferred future process. With a bottom-up methodology, BPR teams can spend too much time on detailing the current process and lose innovative thinking. A mixed approach would encourage the team to consider high-level changes without being cluttered by the details of the current process.

2.4.5 It is important to recognise that an initial BPR study may lead to recommendations for a number of more detailed projects on improving subprocesses, which may only require relatively small changes (perhaps to remove some bottlenecks).

2.5 Six Basic Steps of Several BPR Methodologies

2.5.1 Envision—This stage typically involves a BPR project champion engendering the support of top management. A task force, including senior executives and individuals knowledgeable about a firm's processes, is authorised to target a business process for improvement based on a review of business strategy and IT opportunities in the hope of improving the firm's overall performance.

2.5.2 Initiate—This stage encompasses the assignment of a reengineering project team, setting of performance goals, project planning, and stakeholder/employee notification and buy-in. This is frequently achieved by developing a business case for reengineering via benchmarking, identifying external customer needs and cost-benefit analysis.

2.5.3 Diagnose—This stage is classified as the documentation of the existing process and its subprocesses in terms of process attributes, such as activities, resources, communication, roles, IS and cost. In identifying process requirements and assigning customers value, root causes for problems surface and nonvalue-adding activities are identified.

2.5.4 Redesign—In the redesign stage, a new process design is developed. This is accomplished by devising process design alternatives through brainstorming and creativity techniques. The new design should meet strategic objectives and fit with the human resource and IS architectures. Documentation and prototyping of the new process is typically conducted, and a design of new information systems to support the new process is completed.

2.5.5 Reconstruct—This stage relies heavily on change management techniques to provide reasonable assurance of a smooth migration to new process responsibilities and human resource roles. During this stage, the IT platform and systems are implemented and the users go through training and transition.

2.5.6 Evaluate—The last stage of a BPR methodology requires monitoring of the new process to determine if it met its goals and often involves linkage to a total quality program.

2.6 BPR Tools

2.6.1 The availability of appropriate BPR tools that help in reducing BPR risks can greatly benefit organisations that undertake BPR. Given an existing or a new business process, a typical BPR tool supports its modeling, analysis and evaluation, and the simulation of its probable behaviour.

2.6.2 As the diagnostic phase (2.5.3) is considered the key for the identification of performance improvement opportunities and obstacles, BPR tools play an important role in the BPR project. They should be also reviewed by the IS auditor.

2.7 IS Role in the BPR

2.7.1 IS delivers tools and plays four distinct roles within BPR projects.

2.7.2 IS enables new processes. IS may help to devise innovative business processes, which would otherwise not be attainable. IS can be the key enabler of BPR. The use of IT challenges the assumptions inherent in the work processes that have existed since long before the advent of modern IT applications. Although BPR can have its roots in IS management, it is primarily a business initiative that has broad consequences in terms of satisfying the needs of customers and the organisation's other constituents.

2.7.3 IT tools help to facilitate project management. Project management tools help to analyse processes and define new processes. They can also be used to define the introduction of process-oriented application software packages.

2.7.4 IS lets people work together more closely. Special software systems, such as e-mail, groupware, workflow-management and teleconferencing, are elements of the pervasive role IS is taking.

2.7.5 IS helps to integrate businesses. The process view of businesses includes the integration of business processes within an organisation and also among business partners. ERP systems are totally integrated and help to enforce the reengineering process, by concentrating on the BPR implementation process.

2.8 Risks of BPR Projects

2.8.1 Radically improved business processes may satisfy customer requirements better than before and achieve drastic improvements to the operational results of an organisation. However, the dramatic improvements do not come without risks and a high rate of failure. The benefits of reengineering do not necessarily come in due time. That means that BPR projects must be carefully monitored during the life cycle of the project.

2.8.2 At each step of the change process (design, implementation and operational/rollout) problems related to sponsorship, scope, organisational culture, leadership, skills, human resources and management can arise. Examples of the types of problems are summarised as follows.

2.8.3 Design risks include the following:

- Sponsorship issues
  - CEO not supportive
  - Insufficient top management commitment
  - Management skepticism
  - Wrong executive leading the effort
  - Wrong members on the design team
  - Poor communication of importance
- Scope issues
  - Unrelated to strategic vision
  - Scope too narrow or too ambitious
  - Sacred cows protected
  - Existing jobs protected
  - Analysis paralysis
- Skill issues
  - Insufficient exploration of new ideas
  - Absence of out-of-the-box thinking
  - Closed to new ideas
  - Design misconceptions
  - Cultural change not calibrated to organisation
  - Inadequate consideration of human resource issues
  - Beyond the ability of IS department to support
- Political issues
  - Sabotage by managers losing power
  - Sniping
  - Uncontrolled rumors
  - Fear of change
  - Cultural resistance

2.8.4 Implementation risks include the following:

- Leadership issues
  - Insufficient attention, commitment or clout by top management
  - Ownership struggle
  - CEO/sponsor's political will wavers or falters
  - Switch in CEO/sponsor
  - Inadequate resources
  - Failure to communicate compelling vision
  - Failure of CEO to unify management behind effort
- Technical issues
  - Beyond the capability of IT to build
  - Delayed software implementation
  - Capability of packaged software insufficient
  - Functional and design requirement problems
  - Key issues not initially identified
  - Complexity underestimated
  - Unanticipated scope change
  - Time consuming or costly development strategies
- Transition issues
  - Loss of key personnel from design phase
  - Loss of momentum
  - Staff burnout
- Scope issues
  - Slower than expected results
  - Budget overruns
  - Unrealistic time frames
  - Narrowing of original scope
  - Neglect of human resource issues
  - Magnitude of effort overwhelming

2.8.5 Operational/roll out risks include the following:

- Cultural/human resource issues
  - Cultural resistance increases
  - Dysfunctional behaviour does not diminish
  - Lack of buy in leads to erosion of projected benefits
  - Training insufficient or unsuccessful
  - Outcomes not as promised or generally understood
- Management issues
  - Unsuccessful implementation of new management skills
  - No provision for ongoing continuous improvement activities
  - Ownership/turf/power issues not satisfactorily resolved
  - Insufficient will to overcome problems encountered
  - Poor communication
  - Active or passive sabotage by employees and managers
- Technical issues
  - Support late and/or flawed
  - Operational problems with systems/software bugs
  - Systems do not meet user needs/expectations
  - Inadequate testing
  - Data integrity problems undermine confidence

3. AUDIT CHARTER

3.1 Modifications for BPR Projects

3.1.1 The audit charter of the IS audit function may need to be modified as a result of an organisation's decision to implement BPR projects. BPR considerations require the IS auditor's scope of work or relationships with other audit functions (such as, financial and operational) to be expanded and more closely integrated.

3.1.2 It is imperative that the organisation's senior and system management fully understand and support the IS auditor's role(s) as it relates to BPR project. The IS Auditing Guideline G5 Audit Charter should be reviewed and considered within the context of the BPR projects and related initiatives of the organisation.

4. INDEPENDENCE

4.1 IS Audit Roles in BPR Projects

4.1.1 If the IS auditor is to perform or be responsible for nonaudit roles associated with BPR projects, IS Auditing Guideline G17 Effect of Nonaudit Role on the IS Auditor's Independence should be reviewed and adhered to appropriately.

4.1.2 If the IS auditor is to have a nonaudit role in BPR project, the IS auditor should also review and appropriately adhere to ISACA's Standards of Information Systems Control Professionals.

4.1.3 The reason for this is because there is a substantial likelihood that the IS auditor's independence will be compromised. More specifically, the IS auditor should refuse the review of systems, procedures or processes that have been subjected to a BPR and in which he/she was part of the BPR team.

5. COMPETENCE

5.1 Required Business Knowledge and Technical Skill

5.1.1 IS auditors can play a critical role in the reengineering of core business processes due to their knowledge of systems and controls, even though they have to reengineer their skills and audit approach because much of what IS auditors were accustomed to find in the processes is affected or disappears due to the radical changes of BPR.

5.1.2 In the auditing of a BPR project, the IS auditor is ordinarily a component of the audit team where he/she complements the skills of other auditors in the financial, operational and regulatory areas with his/her skill in the IS areas. However, the IS auditor should ensure that he/she has the necessary business knowledge to review the BPR project. The IS auditor also should provide reasonable assurance he/she has access to the relevant technical skill and knowledge to carry out the review of the BPR project.

6. PLANNING

6.1 Framework for Consideration by the IS Auditor When Reviewing a BPR Project

6.1.1 The initiate and diagnose phases are when the existing processes, the information and the IT systems currently in use are analysed and compared with other systems via benchmarking. At this time, for each of the processes chosen for investigation, the IS auditor can measure the relevant current performance variables and identify the performance gaps. As the use of information and IT can be the levers for dramatic changes in the organisation processes, the IS auditor can provide useful contributions from the early stages of the BPR process.

6.1.2 The redesign phase is when the new processes are redesigned, and new information or new ways to use existing information are searched, the blueprint of the new business system is defined, the migration strategy is developed and the migration action plan is created. The to-be model of the new workflow, how the new information is to be shared across functional areas of the business, the transformation of the IT systems, how new information and new technologies will be introduced, and how old information and IT systems are discarded, how reliable will be the new control system, can all be reviewed by the IS auditor.

6.1.3 The evaluate phase is when the new processes and IS systems are operating. It is a specific task of the IS auditor to determine if the BPR project has met its goals, the transition to the new structure is effective and reliable, and a total quality program has been activated.

7. PERFORMANCE OF AUDIT WORK

7.1 Risk Management Assessment

7.1.1 As reengineering is inherently highly situational and creative—there is no right way to do it—and there are several BPR procedures in the literature. An audit of a BPR project can not be one of compliance to a methodology but the assessment of risk management and how bottom-line improvements in outcomes, which are important to customers and stakeholders, are achieved.

8. REPORTING

8.1 Report Content

8.1.1 In BPR reviews, reporting should be performed progressively as and when risks and issues are identified. These reports should be addressed to the appropriate management for necessary action. A final report listing all issues raised during the review can be issued.

8.1.2 Depending on the type of review, the report should address aspects such as:

- Appropriateness of the BPR approach model and methodology
- Risks and issues, their causes and effects
- Possible risk mitigation actions
- Cost/benefit comparison and effect on the organisation's environment

9. EFFECTIVE DATE

9.1 This guideline is effective for all information systems audits beginning on or after 1 July 2004. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

.

G26 Business Process Reengineering (BPR) Project Reviews cont.

APPENDIX

Reference Literature

- Carter, M.; R. Handfield; *Identifying Sources of Cycle-time Reduction, Reengineering for Time-based Competition*, Quorum Books, 1994
- Hammer, M.; J. Champy; *Reengineering the Corporation: A Manifesto for Business Revolution*, Harper-Collins, USA, 1993
- Harrington, H.J.; *Business Process Improvement*, McGraw-Hill, USA, 1991

BPR Tools and Techniques

A number of tools and techniques have been specifically developed to capture and present process knowledge, while others are already existing tools and techniques considered useful in reengineering studies. Different views of the same process may all help to understand it in some way, but ordinarily they do not enhance the necessary innovative thinking. Tools and techniques can be broadly classified into the following categories:

- Soft systems methods—These are qualitative/brainstorming techniques for formalising the thought process, and are often used in:
  - Setting process/system goals
  - Problem analysis, for example, to identify causes of process failure (such as, cause and effect diagram)
  - Risk analysis
- Presentation tools—These are techniques for presentation of process views to understand and communicate the current process or the proposed future process. Examples are:
  - Role activity diagrams to view the dependency of individuals/teams/departments within the process
  - Process flow diagrams to view the activity dependencies
  - Functional decomposition models, useful for viewing information dependency
  - Time-based process mapping to present decomposition of process lead time into value-added and nonvalue-added components at various stages in the process
- Analysis tools—These are tools that can be used to analyse process behavior over time. Various tools exist with different levels of modeling capability, such as PERT/CPM, Petri Nets and Discrete Event Simulation.

The IS auditor should be aware of the risk of an overemphasis on modeling the as-is process—that can become a substitute for actual decisions.

COBIT Reference

Selection of the most relevant material in COBIT, applicable to the scope of the particular audit, is based on the choice of specific COBIT IT processes and consideration of COBIT information criteria.

The procedure links to the following primary COBIT processes:

- M1 Monitor the Processes
- M2 Assess Internal Control Adequacy
- DS1 Define and Manage Service Levels
- DS10 Manage Problems and Incidents
- AI6 Manage Changes
- PO1 Define a Strategic IT Plan
- PO9 Assess Risks
- PO10 Manage Projects

The procedure links to the following COBIT processes:

- PO4 Define the IT Organisation and Relationships
- PO5 Manage the IT Investment
- PO6 Communicate Management Aims and Direction
- PO7 Manage Human Resources
- PO11 Manage Quality
- DS3 Manage Performance and Capacity
- DS7 Educate and Train Users
- DS13 Manage Operations

The information criteria most relevant to a BPR audit are:

- Effectiveness
- Efficiency
- Compliance
- Reliability of Information

G27 Mobile Computing

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S1 Audit Charter states, “The purpose, responsibility, authority and accountability of the information systems audit function or information system audit assignments should be appropriately documented in an audit charter or engagement letter.”

1.1.2 Standard S4 Professional Competence states, “The IS auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment.”

1.1.3 Standard S5 Planning states, “The IS auditor should plan the information systems audit coverage to address the audit objectives and comply with applicable laws and professional auditing standards.”

1.1.4 Standard S6 Performance of Audit Work states, “IS audit staff should be supervised to provide assurance that audit objectives are accomplished and applicable professional auditing standards are met”.

1.1.5 Procedure P8, Security Assessment—Penetration Testing and Vulnerability Analysis includes detailed steps when performing specific tests.

1.2 Linkage to CobiT

1.2.1 CobiT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."

1.2.2 CobiT *Management Guidelines* provides a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.3.1 Management Guidelines provides example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

1.3.2 Management Guidelines can be used to support self-assessment workshops, and they can also be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.3.3 CobiT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT information criteria.

1.3.4 Refer to the CobiT reference located in the appendix of this document for the specific objectives or processes of CobiT that should be considered when reviewing the area addressed by this guidance.

1.2 Need for Guideline

1.3.5 Mobile and wireless computing is a phenomenon that has begun to draw significant attention in worldwide business operations. Mobile and wireless computing refers to the use of wireless communication technologies to access network-based applications and information from a wide range of mobile devices. The increasing use of this technology and the proliferation of new portable devices with Internet browsing capabilities expand the physical frontiers of organisations and requires the IS auditor to understand this technology to identify the associated risks.

1.3.2 This guideline provides guidance in applying IS auditing standards S1, S4 and S5 when mobile computing security is to be reviewed as a part of an audit assignment or as an independent review. The IS auditor should consider this guideline in determining how to achieve implementation of the above standards, use professional judgment in its application and be prepared to justify any departure.

2. DEFINITIONS

2.1 Wireless Computing

2.1.1 The term wireless computing refers to the ability of computing devices to communicate in a form to establish a local area network without cabling infrastructure (wireless), and involves those technologies converging around IEEE 802.11x and other wireless standards and radio band services used by mobile devices.

2.2 Mobile Computing

2.2.1 The term mobile computing extends this concept to devices that enable new kinds of applications and expand an enterprise network to reach places in circumstances that could never have been done by other means. It is comprised of PDAs, cellular phones, laptops and other mobile and mobile-enabled technologies.

2.3 Usage

2.3.1 As devices that have computing and storage capability, mobile devices can be used to store, process and access applications and data in various ways. They can be used as semi-independent devices that process data in an independent form and periodically connect to a central system or a network to exchange data or applications with other systems, or they can be used as client nodes that access and/or update data stored in another remote system on a real-time basis (they may act as peers as well as in a hierarchy).

2.4 Approach

2.4.1 Mobile devices are computers that are ultimately formed by common components, such as hardware, operating system, applications and communications/connectivity links. This document covers those specific topics associated with an audit/review of the use of a device for mobile computing purposes. The inherent risks associated with the equipment and the rest of the environment are not covered in this document. (Examples of risk areas not covered are firewall configuration, viruses and program maintenance.)

3. TERMS OF REFERENCE

3.1 Scope

3.1.1 The IS auditor should have a clear statement of the objectives and scope of the audit to be performed in regards to mobile computing, which are ordinarily documented in an engagement letter.

4. PLANNING

4.1 Information Gathering

4.1.1 The IS auditor should obtain the security policy that rules the acceptable use of mobile devices.

4.1.2 The IS auditor should obtain information about the intended use of mobile devices, identifying where they are used for business transaction and data processing and/or for personal productivity purposes (i.e., Internet browsing, mail, calendar, address book, to-do list) and about hardware and software technologies used. Key processes—automated and manual—should be documented.

4.1.3 The IS auditor should obtain sufficient information about the risk analysis, along with the likelihood of occurrence and probable impact of the event, performed by the entity to evaluate the impacts of its mobile computing environment.

4.1.4 The IS auditor should obtain sufficient information about the policies and procedures used to manage mobile computing, involving deployment, operation and maintenance of aspects, such as communications, hardware, application software, data security, systems software and security software. Examples of areas to cover are device configuration, physical control, approved software and tools, application security, network security, contingency plans, backup and recovery.

4.1.5 Personal interviews, documentation analysis (such as business case and protocols documentation) and wireless infrastructure testing should be used appropriately in gathering, analysing and interpreting the data.

4.1.6 Where third-party organisations are used to outsource IS or business functions, the IS auditor should review the terms of the agreement, evaluating the appropriateness of the security measures they enforce and the right of the organisation to periodically review the environment of the third party involved in the service it provides.

4.1.7 The IS auditor should also review previous examination reports and consider their results in the planning process.

4.2 Risk Analysis

4.2.1 The IS auditor should consider the risks associated with the use of mobile devices and relate them to the criticality of the information they store and access and the transactions they process, from the business, law and regulatory perspectives.

4.2.2 The portability, capability, connectivity and affordability of mobile devices enables them to be used to process applications that increase risks, such as:

- Damage, loss or theft (due to its portability)
- Damage to network assets by the transfer of viruses, worms, etc. from the mobile device.
- Unauthorised access to data by downloading data from corporate devices or networks (due to its connectivity)
- Unauthorised changes or additions to data by uploading data to corporate devices or networks
- Unauthorised access to data/applications that reside in the device (due to the simplicity of its operating systems that ordinarily include only very basic security functions)

4.2.3 Topics to consider when performing the risk analysis include:

- Privacy—An important component when sensitive information (such as, credit card numbers, financial details and patient records) is transmitted. Privacy protocols and related procedures are very important as wireless transmissions cannot be protected from hacker access by other means (such as physical access controls).
- Authentication—Can be ensured by using a token or certificate that can be verified by a recognised certification authority (CA)
- Two-factor authentication—Used to verify both the device and the identity of the end user during a secure transaction (i.e., confirms that both the device and the user are authorised agents). Two-factor authentication is used to deny network access from stolen or lost devices.
- Data integrity—Involves the detection of any change to the content of a message during the transmission or while stored on the mobile device

- Nonrepudiation—A system to prevent users from denying they processed a transaction. Nonrepudiation requires a successful user authentication, and establishes a credible and legally enforceable record of the user that originated a transaction.
- Confidentiality and encryption—Involves transformation of data using algorithms to avoid unauthorised users or devices that could eventually read and understand it (see IS Auditong Procedure P9 Evaluation of Management Controls Over Encryption Methodologies). Encryption technologies rely on keys to encode and decipher pieces of data during transmission. Procedures for key distribution and safekeeping should also be considered.
- Unauthorised use of equipment and communications, including the risk of using unauthorised access to the Internet to break into a third-party's networks (subjecting the entity to potential legal liability)

4.2.4 The IS auditor should assess the probability that the risks identified will materialise together with their likely effect, and document the risks along with the controls that mitigate these risks. Depending on the scope of the review, the IS auditor should include the most likely sources of threats—internal as well as external sources—such as hackers, competitors and alien governments.

4.3 IS Audit Objectives

4.3.1 According to the objectives and scope of the audit, the IS auditor should include in his/her review security areas, such as:

- Communications (covering risks such as sniffing and denial-of-service, and protocols such as encryption technologies and fault tolerance)
- Network architecture
- Virtual private networks
- Application delivery
- Security awareness
- User administration
- User and session administration (covering risk such as hijacking, spoofing, loss of integrity of data)
- Physical security
- Public key infrastructure
- Backup and recovery procedures
- Operations (such as incident response and back-office processing)
- Technology architecture (such as feasible, expandable to accommodate business needs and usable)
- Security architecture.
- Security software (such as IDS, firewall and antivirus)
- Security administration.
- Patch deployment
- Business contingency planning

4.4 Work Plan

4.4.1 Based on the information obtained and the scope and objectives of the engagement, the IS auditor has to document the way business, security and IS objectives (when applicable) are affected by the identified risks and controls that mitigate those risks.

4.4.2 In this process the IS auditor should evaluate areas of weakness or vulnerabilities that need strengthening. New controls identified as mitigating the risks considered should be included in a work plan for testing purposes.

5. PERFORMANCE OF AUDIT WORK

Execution

In the event of a lack of controls, the IS auditor should consider extending the planned procedures (for example including a penetration test) to identify the real vulnerabilities of the environment and test if they have not impacted on the objectives of the audit.

Reporting

5.2.1 The IS auditor should provide a report in an appropriate form to the intended service user recipients upon the completion of the audit work.

5.2.2 The IS auditor should consider discussing the report with the appropriate stakeholders prior to release.

5.2.3 The report should specify any restrictions on distribution that the IS auditor or management agree to impose. The IS auditor should also consider including a statement excluding liability to third parties.

6. EFFECTIVE DATE

6.1 This guideline is effective for all information systems audits beginning on or after 1 September 2004. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary*.

APPENDIX

CobiT Reference
Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT information criteria:

Primary
PO9—Assess Risks
AI3—Acquire and Maintain Technology Architecture
AI4—Develop and Maintain IT Procedures
AI5—Install and Accredit Systems
AI6—Manage Changes
DS5—Ensure Systems Security
DS9—Manage the Configuration
M2—Assess Internal Control Adequacy

Secondary
AI2—Acquire and Maintain Application Software
DS8—Assist and Advise IT Customers

The CobiT information criteria are confidentiality, integrity and availability, efficiency and reliability.

G28 Computer Forensics

1. BACKGROUND

1.1 Linkage to ISACA Standards

1.1.1 Standard S3 Professional Ethics and Standards states, “The IS auditor should adhere to the ISACA Code of Professional Ethics in conducting audit assignments.”

1.1.2 Standard S3 Professional Ethics and Standards states, “The IS auditor should exercise due professional care, including observance of applicable professional auditing standards in conducting audit assignments.”

1.1.3 Standard S4 Professional Competence states, "The IS auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment."

1.1.4 Standard S5 Planning states, “The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards.”

1.1.5 Standard S6 Performance of Audit Work states, “During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.”

1.2 Linkage to COBIT®

1.2.1 COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management should establish an adequate system of internal control."

1.2.2 COBIT *Management Guidelines* provides a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 *Management Guidelines* provides example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

1.2.4 *Management Guidelines* can be used to support self-assessment workshops, and it can also be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes, control objectives, associated management control practices and consideration of relevant COBIT information criteria.

1.2.6 Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

1.3 Need for Guideline

1.3.1 The IS auditor is often requested to advise on frauds or irregularities made using computer or telecommunication systems (computer crime) and to check organisation compliance with computer-related laws or regulations. A basic understanding of computer forensics is necessary to help the organisation detect or prevent such irregularities. This document is intended to assist the IS auditor in achieving this purpose.

1.3.2 The foremost aim of computer forensics is to establish the truth behind a particular situation by immediately capturing data to identify an attacker and establish proof for criminal proceedings to aid law enforcement. It also aids the organisation in protecting the information assets from future attacks and in gaining an understanding about an attacker and attacks. The main characteristics are:

- Emphasise the need to immediately respond or evidence will be lost/tampered.
- Capture and preserve data as close to the breach as possible.
- Forensically preserve evidence for potential admission in court.
- Minimally invasive data capture process without disruption to business operations
- Identify an attacker and establish proof.

1.3.3 During the conduct of computer investigation, it is critical that confidentiality is maintained and integrity is established for data and information gathered and made available to appropriate authorities only. The IS auditor will play a crucial role in such instances and may help the organisation by indicating whether legal advice is advisable and which technical aspects of the IS environment need appropriate investigation. There may be instances were the IS auditor may be given information about a suspected irregularity or illegal act and may be requested to use data analysis capabilities to gather further information.

1.3.4 Computer forensics has been applied in a number of areas including, but not limited to, fraud, espionage, murder, blackmail, computer misuses, technology abuse, libel, malicious mails, information leakage, theft of intellectual property, pornography, spamming, hacking and illegal transfer of funds. Computer forensics involves the detailed analysis of events in cyberspace and collection of evidence. This guideline briefly describes the elements of computer forensics with the aim to aid the IS auditor in considering such aspects warranted by a situation during the conduct of the assignment. The IS auditor should also communicate the need for computer forensics for Internal investigations, which make up a large percentage of forensic investigations (vs. external attacks):

- Whistle-blower complaints
- HR investigations
- Fraud investigations
- Compliance investigations—enforce compliance to various legal mandates and industry guidelines (e.g., Sarbanes-Oxley, NIST, FISMA)

1.3.5 This guideline provides guidance in applying IS auditing standards S3, Professional Ethics and Standards; S4 Professional Competence; S5 Planning; S6 Performance of Audit Work, while conducting a computer forensic review. The IS auditor should consider it in determining how to achieve implementation of the above standards, use professional judgment in its application and be prepared to justify any departure.

1.4 Guideline Application

1.4.1 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA guidelines.

1.4.2 The IS auditor should consult and apply jurisdictional legal investigation guidelines, if applicable, during a computer forensic engagement.

2. DEFINITIONS

2.1 Computer Forensics

2.1.1 Computer forensics can be defined as the process of extracting information and data from computer storage media using court-validated tools and technology and proven forensic best practices to establish its accuracy and reliability for the purpose of reporting on the same as evidence.

2.1.2 The challenge to computer forensics is actually finding this data, collecting it, preserving it and presenting it in a readable manner that is acceptable in a court of law.

2.1.3 Computer forensics primarily involves exploration and application of scientifically proven methods to gather, process, interpret and utilise digital evidence to support an assertion, such as:

- Provide a conclusive investigation of all activities for the purpose of complete attack verification and enterprise and critical infrastructure information restoration
- Correlate, interpret and predict adversarial actions and their effect on planned operations
- Make digital data suitable and persuasive for introduction into a criminal investigative process

2.1.4 Computer forensics is a science as well as an art for extracting and gathering data from a computer to determine if and how an abuse or intrusion has occurred, when it occurred and who was the intruder. Organisations that employ good security practices and maintain appropriate logs are able to achieve the objectives easily. However, with the right knowledge and tools, forensic evidence can be extracted even from burned, water-logged or physically damaged computer systems.

3. AUDIT CHARTER

3.1 Assignment Mandate

3.1.1 Prior to commencement of the assignment pertaining to computer forensics, the IS auditor should require a clear, written mandate from the appropriate authority to conduct the assignment.

3.1.2 The mandate should specify the responsibilities, authority and limitations of the assignment and ensure independence of the IS auditor in carrying out the assignment. It should also make it clear that the auditor is acting with lawful authority to access the systems and data concerned.

3.1.3 The mandate should also specify the scope and responsibilities where an external expert is utilised by the IS auditor to carry out the assignment.

4. INDEPENDENCE

4.1 Considerations of Independence

4.1.1 Prior to commencing the assignment pertaining to computer forensics, the IS auditor should provide reasonable assurance that there are no possible conflicts of interest.

4.1.2 Where a computer forensic assignment has been initiated by government, statutory body or any authority under a law, the IS auditor must clearly communicate the independence and authority to perform the task, maintain confidentiality on information acquired, be unbiased and submit a report to appropriate authorities.

5. AUDIT CONSIDERATIONS

5.1 Judicial Validity of an Electronic Transaction

5.1.1 To be considered valid, a contract involving selling goods or services should be signed. For electronic contracts, this can be achieved with a digital signature.

5.1.2 The digital signature can achieve the objective of juridical relevance as follows:

- Authentication—There is evidence of data provenience.
- Integrity—The verification process will succeed only if none of the message has been changed.

- Nonrepudiation or paternity—Each key user has the legal responsibility to protect his/her key. Therefore, he/she cannot repudiate or unilaterally modify the content of the signed document. A valid system used to protect the private key might possibly store it in a secure personal device, such a smart card. Is it possible to deny someone's own digital signature? Even if it would be considered admissible, the negation has no value. The other party should only have to demonstrate that the signature was valid when the contract was signed. This means that the owner must prove that his/her private key was stolen or subjected to unauthorised use before the time the contract was signed. The digital signature authenticated by a notary cannot be denied.
- Confidentiality—To add confidentiality to a signed document, it is only necessary to encrypt it using the addressee's public key.

5.2 Identification of Parties and Transaction Content

5.2.1 Only people of legal age (ordinarily 18 years old or more in most jurisdictions) have the capacity to conclude a contract.

5.2.2 Merchants can utilise any means to prove to themselves that the other party is legally authorised to make a transaction. They can request any kind of proof and proceed to store the buyer's data in their archives. In case of error or misuse, the vendor is ultimately responsible for the proper execution of the contract. When using a digital signature system, the responsibility resides with the authority that issued the digital signature. This authority is called a certification authority (CA). If contested, the digital certificate owner should demonstrate if the private key was stolen or misused.

5.2.3 The same considerations apply to the content of the transaction (integrity), which is preserved when using the digital signature system. Otherwise the merchant is responsible for false, incomplete, ambiguous and erroneous data.

5.2.4 The merchant is always responsible for credit card frauds and privacy violation.

5.3 Location Where the Contract Is Concluded

5.3.1 The greatest problem regarding electronic commerce is determining the exact location where the contract is concluded, which determines the legal jurisdiction and the applicable laws and regulations.

5.3.2 In the absence of a specific law applicable to a contract, the only alternative is to refer it to the international jurisdiction. Modern technology allows anyone to connect to his/her service provider from virtually everywhere in the world. This results in the impossibility of defining the exact location where the contract concludes.

5.3.3 The solution is the proper application of international law and consequent application of international agreements.[2]

5.3.4 The most accepted approach states that:

- If the parties have chosen a specific legislation, this is the only legislation that is applicable
- If the parties have not chosen any legislation scheme, the one with the closest relationship to the contract (i.e., residence of the service provider) or, in case of product selling, the law of the consumer's country is applicable

5.3.5 In any case, it is imperative that every kind of prudence is exercised, as it is extremely difficult to determine (and prove) the location of the merchant.

5.4 Category Distinction

5.4.1 The intrinsic characteristic of informatics, regardless of the modalities of conclusion of the contract, is to qualify the acquirer as a consumer because legislation protects the consumer in every country. For this reason, there is a distinction between business-to-business and business-to-consumer electronic commerce.

5.5 Fraud Prevention

5.5.1 The economic system is founded from one side on identification and nonrepudiation of proposals/acceptances, and from the other side on establishing fund transfers reasonably secure both when a subject buys (which implies he/she wants to receive services or a goods) and when the subject sells (which implies he/she wants to receive payment). The digital signature system appears today as the only statutory form of payment online.

5.6 Use of Credit Cards Over the Internet

5.6.1 Today, the credit card constitutes the most utilised payment instrument for transactions over the Internet. Unfortunately there are many possibilities for abuse of credit card data (such as allowing the reproduction of these data online). For example, there is a possibility that the transaction receipt could be read by someone unauthorised to do so.

5.6.2 For online transactions, it is not necessary to have a credit card, but only its data. Credit card crimes are committed simply using card data in an unauthorised manner. There are three types of credit card crime:

- Abuse of card data
- Falsification and possession of false credit card
- Selling or buying an illegal card

5.6.3 The illegal use of a credit card over the Internet includes any action aimed to fraudulently obtain money, goods or services using card data. A crime is committed even when the owner uses the card after its expiration.

---

[2] The Rome Convention, 1980 European law, *www.rome-convention.org/instruments/i_conv_cons_it.htm* and the Vienna Convention, an international agreement regarding import/export of goods signed in 1980, *www.cisg.law.pace.edu/cisg/biblio/volken.html.*

6. KEY ELEMENTS OF COMPUTER FORENSICS FOR AUDIT PLANNING

6.1 Data Protection

6.1.1 It is critical that measures are in place to prevent the sought information from being destroyed, corrupted or becoming unavailable.

6.1.2 It is also important to inform appropriate parties that electronic evidence will be sought through discovery from the computer systems, setting out specific protocols requiring all parties to preserve electronic evidence and to not resort to any means of destroying information.

6.1.3 Response and forensic investigation capability should be in place prior to an incident or event. This includes the infrastructure and processes for incident response and handling.

6.2 Data Acquisition

6.2.1 This involves the process of transferring information and data into a controlled location.

6.2.2 This includes the collection of all types of electronic media, such as disk drives, tape drives, floppy disks, backup tapes, zip drives and any other types of removable media. All media should protected with content (image) being transferred to another medium by an approved method. In addition it is important to check that the media are virus-free and write-protected.

6.2.3 Data and information are also acquired through recorded statements of witnesses and other related parties.

6.2.4 The capture of volatile data, including open ports, open files, active processes, user logons and other data in RAM, are critical in many cases. Volatile data are transient and lost when a computer is shut down. The capture of volatile data assists the investigators in determining what is currently happening on a system

6.3 Imaging

6.3.1 This involves the bit-for-bit copy of seized data for the purposes of providing an indelible facsimile upon which multiple analyses may be performed without fear of damaging the original data or information.

6.3.2 Imaging is made to capture the residual data of the target drive. An image copy duplicates the disk surface sector by sector as opposed to a file-by-file copy that does not capture residual data. Residual data include deleted files, fragments of deleted files and other data that are still existent on the disk surface. With appropriate tools, destroyed data (erased, even by re-formatting the media) can also be recovered from the disk surface.

6.4 Extraction

6.4.1 This involves the identification and separation of potentially useful data from the imaged dataset. This includes the recovery of damaged, corrupted or destroyed data, or data that have been tampered with to prevent detection.

6.4.2 The entire process of imaging and extraction must meet standards of quality, integrity and reliability. This includes the software used to create the image and the media on which the image was made. A good benchmark would be whether the software is used, relied upon or authorised by law enforcement agencies. The copies and evidence must be capable of independent verification, i.e., the opponent and court must be convinced about the accuracy and reliability of the data, and that the data is tamper proof.

6.4.3 Extraction includes examination of many sources of data, such as system logs, firewall logs, intrusion detection system logs, audit trails and network management information.

6.5 Interrogation

6.5.1 This involves the querying of extracted data to determine if any prior indicators or relationships, such as telephone numbers, IP addresses and names of individuals, exist in the data.

6.5.2 Accurate analyses of the extracted data are essential to make recommendations and prepare appropriate grounds of evidence before the enforcement authorities.

6.6 Ingestion/Normalisation

6.6.1 This involves the transfer and storage of extracted data using appropriate techniques and in a format easily understood by investigators. This may include the conversion of hexadecimal or binary information into readable characters, conversion of data to another ASCII language set, or conversion to a format suitable for data analysis tools.

6.6.2 Possible relationships within data are extrapolated through techniques, such as fusion, correlation, graphing, mapping or time lining, to develop investigative hypotheses.

7. REPORTING

7.1 Acceptable to Law

7.1.1 As stated earlier, the challenge to computer forensics is finding the data, collecting it, preserving it and presenting it in a manner acceptable to a court of law. The IS auditor should have complete information and clarity on the intended recipients and the purpose of the report.

7.1.2 The report should be in an appropriate form and should state the scope, objectives, nature, timing and extent of investigation performed.

7.1.3 The report should identify the organisation, intended recipients and restrictions on circulation (if any). The report should clearly communicate the findings, conclusions and recommendations, together with any reservations or qualifications that the IS auditor has with respect to the assignment.

7.2 Evidence

7.2.1 Electronic evidence ranges from mainframe computers and pocket-sized personal data assistant to floppy diskettes, CDs, tapes or even the smallest electronic chip device.

7.2.2 Industry-specified best practices should be adhered to, proven tools should be utilized and due diligence should be exhibited to provide reasonable assurance that evidence is not tampered with or destroyed. Integrity, reliability and confidentiality of the evidence is absolutely necessary for arriving at a fair judgment by the law enforcement authorities. It is also critical that the evidence is produced and made available at an appropriate time to the authorities.

7.2.3 Example of tracing Internet e-mail:

- When an Internet e-mail message is sent, the user typically controls only the recipient line(s) (To and Bcc) and the subject line.
- Mail software adds the rest of the header information as it is processed. An example of an e-mail header follows:

```
      ----- Message header follows -----
(1)   Return-path: <sasrock@o199632.cc.nps.gov.org>
(2)   Received: from o199632.cc.navy.gov by nps.gov.org (5.1/SMI-5.1) id AAO979O; Fri, 7 Nov 2003 18:51:49 PST
(3)   Received: from localhost byo199632.gov.org (5.1/SMI-5.1) id AA41651; Fri 7 Nov 2003 18:50:53 PST
(4)   Message-ID: <9611080150.AA16514@o199632.cc.navy.gov>
(5)   Date: Fri, 7 Nov 2003 18:50:53 -0800 (PST)
(6)   From: "Susan Rock" <sasrock@o199632.cc.nps.gov.org>
(7)   To: Mott Thick <mott.thick@ocean.com>
(8)   Cc: Jokey Ram<J.ram@seabeas.com>
```

- Line 1 tells recipient computers who sent the message and where to send error messages (bounces and warning).
- Lines 2 and 3 show the route the message took from sending to delivery. Each computer that receives this message adds a received field with its complete address and time stamp; this helps in tracking delivery problems.
- Line 4 is the message ID, a unique identifier for this specific message. This ID is logged and can be traced through computers on the message route if there is a need to track the mail.
- Line 5 shows the date, time and time zone when the message was sent.
- Line 6 tells the name and e-mail address of the message originator (the sender).
- Line 7 shows the name and e-mail address of the primary recipient; the address may be for a:
  - Mailing list
  - System-wide alias
  - Personal username
- Line 8 lists the names and e-mail addresses of the courtesy copy (Cc) recipients of the message. There may be blind carbon copy (Bcc) recipients as well; these Bcc recipients get copies of the message, but their names and addresses are not visible in the headers.

8. EFFECTIVE DATE

8.1 This guideline is effective for all information system audits beginning on or after 1 September 2004. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

APPENDIX

COBIT Reference

Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. In the review of computer forensics, the COBIT processes likely to be the most relevant are classified below as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

Primary:

- PO8—Ensure compliance with external requirements
- AI1—Identify automated solutions
- DS1—Define and manage service levels
- DS2—Manage third-party service
- DS5—Ensure security systems
- DS10—Manage problems and incidents
- DS11—Manage data
- M1—Monitor the process

G28 Computer Forensics cont.

- M3—Obtain independent assurance

Secondary:

- PO1—Define a strategic IT plan
- PO4—Define the IT organisation and relationships
- DS6—Identify and allocate costs
- DS12—Manage facilities
- DS13—Manage operations
- M2—Assess internal control adequacy

The information criteria most relevant to a computer forensic review are:

- Primary—Reliability, integrity and compliance
- Secondary—Confidentiality and availability

G29 Post-implementation Review

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, “During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

1.1.2 Standard S8 Follow-up Activities states, “After the reporting of findings and recommendations, the IS auditor should request and evaluate relevant information to conclude whether appropriate action has been taken by management in a timely manner.”

1.2 Linkage to COBIT

1.2.1 High-level control objective M4, Provide for Independent Audit, states, “Control over the IT process of providing for independent audit that satisfies the business requirement to increase confidence levels and benefit from best practice advice is enabled by independent audits carried out at regular intervals and takes into consideration:

- Audit independence
- Proactive audit involvement
- Performance of audits by qualified personnel
- Clearance of findings and recommendations
- Follow-up activities
- Impact assessments of audit recommendations (costs, benefits and risks)

1.2.2 Detailed control objective M4.6, Performance of Audit Work, states, “Audits should be appropriately supervised to provide assurance that audit objectives are achieved and applicable professional auditing standards are met. Auditors should ensure that they obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions should be supported by appropriate analysis and interpretation of the evidence.”

1.3 Reference to COBIT

1.3.1 The COBIT references offer the specific objectives or processes of COBIT to consider when reviewing the area addressed by this guidance. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT’s information criteria.

1.3.2 In a post-implementation review, the first review after the implementation of an IT solution, the following processes are more relevant:

- PO2—Define the Information Architecture
- PO4—Define the IT organisation and relationship
- PO5—Manage the IT investment
- PO8—Ensure Compliance with External Requirements
- PO9—Assess risks
- PO10—Manage projects
- PO11—Manage quality
- AI1—Identify automated solutions
- AI2—Acquire and maintain application software
- AI3—Acquire and maintain technology infrastructure
- AI5—Install and accredit systems
- AI6—Manage changes
- DS7—Educate and Train Users
- DS11—Manage Data
- M1—Monitor the processes

1.3.3 The information criteria most relevant to the post-implementation review are:

- Primary—Effectiveness and efficiency
- Secondary—Availability, compliance, confidentiality, reliability and integrity

1.3.4 International Federation of Accountants (IFAC) Information Technology Committee (ITC) Guidelines includes:

- Implementation of Information Technology Solutions
- Managing Information Technology Planning For Business Impact

1.4 Purpose of the Guideline

1.4.1 The purpose of this guideline is to describe the recommended practices in carrying out the post-implementation review of information technology solutions, so that the relevant standards for information systems auditing are complied with during the course of the review.

1.4.2 Organisations implement various IT solutions to meet their business requirements. Once the solutions are implemented, post-implementation reviews are generally carried out by IS auditors to assess the effectiveness and efficiency of the IT solutions and their implementation, initiate actions to improve the solution (where necessary) and serve as a learning tool for the future.

1.4.3 Certain practices recommended in this guideline may also be appropriate for reviews of projects where implementations are unsuccessful or aborted prior to implementation.

1.4.4 This guideline provides guidance in applying IS Auditing Standards S6 Performance of Audit Work and S8 Follow-up Activities while conducting a post-implementation review. The IS auditor should consider it in determining how to achieve implementation of these standards, use professional judgment in its application and be prepared to justify any departure.

1.5 Guideline Application

1.5.1 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA guidelines

1.6 Definition and General Coverage

1.6.1 Post-implementation review, for the purpose of this guideline, means the **first or subsequent review** of an **IT solution** and/or the process of its implementation, performed after its implementation, to assess any or all of the following:

- Whether the intended objectives of the solution are realised
- Whether actual costs and benefits are compared against budget
- The effectiveness and appropriateness of the implementation process
- Causes of time and/or cost overruns, and quality and/or performance issues, if any
- Productivity and performance improvements resulting from the solution
- Whether business process and internal controls are implemented
- Whether user access controls are implemented in accordance with organisational policy
- Whether users have been appropriately trained
- Whether the system is maintainable and can be further developed effectively and efficiently
- Whether available features and procedures, as relevant, have been implemented
- Compliance with relevant statutory requirements and organisational policies, as relevant
- Compliance with COBIT *Control Objectives* and COBIT *Management Guidelines*, as relevant
- Opportunities for further improvement in either the solution or implementation process

1.6.2 The objectives of a post-implementation review might include:

- Ensure that the intended objectives of implementing the IT solution are met and aligned to meet the business objectives of the organisation
- Evaluate the adequacy of procedures and controls over input, processing and output to ensure that information captured is complete and accurate, information processing complies with required business rules, and information generated is accurate, reliable and timely
- Evaluate the adequacy of procedures and controls over the maintenance and monitoring of the management trail produced by the IT solution
- Verify the accuracy of financial and management reports generated by the IT solution
- Ensure the adequacy of application-level access control enforced by the IT solution
- Verify the adequacy of availability features inherent in the IT solution to recover from any unexpected shutdowns and maintain data integrity
- Ensure that the IT solution can be supported and maintained efficiently and effectively in the absence of the specific personnel responsible for its development and implementation
- Identify potential risks and weakness in controls, as well as provide solutions to mitigate risks and strengthen controls

1.6.3 The post-implementation review essentially seeks to determine whether the investment in the IT solution was worthwhile (as determined and measurable by the organisation) and whether the delivered IT solution can be adequately managed and controlled. These investment returns can be covered as a unique, separate review often called a benefits realisation review (section 8.1). The scope of a post-implementation review should consider:

- The nature of the IT solution
- The intended usage of the IT solution (for what purpose, who by whom, when and where)
- The criticality of the IT solution in achieving business objectives
- The scope of the review agreed with the auditee (organisation) management
- Whether the IT solution was subject to audit review during the initiation, development and testing stage
- Where there has been any non-audit involvement of IS auditors during the project implementation

2. AUDIT CHARTER

2.1 Mandate

2.1.1 Before commencing a post-implementation review, the IS auditor should have the requisite mandate to carry out the review. Where the review is initiated by a third party, the IS auditor should obtain reasonable assurance that the third party has the appropriate authority to commission the review.

3. INDEPENDENCE

3.1 Professional Objectivity

3.1.1 Before accepting the assignment, the IS auditor should provide reasonable assurance that his/her interest, if any, in the IT solution that is the subject of the post-implementation review will not impair the objectivity of the review. Any possible conflict of interest should be communicated explicitly to the organisation, and if possible, a written statement of the organisation's awareness of the conflict should be obtained before accepting the assignment.

3.1.2 Where the IS auditor had any non-audit roles in the implementation of the IT solution being reviewed, the IS auditor should consider guideline G17 Effect of Nonaudit Roles on the IS Auditor's Independence which provides guidance.

4. PROFESSIONAL ETHICS AND STANDARDS

4.1 Pre- and Post-implementation Reviews

4.1.1 As compared to a pre-implementation review, post-implementation review is ordinarily performed when the IT solution has been in operation for a reasonable period (ordinarily a number of months or process cycles) and user procedures, as well as application-level securities, have been implemented.

4.1.2 Pre-implementation reviews examine the conceptual design of controls and management trails, or how they operate in test environments. Post-implementation reviews examine how controls and management trails are operating once the IT solution is installed, configured and operating in the production environment. Where a pre-implementation review has been performed satisfactorily, the IS auditor should use his/her discretion whether to limit the post-implementation review to examine actual operation of the system in production.

4.1.3 Where resources are available, It is preferable to perform it is preferable for both pre-implementation and post-implementation and post-implementation reviews to be performed, since last-minute changes can be made prior to actual implementation of the IT solution, if resources are available,.

4.1.4 When carrying out a post-implementation review the IS auditor should provide reasonable assurance that the project owner responsible for implementing the IT solution and the project team is involved in the review process. Team members consulted as part of the review should typically include:

- People connected with the design, development and deployment of the IT solution
- People with working knowledge of the area under review, and current and proposed business processes
- People with relevant technical knowledge
- People with knowledge of the organisation's business strategy and the proposed contribution of the IT solution to the achievement of the strategy
- People involved in the measurement and monitoring of the benefits realisation process

5. COMPETENCE

5.1 Skills and Knowledge

5.1.1 The IS auditor also should provide reasonable assurance that he/she possess the relevant skills and knowledge to carry out the post-implementation review of the IT solution. Where expert input is necessary, appropriate input should be obtained

6. PLANNING

6.1 Scope and Objectives of the Review

6.1.1 The IS auditor, in consultation with the organisation as appropriate, should clearly define the scope and objectives of the Post Implementation Review. The aspects to be covered by the review should be stated explicitly as part of the scope.

6.1.2 For the purpose of the review, the stakeholders in the implementation should be identified.

6.1.3 The findings and conclusions of any prior reviews of the IT solution or implementation process—pre-implementation or concurrent reviews—should be considered in determining the scope and in audit planning.

6.2 Sign-off for the Terms of Reference

6.2.1 Depending on the organisational practices, the IS auditor should obtain the concurrence of the relevant parties in the organisation for the terms of reference and the approach. If the review is being initiated by a third party, they should also agree to the terms of reference.

6.3 Approach

6.3.1 The IS auditor should formulate the approach to provide reasonable assurance that the scope and objectives of the review can be fulfilled in an objective and professional manner. The approach should be appropriately documented. The use of expert input should be specified as part of the approach. Post-implementation reviews are not limited to the first review after implementation of the IT solution. Multiple reviews may be performed to identify improvements in the implemented solution.

7. PERFORMANCE OF AUDIT WORK

7.1 Execution of Post-Implementation Review

7.1.1 A post-implementation review should be scheduled at a reasonable time after the IT solution has been implemented. Typical periods can range from four weeks to six months, depending upon the type of solution and its environment.

7.1.2 A post-implementation review is intended to be an assessment and review of the final working IT solution. Ideally, there should have been at least one full implementation and reporting cycle completed to perform a proper review. The review should not be performed while still dealing with initial issues and teething troubles, or while still training, and educating users. However, where possible, the review should be performed while the opportunity remains to incorporate final improvements to derive optimum benefit from the IT solution.

7.1.3 Review procedures should include the study of available documentation (such as business case, business requirements including business controls, feasibility study, system, operational and user documentation, progress reports, minutes of meetings, cost/benefit reports, testing and training plans and scripts, etc.), discussions with stakeholders, hands-on experimentation and familiarisation with the IT solution, observation and inquiry of business and project personnel, and examination of operational and control documentation.

7.1.4 Appropriate resources to carry out the post-implementation review should be identified and allocated, and the performance of the review should be planned in conjunction with relevant auditee personnel.

7.1.5 Agreement should be reached regarding the format, content, audience and timing, where possible, of reporting the results of the post-implementation review.

7.1.6 The stated objectives of the IT solution, costs and benefits should be studied in detail. The extent of achievement of the objectives and actual costs and benefits should be evaluated together with the processes and systems used to capture, monitor and report performance, costs and benefits. As part of this exercise, the productivity/performance improvements delivered by the IT solution should also be studied. Suitable measurement criteria should be used in this context. The cost and/or time overrun, if any, should be analysed by reference to their causes and their effects. Controllable and uncontrollable causes should be identified separately.

7.1.7 The process followed for defining and implementing the IT solution should be evaluated with reference to its appropriateness, as well as its effectiveness.

7.1.8 The adequacy and effectiveness of education and training provided to users and staff supporting the IT solution should be reviewed.

7.1.9 The reports of any prior reviews performed either internally or by external reviewers on a pre-implementation basis or concurrently with the implementation process should be studied, and the status of recommendations and actions taken verified.

7.1.10 Since the post-implementation review is examining an IT solution, in general, the IT solution should satisfy appropriate COBIT control objectives. The extent of compliance with relevant control objectives and the effect of noncompliance should be analysed and reported. Further, critical success factors, key goal indicators, key performance indicators and maturity model benchmarks from COBIT *Management Guidelines* should be adapted as appropriate for the IT solution and implementation process being reviewed.

7.1.11 Appropriate management trails should be maintained for the data gathered, analysis made, inferences arrived at as well as corrective actions recommended.

7.1.12 The extent of compliance with statutory and regulatory requirements and organisational policies and standards of the IT solution and implementation process should be reviewed.

7.1.13 Where appropriate, automated testing tools and CAATs may be used to test relevant aspects of the IT solution.

7.1.14 The review should highlight risks and issues for necessary corrective action, together with opportunities for improvement in controls or increased effectiveness of the implementation process.

7.1.15 Reported findings, conclusions and recommendations should be based on an objective analysis and interpretation of the information and evidence obtained during the post-implementation review.

8. BENEFITS REALISATION REVIEWS

8.1 Benefits Realisation Review

8.1.1 All IT projects are actually business projects and should have a business rationale from the outset. Their success or failure should be measured either in financial terms or as a contribution to achievement of the strategic business plan. Benefits realisation reviews should focus not only on what has been achieved but what remains to be done. Organisations that undertake benefits realisation reviews to fine tune best practices and learn lessons reap benefits when their next project is undertaken.

8.2 Benefits Realisation Review Objectives

8.2.1 The objectives of a benefits realisation review are to evaluate the operational success of the new IT solution, and to assess the actual costs, benefits and savings in comparison with budgeted amounts. The review may also examine the effectiveness of the process used to deliver and implement the IT solution. A key consideration is whether or not the original system objectives and schedules have been achieved. This requires a detailed understanding of as-is and to-be processes, to assess the extent to which the objectives of the to-be processes have been achieved.

8.2.2 The benefits realisation component of a post-implementation review report should address:

- Actual costs compared to budgeted costs
- Actual benefits compared to budgeted benefits
- Return on investment
- Actual savings compared to budgeted savings
- Actual project completion dates compared to planned completion dates
- Original objectives compared to accomplished objectives

- Assessment of the adequacy and quality of documentation and controls, including management trails
- Actual IT solution performance compared to anticipated performance
- Overall user satisfaction and understanding of the new IT solution system
- Performance improvement suggestions for future IT solution implementation projects

9. OUTSOURCING

9.1 Outsourcing of IT

9.1.1 Where the organisation has partially or fully delegated some or all of its IT solution implementation to an external provider of such services (the service provider), the IS auditor should assess the effect of such arrangements and review the adequacy of, and conformance/compliance with, contracts, agreements and regulations with the service provider.

9.1.2 The IS auditor should obtain an understanding of the nature, timing and extent of the outsourced services. Also, the IS auditor should establish what controls the service user has put in place to address the business requirements and controls required by the organisation (refer to guideline G4 Outsourcing of IS Activities to Other Organisations.

10. REPORTING

10.1 Report Content

10.1.1 The report on the post-implementation review should address the following aspects depending on the objectives and scope of the review:

- The scope, objectives, methodology followed and assumptions made
- Assessment of whether the intended objectives of implementing the IT solution has been met, and whether the IT Solutions are aligned to meet the business objectives.
- An overall assessment of the implementation process in terms of key strengths and weaknesses as well as the likely effects of the weaknesses
- Recommendations to overcome the significant weaknesses and to improve the implementation process
- Potential risks and means to mitigate such risks
- The extent of compliance with CobiT's information criteria
- Recommendations to improve future IT solutions and implementation processes
- Training of the users on the IT solution implemented
- Acceptance and adaptability of the IT solutions across the organisations

10.1.2 The observations and recommendations should be validated with the stakeholders and organisation (and service provider if applicable), as appropriate, and responses obtained before finalising the report.

10.2 Weaknesses

10.2.1 Weaknesses identified during the post-implementation review, either due to lack of controls, poor implementation processes or nonmitigation of associated risks to acceptable levels, should be brought to the attention of the business process owner and to IS management responsible for the implementation of the IT solution. Where weaknesses identified during the post-implementation review are considered to be significant or material, the appropriate level of management should be advised immediately to allow early corrective action.

10.2.2 Since effective controls over IT solutions are dependent on general IT controls, any weaknesses in these areas should also be reported. In the event that general IT controls are not examined, this fact should be included in the report.

10.2.3 The IS auditor should include appropriate recommendations in the report to strengthen controls to mitigate associated risks.

11. FOLLOW-UP ACTIVITIES

11.1 Timeliness

11.1.1 The effects of any weaknesses identified by the post-implementation review are likely to be wide-ranging and high-risk. Therefore, the IS auditor should carry out, where appropriate, sufficient, timely follow-up work to verify that management action is taken to address weaknesses and manage risk effectively.

12. EFFECTIVE DATE

12.1 This guideline is effective for all information systems audits beginning 1 January 2005. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

Reference

IS Auditing Guideline G23 System Development Life Cycle (SDLC) Review

G30 Competence

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S4 Professional Competence states, "The IS auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment. The IS auditor should maintain professional competence through appropriate continuing professional education and training."

1.2 Linkage to COBIT

1.2.1 High-level control objective M3 (Obtain Independent Assurance) states, "…obtaining independent assurance to increase confidence and trust amongst the organisations, customers and third-party providers."

1.2.2 High-level control objective M4 (Provide for Independent Audit) states, "…providing for independent audit to increase confidence levels and benefit from best practice advice."

1.2.3 Detailed control objective M3.7 (Competence of Independent Assurance Function) states, "Management should ensure that the independent assurance function possesses the technical competence, skills and knowledge necessary to perform such reviews in an effective, efficient and economical manner."

1.2.4 Detailed control objective M4.4 (Competence) states, "Management should ensure that the auditors responsible for the review of the organisation's IT activities are technically competent and collectively possess the skills and knowledge (i.e., CISA domains) necessary to perform such reviews in an effective, efficient and economical manner. Management should ensure that audit staff assigned to information systems auditing tasks maintain technical competence through appropriate continuing professional education".

1.3 COBIT Reference

1.3.1 The COBIT references offer the specific objectives or processes of COBIT to consider when reviewing the area addressed by this guidance. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the requirement, the processes in COBIT likely to be the most relevant are selected and adapted and are classified below as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 Primary:

- PO7—Manage Human Resources
- M2—Assess Internal Control Adequacy
- M3—Obtain Independent Assurance
- M4—Provide for Independent Audit

1.3.3 Secondary:

- DS1—Define and Manage Service Levels
- DS2—Manage Third Party Services
- DS3—Manage Performance and Capacity
- DS7—Educate and Train Users
- M1—Monitor the Process

1.3.4 The information criteria most relevant to competence are:

- Primary: effectiveness, efficiency and availability
- Secondary: confidentiality, integrity, compliance and reliability

1.4 Purpose of the Guideline

1.4.1 IS auditors are expected to be highly competent. To meet this objective, IS auditors need to acquire the necessary skills and required knowledge to carry out assignments. The additional challenge is to maintain competence by continually upgrading knowledge and skills.

1.4.2 By agreeing to provide professional services, IS auditors imply the availability of the desired level of competence required to perform professional services and that the knowledge and skill of the IS auditor will be applied with due care and diligence.

1.4.3 In view of the expectations of high competence, IS auditors should refrain from performing any services that they are not competent to carry out unless advice and assistance is obtained to provide reasonable assurance that the services are performed satisfactorily.

1.4.4 The IS auditor should perform professional services with due care, competence and diligence and has a continuing duty to maintain professional knowledge and skill at a required level to provide reasonable assurance that the requirements of professional auditing standards are met and the audited organisation receives the advantage of competent professional service based on up-to-date developments in practice, legislation and techniques.

1.4.5 ISACA's stated vision is to be the recognised global leader in IT governance, control and assurance. In the preface to the vision, it is clearly amplified that future success in the professions served by ISACA will require skills and competencies complementary to those measured by the CISA designation. ISACA is in the forefront of identifying these skills and competencies and devising ways to quantify and assess them. It is in this context that there is a need for a guideline to provide guidance to IS auditors to acquire necessary skills and knowledge and maintain competence while carrying out audit assignments.

1.4.6 This guideline provides guidance in applying IS Auditing Standard S4 Professional Competence. The IS auditor should consider this guideline in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

1.5 Guideline Application

1.5.1 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards and guidelines.

2. RESPONSIBILITY

2.1 Skills and Knowledge

2.1.1 Primarily, the IS auditor should be responsible for acquiring the required professional and technical skills and knowledge to carry out any assignment the IS auditor agrees to perform.

2.1.2 Audit management has the secondary responsibility to entrust the audit assignment after ensuring that the IS auditor possesses the required professional and technical skills and knowledge to perform the tasks.

2.1.3 Audit management is responsible for ensuring that the team members performing the audit have the requisite skills and knowledge.

2.1.4 Skills and knowledge vary with the IS auditor's position and the role with respect to the audit. Requirement for management skills and knowledge should be commensurate with the level of responsibility

2.1.5 Skills and knowledge include proficiency in the identification and management of risks and controls, as well as audit tools and techniques. The IS auditor should possess analytical and technical knowledge together with interviewing, interpersonal and presentation skills.

2.2. Competence

2.2.1 Competence implies possessing skills and knowledge, and expertise through an adequate level of education and experience.

2.2.2 The IS auditor should provide reasonalble assurance that he/she possesses the skills and knowledge necessary to attain the required level of competence.

2.2.3 The IS auditor should design the desired and/or expected level of competence based on appropriate benchmarks and such benchmarks are periodically reviewed and updated.

2.2.4 IS auditor and/or audit management should provide reasonable assurance of the availability of competent resources required to carry out any audit assignment prior to accepting the assignment/engagement, and the availability of such competent resources should be confirmed/ensured prior to commencement of an audit.

2.2.5 Audit management is responsible for ensuring the team members are competent to perform the audit assignment. Identification of core competencies of team members will assist in efficient utilisation of available resources.

2.2.6 It is considered appropriate for the IS auditors to share their experiences, adopted best practices, lessons learned and knowledge gained amongst team members to improve the competence of the resources. The competence of team members is also improved through team building sessions, workshops, conferences, seminars, lectures and other modes of interaction.

2.3 Continual Maintenance

2.3.1 The IS auditor should continually monitor their skills and knowledge to maintain the acceptable level of competence.

2.3.2 Maintenance through continuing professional education (CPE) may include, and is not limited to, training, educational courses, certification programmes, university courses, conferences, seminars, workshops, teleconferences, web casts and study circle meetings.

2.3.3 Acquiring skills and knowledge and maintaining competence levels should be monitored on a continual basis, and such skills, knowledge and competence should be evaluated periodically.

2.4 Evaluation

2.4.1 Evaluation should be carried out in a manner that is fair, transparent, easily understood, unambiguous, without bias and considered a generally acceptable practice given the respective employment environment.

2.4.2 Evaluation criteria and procedures should be clearly defined, but may vary depending upon circumstances such as geographic location, political climate, nature of assignment, culture and other similar circumstances.

2.4.3 In the case of an audit firm or a team of auditors, evaluation should be carried out internally amongst teams or individuals on a cross-functional basis.

2.4.4 In the case of a single (sole) independent IS auditor, evaluation should be carried out by a peer relationship to the extent possible. If a peer review is not possible, self-evaluation should be conducted and documented.

2.4.5 An appropriate level of management is required to evaluate the performance of the internal IS auditor and also, wherever appropriate and necessary, the performance of external IS auditor(s).

2.4.6 Gaps noted during evaluation should be addressed appropriately.

2.5 Gap Analysis and Training

2.5.1 Gaps noted based upon variances in the actual level of competence to the expected level of competence should be recorded and analysed. Where deficiency exists in any resource, such resources should not be utilised to conduct the audit assignment unless adequate measures to rectify the deficiency are undertaken. However, if the deficiency is noticed after commencement of the audit assignment, the IS auditor/audit management should consider withdrawing the deficient resource(s) and replacing it with a competent resource. However due to compulsions, if it is proposed to continue to use the resource for the continuance of the audit assignment, the existence of the gap should be communicated to the auditee. The concurrence of the auditee should be obtained for the continued use of the deficient resource, provided that the IS auditor is able to reasonably assure the quality of the audit.

2.5.2 It is important that the root cause analysis is performed to ascertain the reason for the gap and that appropriate corrective action measures, such as training, are conducted as soon as possible.

2.5.3 Training activities required for an audit engagement should be completed within a reasonable time and before commencement of the audit activity.

2.5.4 Effectiveness of training should be measured on completion of training after a reasonable time period.

2.6 Availability of Competent Resources

2.6.1 The IS auditor/audit management should understand and analyse the requirement of skills and knowledge of the proposed audit assignment, before responding to a request for proposal.

2.6.2 The IS auditor/audit management should provide reasonable assurance that requisite resources with the necessary skills, knowledge and required level of competency are available before commencing the audit assignments.

2.6.3 IS auditors should not portray themselves as having expertise, competence or experience they do not possess.

2.7 Outsourcing

2.7.1 Where any part of the audit assignment is outsourced or expert assistance obtained, it must be reasonable assurance must be provided that the external expert or the outsourced agency possesses the requisite competence. This guideline also applies for selection of an external expert.

2.7.2 Where expert assistance is obtained on a continual basis, competencies of such external experts should be measured and monitored/reviewed periodically.

3. CONTINUING PROFESSIONAL EDUCATION

3.1 Requirements of Professional Bodies

3.1.1 Continuing professional education (CPE) is the methodology adopted to maintain competence and update skills and knowledge.

3.1.2 IS auditors should adhere to the requirements of the CPE policies established by the respective professional bodies with which they are associated.

3.2 Eligible Programmes

3.2.1 CPE programmes should aid in the enhancement of skill and knowledge and must relate to professional and technical requirements of IS assurance, security and governance

3.2.2 Professional bodies ordinarily prescribe programmes eligible for CPE recognition. IS auditors should adhere to such norms prescribed by their respective professional bodies.

3.3 Attainment of CPE credits

3.3.1 Professional bodies ordinarily prescribe the methodology of attainment of CPE credits and the minimum credits that should be obtained periodically by their constituents. IS auditors must adhere to such norms prescribed by their respective professional bodies.

3.3.2 Where the IS auditor is associated with more than one professional body for the purpose of attainment of minimum credits, the IS auditor may use his/her judgement to avail CPE credits in a common manner from the eligible programmes, provided the same is consistent with the rules/guidelines framed by the respective professional bodies.

3.4 ISACA's CPE Policy

3.4.1 ISACA has a comprehensive policy on continuing professional education, applicable to its members and holders of the CISA designation. IS auditors with the CISA designation must comply with ISACA's **CPE policy**. Details of the policy are available on the ISACA web site, *www.isaca.org/CISAcpePolicy*. The policy explains the criteria for:

- Certification requirements
- Verification of attendance form
- Code of Professional Ethics
- Audits of continuing professional education hours
- Revocation, reconsideration and appeal
- Retired and nonpracticing CISA status
- Qualifying educational activities
- Calculating continuing professional education hours

4. RECORDS

4.1 Skill Matrix and Training Records

4.1.1 A skill matrix indicating the skill, knowledge and competence required for various job levels should be formulated. This matrix is cross-referenced to the available resources and their skill and knowledge. This matrix will aid in the identification of gaps and training needs.

4.1.2 Records of training provided, together with feedback on training and effectiveness of training, should be maintained, analysed and referenced for future use.

4.2 CPE Records

4.2.1 As prescribed by respective professional bodies, including ISACA, IS auditors are required to maintain appropriate records of CPE programmes, retain them for specific periods and, if required, make them available for audits.

5. EFFECTIVE DATE

5.1 This guideline is effective for all information systems audits beginning 1 June 2005. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

G31 Privacy

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S1 Audit Charter states, "The purpose, responsibility, authority and accountability of the information systems audit function or information systems audit assignments should be appropriately documented in an audit charter or engagement letter."

1.1.2 Standard S5 Planning states, "The IS auditor should plan the information systems audit coverage to address the audit objectives and comply with applicable laws and professional auditing standards."

1.1.3 Standard S6 Performance of Audit Work states, "During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

1.2 Linkage to COBIT

1.2.1 High-level control objective PO8, Ensure compliance with external requirements, states, "Control over the IT process of ensuring compliance with external requirements that satisfies the business requirement to meet legal, regulatory and contractual obligations is enabled by identifying and analysing external requirements for their impact, and taking appropriate measures to comply with them and takes into consideration:

- Laws, regulations and contracts
- Monitoring legal and regulatory developments
- Regular monitoring for compliance
- Safety and ergonomics
- Privacy
- Intellectual Property"

1.2.2 Detailed control objective PO8.4, Privacy, intellectual property and data flow states, "Management should ensure compliance with privacy, intellectual property, transborder data flow and cryptographic regulations applicable to the IT practices of the organisation."

1.3 Reference to COBIT

1.3.1 The COBIT reference for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IS processes and consideration of COBIT control objectives and associated management practices. In a privacy issue, the processes in COBIT likely the most relevant to be selected and adapted are classified as primary and secondary in the following list. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 Primary:

- PO8—Ensure compliance with external requirements
- DS5—Ensure systems security

1.3.3 Secondary:

- PO7—Manage Human Resources
- DS1—Define and manage service levels
- DS2—Manage third-party services.
- DS10—Manage problems and incidents
- DS11—Manage data
- DS13—Manage operations
- M1—Monitor The process
- M2—Access internal control adequacy
- M3—Obtain independent assurance
- M4—Provide for independent audit

1.3.4 The information criteria most relevant to a privacy review are:

- Primary—Effectiveness, compliance, confidentiality and integrity.
- Secondary—Reliability and availability.

1.4 Purpose of the Guideline

1.4.1 The purpose of this guideline is to assist the IS auditor to appreciate privacy and appropriately address the privacy issues in carrying out the IS audit function. This guideline is aimed primarily at the IS audit function; however, aspects could be considered for other circumstances.

1.4.2 This guideline provides guidance in applying IS Auditing Standards. The IS auditor should consider it in determining how to achieve implementation of the above standard, use professional judgment in its application and be prepared to justify any departure.

1.5 Guideline Application

1.5.1 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards and guidelines.

1.6 Definition of Privacy in an IS Auditing Context—Limits and Responsibilities

1.6.1 Privacy means adherence to trust and obligation in relation to any information relating to an identified or identifiable individual (data subject). Management is responsible to comply with privacy in accordance with its privacy policy or applicable privacy laws and regulations.

1.6.2 Personal data is any information relating to an identified or identifiable individual.

1.6.3 The IS auditor is not responsible for what is stored in the personal databases, he/she should check whether personal data are correctly managed with respect to legal prescriptions by adoption of the correct security measures.

1.6.4 The IS auditor should review management's privacy policy to ascertain that it takes into consideration the requirements of applicable privacy laws and regulations including transborder data flow requirements, such as Safe Harbor and OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (see reference section).

1.6.5 IS auditors should review the privacy impact analysis or assessment carried out by management. Such assessments should:

- Identify the nature of personally identifiable information associated with business processes
- Document the collection, use, disclosure and destruction of personally identifiable information
- Provide management with a tool to make informed policy, operations and system design decisions based on an understanding of privacy risk and the options available for mitigating that risk
- Provide reasonable assurance that accountability for privacy issues exists
- Create a consistent format and structured process for analysing both technical and legal compliance with relevant regulations
- Reduce revisions and retrofit the information systems for privacy compliance
- Provide a framework to ensure that privacy is considered starting from the conceptual and requirements analysis stage to the final design approval, funding, implementation and communication stage

1.6.6 IS auditors should determine whether these assessments are conducted as part of an initial privacy review and on an ongoing basis for any change management project, such as:

- Changes in technology
- New programs or major changes in existing programs
- Additional system linkages
- Enhanced accessibility
- Business process reengineering
- Data warehousing
- New products, services, systems, operations, vendors and business partners

1.6.7 In assessing applicable privacy laws and regulations that need to be complied with by any particular organisation, particularly for organisations operating in different parts of the globe, IS auditors should seek an expert opinion as to the requirement of any laws and regulations and should carry out the necessary compliance and substantive tests to form an opinion and report on the compliance of such laws and regulations.

1.6.8 Data controller is a party who is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.

2. AUDIT CHARTER

2.1 Privacy in the Connected World

2.1.1 The advancement of communication technology such as the World Wide Web and electronic mail allows the efficient dissemination of information on a global scale. Controls should be in place to ensure the ethical use of this technology and the projection of electronic/digitalised and hard copy personal information. Furthermore, the global promulgation of legislation requires that organisations implement controls to protect individual privacy. This guideline provides a common set of criteria that the IS auditor can apply to assess the effectiveness of security controls designed to ensure personal privacy.

3. INDEPENDENCE

3.1 Sources of Information

3.1.1 The auditor should consider local regulations about privacy and, after that, global regulations that the organisation is adopting. If the organisation is international, it should consider that local regulations take precedent over enterprise policies, but in this case, the organisation additionally must comply with both (i.e., Sarbanes Oxley for EEUU companies).

4. PROFESIONAL ETHICS AND STANDARDS

4.1 Need for Personal Data Protection

4.1.1 An increasing number of connections between internal and external registries/data sources and use of the Internet increases the need for privacy in both public and private enterprises. Information regarding life, health, economy, sexual predilection, religion, political opinion, etc., may, if exposed to unentitled people, cause irretrievable harm for individuals.

4.1.2 Laws and regulations regarding privacy exist in many countries, but these are often not well known or specific enough. Therefore, an IS auditor must have a basic knowledge of privacy matters and, when necessary, be aware of the basic differences between various countries' regulations to evaluate the level of protection regarding personal information in an enterprise.

5. COMPETENCE

5.1 Approach for Personal Data Protection

5.1.1 There must be requirements and rules for treating digitalised and hard copy personal information to secure confidentiality, integrity and availability of personal information. Every organisation must have an approach for protecting all types and forms of personal information and should consider:

- Privacy management—The chief executive officer or the person in charge of the organisation should have the primary responsibility for privacy. The objective and superior guidelines for the use of personal information should be described in security objectives/policy and strategy. There should be formalised routines for frequent evaluation to provide reasonable assurance that use of personal information is compliant with the needs of the organisation and public rules and regulations. The results of the evaluation should be documented and used as the basis for possible change in security policy and strategy.
- Risk assessment—The organisation should have an overview of the various kinds of personal information in use. The organisation must also determine the criteria for acceptable risk connected to treatment of personal information. The responsibility for personal information should be attached to a “data controller.” The data controller is responsible for execution of risk assessments to identify probability for, and consequences of, security incidents. New risk assessments should be carried out according to changes of significance for information security. The result of the risk assessments should be documented.
- Security audit—Security audit regarding use of information systems should be carried out on a regular basis. Security audit should encompass the organisation, security efforts and cooperation with partners and vendors. The results should be documented.
- Deviation—Any use of information systems that is not compliant with formalised routines and which may cause security breaches should be treated as a deviation. The objective of deviation treatment is to reestablish normal conditions, remove the cause that lead to the deviation and prevent recurrence. If deviations have caused unauthorised release of confidential information, the local authorities may need to be notified. The results should be documented.
- Organisation—Responsibility for use of the information systems should be established and documented. The responsibility should be unchangeable without authorisation from appropriate management. The information system should be configured to achieve satisfactory information security. Configuration should be documented and only changed with authorisation from appropriate management.
- Staff—Employees should use personal information according to their tasks and have the necessary authorisation. Furthermore, employees should have the necessary knowledge to use the information system according to formalised routines. Authorised use of information systems should be registered.
- Professional secrecy—Employees should sign a formal agreement to not disclose any kind of personal information where confidentiality is necessary. This professional secrecy should also encompass other information of importance for information security.
- Physical security—The organisation should implement measures to prevent unauthorised access to technical equipment in use to process personal information. Security measures should also encompass other equipment of importance for information security. Equipment should be installed in a way that does not affect the treatment of personal information.
- Confidentiality—The enterprise should take measures to prevent unauthorised access to personal information where confidentiality is necessary. Security measures should also prevent unauthorised access to other information of importance for information security. Confidential personal information that is being transferred electronically to external partners should be encrypted or secured in another manner. Stored information containing confidential personal information should be marked appropriately.
- Integrity—Measures should be taken against unauthorised change of personal information to provide reasonable assurance of integrity. Security measures should also prevent unauthorised changes of other information of importance for information security. Furthermore, measures should be taken against malicious software.
- Availability—Measures should be taken to provide reasonable assurance of access to personal information. Security measures should also encompass other information of importance for information security. Backup and recovery routines should be in place to provide reasonable assurance of access to information in situations when normal operations fail. Proper backup routines should be established.
- Security measures—Security measures should be in place to prevent unauthorised use of information systems and make it possible to discover unauthorised access attempts. All unauthorised access attempts should be logged.

- Security measures should encompass efforts that can not be influenced or bypassed by staff, and should not be limited to legal actions taken against individuals. Security measures should be documented.
- Security toward external partners—The data controller is responsible for clarifying responsibility and authority toward external partners and vendors. Responsibility and authority should be formalised in a written document. The data controller must have proper knowledge about the security strategy of partners and vendors, and on a regular basis ensure that the strategy gives satisfactory information security.
- Documentation—Routines for use of information systems and other information of relevance for information security should be documented. Documentation should be stored according to national laws and regulations. Incident logs from information systems should be stored for at least three months. Policy, standards and procedures should be deployed to specify approved use of personal information.
- Awareness and training sessions—These should be implemented to communicate the privacy policy to employees and providers, especially to those persons handling the personal information of customers (i.e., customer service).

6. PLANNING

6.1 Overview of Privacy Laws in Various Countries Principles and Main Differences

6.1.1 Most countries have already issued their own privacy regulations. The principles are basically the same, but with significant differences in terms of definition of personal data, basic security measures to adopt, etc. These differences can affect the IS auditor's role, especially when the assignment involves more than one country and/or data repositories are located in another area.

6.1.2 **Table 1** lists general principles from "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," published by the Organisation for Economic Co-operation and Development (OECD) in 1980 and revised in 2002.

Table 1—GENERAL PRINCIPLES

N°	PRINCIPLE	EXPLANATION
1	Collection limitation	The collection of personal data is possible with the (explicit) consent and knowledge of the data subject.
2	Data quality	Personal data are relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, are accurate, complete and kept up-to-date.
3	Purpose specification	The purposes for which personal data are collected, are specified not later than the time of data collection and the subsequent use is limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4	Use limitation	Personal data cannot be disclosed, made available or otherwise used for purposes other than those specified above (except with the consent of the data subject or by the authority of law).
5	Security safeguards	Personal data should be protected by reasonable security safeguards against risks, such as loss or unauthorised access, destruction, use, modification or disclosure of data.
6	Openness	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available to establish the existence and nature of personal data, the main purposes of their use, and the identity and usual residence of the data controller.
7	Individual participation 1	An individual has the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him/her.
8	Individual participation 2	An individual has the right to have communicated to him/her, data relating to him/her: • Within a reasonable time • At a charge, if any, that is not excessive • In a reasonable manner • In a form that is readily intelligible to him/her
9	Individual participation 3	An individual has the right to be given reasons if a request, such as those in principles 7 and 8, is denied, and to challenge such denial.
10	Individual participation 4	An individual has the right to challenge data relating to him/her and, if the challenge is successful, to have the data erased, rectified, completed or amended.
11	Individual participation 5	Specific procedures must be established so that the individual can communicate to the company if he/she changes his/her mind about the use and disposal of his/her personal information, and these changes must be reflected in all systems and platform where his/her data is used.
12	Accountability of data controller	The data controller is accountable for complying with measures that give effect to the principles stated above.

6.1.3 Based on the aforementioned principles, the checklist in **table 2** should help to build a comparison between various countries' regulations and represent a rough indicator of how those principles are actually applied. The "ref" column is the reference number to the principles listed in **Table 1**.

Table 2—CHECKLIST		
N°	**REF.**	**Questions**
1	1	Is collection of personal data regarding an individual, for any kind of processing, NOT possible without either the unambiguous consent of the individual or for the fulfillment of a contract with the individual or in accordance with other condition explicitly permitted by law? Except for special cases such as public security or national security, which should be done by the authority of law and authorised by an entity different from the collector.
2	1	Is consent to collecting and/or processing personal data necessary for any third party who needs to access/manipulate them (e.g., outsourcing) and must it be exploited by the data subject by written consent, distinct from the one given to the main contractor (in other words, no data controller can give access to any third party to data without unambiguous explicit authorisation of the data subject)?
3	2	Are data controllers compelled to periodically verify the accuracy of data, and to update or delete irrelevant/excessive/outdated (for the scope of processing) information?
4	3	Are data controllers compelled to communicate the scope of collecting data to the data subject(s)?
5	3	Are data controllers compelled to limit the use of data to those communicated to the data subject(s) when the data were collected?
6	3	Are data controllers compelled to communicate any change of purpose of collecting/processing data to the data subject(s) and to obtain his approval?
7	4	Are there limitations to the use of data which forbid any utilisation/disclosure not explicitly authorised by the data subject(s)?
8	5	Are there requirements about minimum security safeguards requested of the data controllers to protect data against unauthorised disclosure/utilisation?
9	5	Must data controllers prepare and periodically update a security plan?
10	5	Must data controllers periodically conduct a risk assessment?
11	5	Are there requirements that make any individual (belonging to data controller's organisation) uniquely identifiable and accountable for access to any subject(s) data?
12	6	Is the identity of the data controller (as an individual or an organisation) necessarily communicated to the data subject(s) as well as the nature of data collected/processed?
13	6	Are there any training or awareness programs in place to alert staff to the requirements of personal information protection?
14	7	Can a data subject(s) ask the data controller for information regarding the existence or nature of data pertaining him/her?
15	7	Can a data subject(s) obtain his/her data from the data controller and verify them?
16	8	Is there a maximum period of time fixed to answer questions 15 and 16? Yes, the information should be provided in a reasonable manner and ion an intelligible form.
17	9	Can a data subject(s) challenge any denial by the data controller to communicate to him/her the existence of data/processing pertaining to him/her?
18	10	Can a data subject(s) have the data pertaining him/her erased by the data controller? Yes.
19	11	Can a data subject deny at any time to anyone (even if authorised before) the consent to collect data regarding him/her?
20	12	Are there sanctions against data controllers who are not compliant to the above stated principles?
21	12	Are there organisations that have a duty to verify compliance of a data controller to the above stated principles?

7. PERFORMANCE OF AUDIT WORK

7.1 Reviewing an Organisation's Privacy Practices and Procedures

7.1.1 The IS auditor should have a good understanding of the audit planning process. An audit program should be developed including the scope, objectives and timing of the audit. Reporting arrangements should be clearly documented in the audit program.

7.1.2 Consideration should be given to the nature and size of the organisation and its stakeholders. Knowledge of transborder relationships (both within the country and internationally) is important and will help determine the scope and time required for the audit.

7.1.3 The IS auditor should gain an understanding of the organisation's mission and business objectives, the types of data collected and used by the organisation and the legislation applicable to the organisation, which may include privacy requirements. Also, an understanding of the organisational structure, including roles and responsibilities of key staff including the information managers and owners is needed.

7.1.4 A primary objective of the audit planning phase is to understand the risks to the organisation in the event of nonadherence to privacy legislation/regulations.

7.2 Steps to Perform

7.2.1 The IS auditor should conduct a preliminary privacy assessment to help determine the impact on the organisation if compliance with the relevant privacy legislation is not achieved. This helps to define the scope of the review and should also take into account factors such as the type of information collected, stored and used for various purposes within the organisation.

7.2.2 The IS auditor should determine whether the organisation has the following in place:

- Privacy policy
- Privacy officer
- Data controller

- Training and awareness plan in relation to privacy
- Privacy complaint management process
- Regime of privacy audits conducted against the privacy legislation
- Privacy requirement for outsourced and contractors

These, if available, should be assessed by the IS auditor to ensure they are in line with the relevant privacy legislation and/or regulations.

7.2.3 The IS auditor should conduct a privacy impact analysis. This involves:

- Identifying, analysing and prioritising the risks of nonadherence to privacy legislation
- Understanding the various privacy measures currently in place in the organisation
- Assessing the weaknesses and strengths
- Recommending strategies for improvement

7.2.4 A report should be written by the IS auditor that documents the results of the privacy review. The report should include an outline of the objectives and scope and provide a summary of the type of data and information collected, stored and used by the organisation.

7.2.5 The report should include information on the privacy related risks that face the organisation and a summary of the risk reduction measures or privacy protection strategies that exist.

7.2.6 Weaknesses identified in the privacy review either due to an absence of risk reduction measures or inadequate measures should be brought to the attention of the information owners and to the management responsible for the privacy policy.

7.2.7 Where weaknesses identified during the privacy review are considered to be significant or material, the appropriate level of management should be advised to undertake immediate corrective action.

7.2.8 The IS auditor should include appropriate recommendations in the audit report to provide management with opportunities to strengthen the organisation's privacy controls.

8. REPORTING

8.1 Security Measures Verification Regulations

8.1.1 Local privacy regulations may require that some security measure are in place to ensure personal data are properly protected against risks of unauthorised access, improper disclosure, modification and/or loss.

8.1.2 The following is a list of key controls to help provide reasonable assurance that local privacy requirements are satisfied. Please note that local laws or regulations can impose additional measures. The IS auditor should check the applicability and completeness of this table before starting the audit, as stated in **table 2** of section 6.1.3.

8.2 Media Reuse

8.2.1 A formal procedure to provide reasonable assurance that due care is taken by all personnel with custody of media and documentation containing personal data should exist and be verified.

8.2.2 Before reusing media (e.g., electronic/digitalised or paper) that previously contained personal data reasonable assurance should be provided that all information has been deleted. Sometimes, according to data sensitivity or media nature, it is necessary to destroy the media itself.

8.3 Training

8.3.1 Security training should be scheduled regularly for all personnel dealing with personal data.

8.4 Access Control

8.4.1 As a general principle, the "need-to-know" philosophy must be enforced (i.e., any person should be granted access only to the files and archives necessary to perform his/her work).

8.4.2 Access privileges and user IDs should be assigned according to this policy.

8.4.3 A written procedure to immediately update/delete user IDs when an employee leaves or is assigned to another department/function should exist and be verified.

8.4.4 Proper instructions regarding the use of personal computers should be provided and verified. They must include every aspect of individual data security, such as the necessity of performing regular data back-up, that workstations should not be left unattended, etc.

8.4.5 The internal network should be adequately protected by the use of security devices, such as firewalls.

8.4.6 The existence of a contingency plan to restore personal data archives within defined time limits should be verified.

8.5 Maintenance and Support

8.5.1 Every maintenance and support access should be logged and monitored.

8.6 Data Integrity

8.6.1 Reasonable assurance that the antivirus software is installed in every workstation and that it is regularly updated by subscription to the selected antivirus company should be provided.

8.6.2 The operating system and any applicable software vendors should be checked regularly for patches/updates availability.

8.6.3 Data back-up should be scheduled regularly, on servers, mainframes and personal computers.

8.7 Access Control to Facilities

8.7.1 Any person entering the organisation facilities should be registered. Employees coming to work during off-hours should sign a logbook.

8.8 Risk Analysis
8.8.1 A risk analysis aimed to identify personal data risks and exposures should be carried out on a regular basis.

9. EFFECTIVE DATE

9.1 This guideline is effective for all information systems audits beginning 1 June 2005. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

APPENDIX

References

"AICPA/CICA Privacy Framework," American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Certified Accountants (CICA), 2003
"Privacy : Assessing the Risk," The Institute of Internal Auditors (IIA) Research Foundation, April 2003
"OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," Organisation for Economic Co-operation and Development (OECD), 1980, 2002
"Guidelines for the Regulation of Computerized Personal Data Files," Office of the United Nations High Commissioner for Human Rights, 1990
"The International E-commerce Standard for Security, Privacy and Service (Business to Business)," International Standards Accreditation Board (ISAB), IES: 2000 (B2B), 2000
"The International E-commerce Standard for Security, Privacy and Service (Business to Consumer)," International Standards Accreditation Board (ISAB), IES: 2000 (B2C), 2000
"Safe Harbor Privacy Principles," US Department of Commerce, USA, 21 July 2000
"US Department of Commerce Safe Harbor," US Department of Commerce, USA, *www.export.gov/safeharbor*

G32 Business Continuity Plan (BCP) Review From IT Perspective

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, "During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

1.2 Linkage to CobiT

1.2.1 High-level control objective DS4, *Ensure continuous service*, states, "Control over the IT process of ensuring continuous service that satisfies the business requirement to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption."

1.3 Reference to CobiT

1.3.1 Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IS processes and consideration of CobiT's control objectives and associated management practices. In a BCP review from an IT perspective, the most relevant processes in CobiT are classified below as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 Primary:

- PO9—Assess risk
- AI6—Manage changes
- DS1—Define and manage service levels
- DS4—Ensure continuous service
- DS10—Manage problems and incidents
- DS11—Manage data
- DS12—Manage facilities
- DS13—Manage operations

1.3.3 Secondary:

- PO4—Define the IT organisation and relationships
- PO8—Ensure compliance with external requirements
- PO7—Manage human resources
- AI5—Install and accredit systems
- DS2—Manage third-party services
- DS5—Ensure systems security
- DS9—Manage the configuration
- M1—Monitoring the process

1.3.4 The information criteria most relevant to a BCP review are:

- Primary—Effectiveness, efficiency, availability and compliance
- Secondary—Confidentiality, integrity and reliability

1.4 Purpose of the Guideline

1.4.1 In today's interconnected economy, organisations are more vulnerable than ever to the possibility of technical difficulties disrupting business. Any disaster, from floods or fire to viruses and cyberterrorism, can affect the availability, integrity and confidentiality of information that is critical to business.

1.4.2 The primary objective of BCP is to manage the risks for an organisation in the event that all or part of its operations and/or information systems services are rendered unusable and aid the organisation to recover from the effect of such events.

1.4.3 The purpose of this guideline is to describe the recommended practices in performing a business continuity plan (BCP) review from an IT perspective.

1.4.4 The purpose of the guideline is to identify, document, test and evaluate the controls and the associated risks relating to the process of BCP, from an IT perspective, as implemented in an organisation to achieve relevant control objectives, both primary and secondary.

1.4.5 This guideline provides guidance in applying IS Auditing Standard S6 Performance of Audit Work to obtain sufficient, reliable, relevant and useful audit evidence during review of the business continuity plan from an IT perspective. The IS auditor should consider it in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

1.5 Guideline Application

1.5.1 This guideline is applied when conducting a review of BCP from an IT perspective in an organisation.

1.5.2 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards and guidelines.

1.6 Terminology

1.6.1 Acronyms:

- Business continuity plan (BCP)
- Business impact analysis (BIA)
- Disaster recovery plan (DRP)

1.6.2 Business continuity planning refers to the process of developing advance arrangements and procedures that enable an organisation to respond to an interruption in such a manner that critical business functions continue with planned levels of interruption or essential change. In simpler terms, BCP is the act of proactively strategising a method to prevent, if possible, and manage the consequences of a disaster, limiting the consequences to the extent that a business can absorb the impact.

1.6.3 The term BCP refers to the complete process of business continuity planning; it includes *inter-alia* business, technological, human and regulatory aspects.

1.6.4 The BCP defines the roles and responsibilities and identifies the critical information technology application programs, operating systems, networks, personnel, facilities, data files, hardware and time frames needed to assure high availability and system reliability based on the business impact analysis. A BCP is a comprehensive statement of consistent actions to be taken before, during and after a disaster. Ideally, BCP enables a business to continue operations in the event of a disruption and survive a disastrous interruption to critical information systems.

1.6.5 BIA involves the identification of critical business functions and workflow, determines the qualitative and quantitative impact of a disruption, and prioritises recovery time objectives (RTOs).

1.6.6 DRP, a key component of BCP, refers to the technological aspect of BCP—the advance planning and preparations necessary to minimise loss and ensure continuity of critical business functions in the event of a disaster. DRP comprises consistent actions to be undertaken prior to, during and subsequent to a disaster. A sound DRP is built from a comprehensive planning process, involving all of the enterprise business processes. Disaster recovery strategies include the use of alternate sites (hot, warm and cold sites), redundant data centres, reciprocal agreements, telecommunication links, disaster insurance, business impact analyses and legal liabilities.

2. AN OVERVIEW OF BCP FROM AN IT PERSPECTIVE

2.1 Components of BCP From IT Perspective

2.1.1 The IT component of BCP defines the response and recovery process that assures the availability of IT operations, reintegration of procedures, applications, operations, systems, data storage, networks and facilities that are critical to supporting the business process.

2.1.2 BCP components include the following:

- Identification—Identify potential threats and risks of the business.
- Prevention—Prevent or minimise the probability of the incident.
- Detection—Identify the circumstances under which the organisation determines entering contingency status.
- Declaration—Specify the conditions on which contingency is declared and identify the person(s) who can declare it.
- Escalation—Specify the conditions on which contingency is escalated and identify the person(s) and order of escalation in the event of contingency.
- Containment—Specify the immediate action required to contain or minimise the effect of the incident on customers, suppliers, service providers, stakeholders, employees, assets, public affairs and the business process.
- Implementation—Specify the complete list of actions to be followed to declare contingency status (such as offsite processing, backup recovery, offsite media and manuals, employee transportation, and distribution and provider contracts).
- Recovery—Recovery is the advance planning and preparations that are necessary to minimise adverse business impact (such as financial loss and image damage) and facilitate faster recovery and ensure continuity of core technology assets that support the critical business functions of an organisation in the event of disaster within an acceptable time frame. The key aspects to be reviewed are:
  - Resumption—Resumption of critical and time-sensitive processes immediately after the interruption and before the declared mean time between failures (MTBF)
  - Revival—Revival of vital and less time-sensitive processes is related to resumption of critical processes
  - Restoration—Repairing and restoring the site to original status and resuming business operations in totality, or putting in place a complete new site
  - Relocation—Relocating to alternative site temporarily or permanently depending upon the interruption. Relocation may not be required in all kinds of interruptions.
  - Crisis management—The overall coordination of the organisation's response to a crisis in an effective, timely manner, with the goal of avoiding or minimising damage to the organisation's profitability, reputation or ability to operate

2.2 Elements of BCP

2.2.1 An essential element of BCP is risk assessment, which involves the task of identifying and analysing the potential vulnerabilities and threats, including the source. Risk assessment involves the process of identifying the potential risks to the organisation, assessing the critical functions necessary for the organisation to continue business operations, defining controls in place to reduce exposure and evaluating the cost of such controls. A risk benefit analysis—the outcome of the risk assessment—elaborates the potential threats and the related exposure together with the contingency and mitigation action required, and concludes by describing the benefits arising out of covering the risks.

2.2.2 A risk assessment followed by a BIA must be performed to assess the overall financial exposures and operational effects resulting from a disruption in business activities. The BIA should identify and help to prioritise the critical business processes supported by the IS infrastructure including, but not limited to, a cost-benefit analysis of controls in different disruption scenarios.

2.3 Key Factors of BCP

2.3.1 The BCP must:

- Be understandable and easy to use and maintain.
- Provide management with a comprehensive understanding of adverse effects on business due to normal systems processing disruption, and the total effort required to develop and maintain an effective BCP.
- Obtain executive-management-level commitment to support and participate in the effort.
- Identify critical information resources related to core business processes.
- Identify methods to maintain the confidentiality and integrity of data.
- Assess each business process to determine its criticality. Indications of criticality include:
  - The process supports lives or people's health and safety.
  - The process is required to meet legal or statutory requirements.
  - Disruption of the process would affect revenue.
  - There is a potential impact to business reputation, including that of the customers.
- Focus the plan's attention on:
  - Disaster management
  - Minimising the effect of disaster, in the eventuality that the disaster is not manageable
  - Orderly recovery
  - Continuity of operations and key services
- Validate RTOs and recovery point objectives (RPOs) for various systems and their conformance to business objectives.
- Identify the conditions that activate the contingency plan.
- Identify which resources will be available in a contingency stage and the order in which they will be recovered.
- Identify the enablers (people and resources) required for recovery.
- Select project teams in accordance with technological and business environments to provide reasonable representation of core and critical functional areas to develop the plan.
- Identify the methods of communication between enablers, support staff and employees.
- Identify geographical conditions related to the recovery of operations.
- Define recovery requirements from the perspective of business functions.
- Define how the BCP considerations must be integrated into ongoing business planning and system development processes for the plan to remain viable over time.
- Implement a process for periodic review of the BCP's continuing suitability as well as timely updating of the document, specifically when there are changes in technology and processes, legal or business requirements. The BCP strategies may also be modified based upon results of risk assessments and vulnerability assessments.
- Develop a comprehensive BCP test approach that includes management, operational and technical testing.
- Implement a process of change management and appropriate version controls to facilitate maintainability.
- Identify mechanisms and decision makers for changing recovery priorities resulting from additional or reduced resources as compared to the the original plan.
- Document formal training approaches.

3. INDEPENDENCE

3.1 Professional Independence

3.1.1 Where the IS auditor has been involved previously in the design, development, implementation or maintenance of any process related to the BCP in an organisation and is assigned to an audit engagement, the independence of the IS auditor may be impaired. In the event of any possible conflict of interest, the same should be explicitly communicated to the organisation and the organisation's concurrence should be obtained in writing before accepting the assignment. The IS auditor should refer to appropriate guidelines to deal with such circumstances.

4. COMPETENCE

4.1 Skills and Knowledge

4.1.1 The IS auditor should provide reasonable assurance that the auditor has the required knowledge and skill to carry out the review of the BCP and its components.

4.1.2 The IS auditor should be competent to determine whether the BCP is in line with the organisation's needs.

4.1.3 The IS auditor should have adequate knowledge to review the aspects related to the BCP. Where expert inputs are necessary, appropriate inputs should be obtained from external professional resources. The fact that external expert resources would be used should be communicated to the organisation in writing.

4.1.4 A BCP review is essentially enterprise-specific, and for the review to be effective, the IS auditor must, at the outset, gain an overall understanding of the business environment, including an understanding of the organisation's mission, statutory or regulatory requirements peculiar to the organisation, business objectives, relevant business processes, information requirements for those processes, the strategic value of IS and the extent to which it is aligned with the overall strategy of the enterprise/organisation.

4.1.5 The IS auditor should undertake the development of a BCP or policies, testing and recovery plans, only if the IS auditor has the necessary knowledge, competence, skills and resources. The IS auditor should refer to appropriate guidelines to deal with such circumstances.

G32 Business Continuity Plan (BCP) Review From IT Perspective cont.

5. PLANNING

5.1 Scope and Objectives of the Review

5.1.1 The IS auditor should, in consultation with the organisation and where appropriate, clearly define the scope and objective of the BCP review. The aspects to be covered by the review should be explicitly stated as part of the scope.

5.1.2 For the purpose of the review, the stakeholders in the solution and recipients of the report should also be identified and agreed upon with the organisation.

5.2 Approach

5.2.1 The IS auditor should formulate the audit approach in such a way that the scope and objectives of the review could be fulfilled in an objective and professional manner.

5.2.2 The audit approach depends upon the phase of the BCP in the organisation.

5.2.3 The approach should consider that the BCP review is a team effort that includes active and stable members as well as discussions with user groups.

5.2.4 The approach should be appropriately documented and identify the requirements of external expert inputs, if appropriate.

5.2.5 Critical areas, such as prioritisation of business processes and technologies and results of a risk assessment, should provide reasonable assurance that the plan is effectively implemented as required.

5.2.6 Depending on the organisational practices, the IS auditor may obtain the concurrence of the organisation for the BCP audit plan and approach.

6. PERFORMANCE OF BCP REVIEW FROM IT PERSPECTIVE

6.1 Execution

6.1.1 The aspects to be reviewed and the review process should be decided, taking into account the intended scope and objective of the review as well as the approach defined as part of the planning process.

6.1.2 In general, the study of available documentation (such as BCP, DRP, BIA, business risk analysis and enterprise risk management framework) should be used appropriately in gathering, analysing and interpreting the data. While all of this information may not be readily available, there must be at a minimum a basic risk assessment analysis that defines critical business processes together with IT-based risks.

6.1.3 Main areas of risk of a BCP should include previously detected BCP weaknesses and changes introduced to the systems environment (such as applications, equipment, communications, process and people) since the last BCP test.

6.1.4 To identify any problems relating to the BCP that have been noted previously and may require follow-up, the IS auditor should review the following documents:

- Incidence reports
- Previous examination reports
- Follow-up activities
- Audit work papers from previous examinations
- Internal and external audit reports
- Internal test reports and remedial action plan
- Published Industry information and references

6.1.5 To identify changes to the systems environment, the IS auditor should interview the organisation's personnel and service providers, as well as analyse spending records and reports, inspect IT premises, review hardware and software inventories, and use specialised software to analyse appropriate data.

6.1.6 The IS auditor should consider in the review each of the following phases of testing:

- Pretest—A set of actions required to set the stage for the actual test
- Test—The real action of BCP test
- Posttest—The cleanup of group activities
- Postinvocation review—The review of actions following the real invocation of the plan

6.1.7 The test plan objectives should be reviewed to verify whether the test plan accomplishes the following:

- Verifies the completeness and precision of the BCP
- Evaluates the performance of the personnel involved in the BCP
- Appraises the training and awareness of the teams
- Evaluates coordination between BCP teams, DRP teams, external vendors and service providers
- Measures the ability and capacity of the backup site to meet the organisation's requirements
- Assesses retrieval capability of vital records
- Evaluates the state and quantity of equipment and supplies that have been relocated to the recovery site
- Measures the overall performance of the operational and processing activity of the organisation

6.1.8 BCP testing should be designed carefully to avoid disruption to the business processes. Appropriate areas of BCP testing should be identified as part of the annual review of risk, and duplication of efforts should be avoided. In reviewing the plan of a BCP test, the IS auditor should verify:

- Scope and objectives of the test plan

- Frequency, methodology and revisions to test plan
- Type, appropriateness and sufficiency of tests
- Applications
- Volume of data
- Business areas
- Network rerouting
- System vulnerability, penetration and incidence response
- Change, configuration and patch management
- Audit evidence criteria and requirements
- The test environment is representative of the operational environment and exceptions are documented
- Test effectiveness and its relation to risk assessment and business impact conclusions

6.1.9 In reviewing a postevent scenario, the IS auditor should verify:

- The cause and nature of disruption
- The extent of damage to personnel, infrastructure and equipment
- The severity of impact
- Mitigation exercises underway
- Services affected
- Records damaged
- Salvageable items
- Items that can be repaired, restored and/or replaced
- Insurance claims
- Processes affected
- Time to restore the IT process
- Action plan, restoration teams, roles and responsibilities

6.1.10 The inferences and recommendations should be based on an objective analysis and interpretation of the data.

6.1.11 Appropriate audit trails should be maintained for the data gathered, analysis made, inferences arrived at and corrective actions recommended.

6.1.12 The observations and recommendations should be validated with the organisation, as appropriate, before finalising the report.

6.2 Aspects to Review

6.2.1 Typically, the BCP should address the following key issues:

- Why should it be done?
- How should it be done?
- Who needs to do it?
- What needs to be done?
- When should it be done?
- Where should it be done?
- Under what policies, rules and standards should it be done?
- Who can change the plan and under what circumstances?
- Under what conditions is a disaster declared ‘over’?

6.2.2 Organisational aspects should be reviewed to consider that:

- The BCP is consistent with the organisational overall mission, strategic goals and operating plans
- The BCP is routinely updated and considered current
- The BCP is periodically tested, reviewed and verified for continuing suitability
- Budget allocation is available for the BCP testing, implementation and maintenance
- Risk analyses are performed routinely
- A formal procedure is in place to regularly update the IT and telecom inventory
- Management and personnel of the organisation have the required skills to apply the BCP and an appropriate training programme is in place
- Measures to maintain an appropriate control environment (such as segregation of duties and control access to data and media) are in place in case of a contingency
- Enablers are identified and the individuals’ roles and responsibilities are adequately defined, published and communicated. Typically, core teams such as the emergency action team, damage assessment team and emergency management team are

constituted. The core teams will be supported by the offsite storage team, software team, application team and security team. There is an emergency operation team, network recovery team, communication team, transportation team, user hardware team, data preparation and record team, administrative support team, supplies team, salvage team, and relocation team.

- Communication channels are fully documented and publicised within the organisation
- The interface and its impact between departments/divisions within the organisation is understood
- Roles and responsibilities of external service providers are identified, documented and communicated
- Coordination procedures with external service providers and customers are documented and communicated.
- BCP teams have been identified for various BCP tasks, clearly establishing roles and responsibilities and management reporting that defines accountability
- Compliance with statutory and regulatory requirements is maintained

6.2.3 Planning aspects should be reviewed to consider that:

- A methodology to determine activities that constitute each process is in place as part of a key business process analysis
- The planned IS technology architecture for the BCP is feasible and will result in safe and sound operations if a business interruption impacts key IT processes
- A risk assessment and BIA were performed before the BCP implementation
- BIA includes changes in the risks and corresponding effect on the BCP
- The BIA identifies the key recovery time frames of the critical business processes
- There is a periodic review of risks
- There are appropriate incident response plans in place to manage, contain and minimise problems arising from unexpected events, including internal or external events
- An appropriate schedule is in place for BCP testing and maintenance
- An onsite test, simulation, triggering of events and their potential impacts should be performed
- A BCP life cycle exists and whether it is followed during development, maintenance and upgrade
- The BCP is reviewed at periodic intervals to confirm its continuing suitability to the organisation

6.2.4 Procedural aspects should be reviewed to consider that:

- Top management is a serious driving force in implementation of the BCP
- Top priority is provided for safety of employees, personnel and critical resources
- Resources and their recovery have been prioritised and communicated to the recovery teams
- Awareness is created across the entire organisation on the effect to the business in the event of a disaster
- Adequate emergency response procedures are in place and tested
- The people involved in the disaster assessment/recovery process are clearly identified and roles and responsibilities are delineated throughout the organisation
- Appropriate levels of training are conducted including mock test drills
- Evacuation plans are in place and are periodically tested
- Backup human resources are identified and available
- Cell, telephone or other such communication call trees are reviewed, tested and routinely updated
- Alternative communications strategies are identified
- Backup and recovery procedures are part of the BCP
- Backups are retrievable
- An appropriate backup rotation practice is in place
- Offsite locations (hot, warm or cold sites) are tested for availability and reliability
- Appropriate offsite records are maintained
- Confidentiality and integrity of data and information are maintained
- Media liaison strategies are in place, where appropriate
- The BCP is periodically tested and test results documented
- Corrective actions are initiated based upon test results
- There is adequate insurance protection

6.3 Outsourcing of IS

6.3.1 Any adverse effect or disruption to the business of the service provider has a direct bearing on the organisation and its customers. Where the organisation has partially or fully delegated some or all of its IS activities to an external provider of such services (the service provider), which have an effect on the process of BCP, the IS auditor should review whether the service provider's BCP process conforms with the organisation's BCP and documented contracts, agreements and regulations remain with the service user.

6.3.2 The review should also verify that the agreement with the outsourced service provider includes a description of the means, methods, processes and structure accompanying the offer of information systems services and products as well as the control of quality.

6.3.3. The IS auditor should obtain an understanding of the nature, timing and extent of the outsourced services. The IS auditor should establish what controls the service user has put in place to address the business requirement of the organisation's business continuity *vis-à-vis* BCP of the service provider. The IS auditor should consider all the audit requirements stated above in reviewing an outsourced activity, in addition to :

- Whether the agreement provides open and unimpeded rights to audit the service provider, as considered necessary by the organisation
- Whether the agreement provides adequate protection for the organisation in case of disruption to the business of the service provider
- Whether the agreement provides continuity of services in the event of a disaster
- Integrity, confidentiality and availability of the organisation's data with the service provider
- Organisation personnel disgruntled over outsourcing arrangement/lack of loyalty due to outsourcing
- Access control/security administration at the service provider premises
- Violation reporting and follow-up by the service provider
- Network controls, change controls and testing at the service provider premises

7. REPORTING

Report Content

7.1.1 The IS auditor should produce reports on the processes, facilities and technologies involved in the BCP, the risks assumed and how those risks are managed in case of a contingency. Monitoring performance of the review is a key success factor. The report, produced as a result of the BCP review, should include aspects such as:

- The scope, objective, period of coverage, methodology followed and assumptions
- Overall assessment of the solution in terms of key strengths and weaknesses as well as the likely effects of the weaknesses
- Recommendations to overcome the significant weaknesses and to improve the solution
- The extent of compliance with CobiT's control objectives, associated management control practices and CobiT information criteria as relevant, along with the effect of any noncompliance
- Reasonable assurance on BCP process and relevant internal controls to ensure that IT systems can be recovered within an acceptable time frame in event of a disruption. The report should state the conclusions, recommendations and any reservations or qualifications.
- Recommendations regarding how the experience could be used to improve similar future solutions or initiatives
- Depending on the scope of the assignment, other topics

7.1.2 The report should be submitted to the the appropriate level of management and the audit committee if one is established.

7.2 Weaknesses

7.2.1 Weaknesses identified in the BCP review, either due to lack of controls, poor implementation or nonmitigation of associated risks to agreeable levels, should be brought to the attention of the business process owner and to IS management responsible for the implementation of the BCP process. Where weaknesses identified during the BCP review are considered to be significant or material, the appropriate level of executive management should be advised to undertake immediate corrective action.

7.2.2 Since effective BCP controls are dependent on the business continuity planning process and related controls, weaknesses in the related controls should also be reported.

7.2.3 The IS auditor should include appropriate recommendations in the report to strengthen controls to mitigate the associated risks.

8. FOLLOW-UP ACTIVITIES

8.1 Timeliness

8.1.1 The effects of any weaknesses in the BCP are ordinarily wide-ranging and high-risk. Therefore, the IS auditor should, where appropriate, carry out sufficient, timely follow-up work to verify that management action to address weaknesses is taken promptly.

8.2 Effectiveness

8.2.1 To provide reasonable assurance of the effectiveness of the review, the IS auditor should conduct a follow-up review to oversee that the recommendations have been carried out and verify the effectiveness of corrective measures implemented.

9. EFFECTIVE DATE

9.1 This guideline is effective for all information systems audits on 1 September 2005. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

G33 General Considerations on the Use of the Internet

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S4 Competence states, “The IS auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment”.

1.1.2 Standard S5 Planning states, “The IS auditor should plan the information systems audit coverage to address the audit objectives and comply with applicable laws and professional auditing standards”.

1.1.3 Standard S6 Performance of Audit Work states, “The audit process should be documented, describing the audit work and the audit evidence that supports the IS auditor's findings and conclusions”.

1.2 Linkage to Complementary Guidelines and Procedures

1.2.1 Guidelines:

- G22 B2C E-commerce Reviews
- G24 Internet Banking

1.2.2 Procedures:

- P2 Digital Signatures and Key Management
- P3 IDS Review
- P6 Firewalls
- P8 Security Assessment—Penetration Testing and Vulnerability Analysis
- P9 Evaluation of Management Controls Over Encryption Methodologies

1.3 Linkage to CobiT

1.3.1 Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT’s control objectives and associated management practices. To meet the responsibility, authority and accountability requirement of IS auditors, the processes in CobiT most likely to be relevant, selected and adapted are classified below as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 Primary:

- M2—*Assess internal control adequacy.*
- M3—*Obtain independent assurance.*
- M4—*Provide for independent audit.*

1.3.3 Secondary:

- PO6—*Communicate management aims and direction.*
- PO7—*Manage human resources.*
- PO8—*Ensure compliance with external requirements.*
- DS1—*Define and manage service levels.*
- DS2—*Manage third-party services.*
- DS10—*Manage problems and incidents.*
- M1—*Monitor the process.*

1.3.4 The information criteria most relevant to Internet use are:

- Primary: effectiveness, efficiency and confidentiality
- Secondary: availability, integrity and reliability

1.4 Need and Purpose for Guideline

1.4.1 IS auditors play a crucial role in responding to rapidly changing information technology, its associated vulnerabilities and potential exposures. The purpose of this guideline is to describe the recommended practices in performing a review of Internet use, access to and/or connections. An IS auditor should be able to identify, document, test and evaluate the controls and the associated risks to achieve relevant control objectives to protect an organisation’s assets.

1.4.2 This guideline provides guidance in applying IS Auditing Standard S6 Performance of Audit Work to obtain sufficient, reliable, relevant and useful evidence during review of Internet connections. The IS auditor should consider it in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

1.4.3 The Internet is becoming more and more a part of the infrastructure in enterprises and is frequently used for several purposes. In general, use of the Internet can be split into four parts. The Internet can be used as:

- A source for collecting and sharing information
- A communication channel
- A window for presentation of enterprises, organisations or persons
- As an electronic marketplace for trading

1.4.4 This guideline encompasses primarily the use of the Internet as a communication channel and as a source of information for enterprises and organisations. The guideline also, to a certain degree, deals with the Internet as a presentation and trade channel.

1.4.5 An enterprise is exposed to many threats by connecting to the Internet. To deal with those threats, it is important to run a risk analysis and take the necessary security precautions. It is also important to be aware that the Internet is not static. It changes frequently and so do the threats and need for security measures.

1.4.6 For every service, examples regarding different threats are mentioned. In such an overall and brief document, the risk picture is not covered completely. New hacker tools appear and new security weaknesses in IT systems are constantly disclosed. Therefore, it is important to obtain updated information about threats and security measures before connecting to the Internet.

1.4.7 There is no overall or international centralised control connected with the use of the Internet. It is a matter for every single enterprise to take the necessary security precautions.

1.5 Guideline Application

1.5.1 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards, guidelines and procedures. This guideline is not necessarily exhaustive or up to date over time.

2 GENERAL CONSIDERATIONS ABOUT INTERNET CONNECTIONS

2.4 Ways of Connecting to the Internet

2.1.1 There are several ways of connecting to the Internet and each has a different need for security measures. Some examples are:

- Detached PCs with modems connected through an Internet service provider (ISP)
- PCs in local networks with modems connected to the Internet through an ISP
- Detached PCs with cellular data connections
- PCs in local networks with cellular data connections
- Local networks connected to the Internet via a router
- Local networks connected to the Internet via a firewall
- Two separate networks—one local network with PCs, which are being used for organisation activities, and one network with PCs for Internet communication

2.1.2 Some of these connections can be combined with service delivery or use of the Internet as an information channel, such as:

- A local network connected to the Internet offering internal/external services from a server in the local network
- A local network connected to the Internet where internal/external services are offered from a server installed in a DMZ
- Two local networks in the same enterprise connected using the Internet as a communication channel
- A local network in an organisation connected to a collaborating partner's network where the Internet is being used as a communication channel (extranet)

2.2 Threats

2.2.1 Threats in a closed network without external connections will, in general, include technical failures, user errors, misuse of systems or disloyal employees spreading confidential information. This risk picture changes when an enterprise connects permanently to the Internet.

2.2.2 Attacks can be divided into the following groups:

- Passive attacks, such as:
  - Network monitoring—Reading usernames and passwords transferred via the Internet by using sniffer software
  - Tapping data—Obtaining confidential information by reading/copying incoming or outgoing e-mail
  - Spyware use—Using a broad category of malicious software to intercept or take partial control of a computer's operation without the user's informed consent. Users ordinarily get infected by visiting certain web sites.
- Active attacks, such as:
  - Attempts to get access through weaknesses in security measures—Accessing local networks and internal IT systems without authorisation when security measures are not properly implemented
  - Obtaining passwords—Using freeware to access password files
  - Masking—Configuring a computer with a trusted network address to obtain access to confidential information
  - Virus infection—Spreading a malicious code that incorporates itself into an IT system and often spreads to other systems and computers when the system is running
  - Trojan horse—Using a malicious program that seems to have a useful function, but carries a virus or an operation that catches passwords that can be used for unauthorised access to the system
  - Introducing worms—Using malicious code that spreads from one IT system to another without any action from the user
  - Exploiting faults and weaknesses in operating systems and applications—Using faults or weaknesses, contained in most systems, to carry out unauthorised activities
  - Exploiting misconfigured IT systems and communication units—Accessing systems because of mistakes made by the system administrators during system configuration or failure to update the configuration after installation of new software or hardware
- Service attacks, such as:
  - Attempting to stop or prevent services—Exploiting errors in data streams to transfer larger amounts of data than that for which the service is prepared. This may result in a data crash.

- Occupying system capacity—Sending continuous requests to online service computers that are not properly configured to reduce system capacity
- Terminating IT systems—Overloading a computer by sending larger amounts of data than it is designed to handle to cause a data crash. There are many ways to provoke an unexpected system termination, called denial of service (DoS).
- Rerouting transactions—Copying homepages from a service provider to a remote server that is configured with the service provider's network address to get credit card numbers from e-business transactions
- Social engineering—Pretending to be a trusted associate to manipulate an authorised user to provide access to confidential business secrets or information about usernames and passwords

2.3 Internet Services

2.3.1 There are several services available on the Internet and new services appear frequently. The most popular services today are:

- E-mail
- World Wide Web (WWW)
- File transfer protocol (FTP)
- News
- Telnet/remote interactive access
- Internet relay chat (IRC)/Instant messaging

2.3.2 E-mail is the most frequently used service on the Internet. This service has become more and more a replacement for ordinary letters and fax because of its speed, lower cost and user friendliness. E-mail was not designed to be a secure service and has several security weaknesses. The most striking points of weakness are:

- Sender—No one can be sure that the sender of an e-mail is the real sender. It is simple to change a name and there is no identity control of the sender. This weakness can be eliminated by using digital signatures, which are often used between business associates; however, this feature is not common in the exchange of e-mails between occasional partners.
- Messages in plaintext—Messages sent via the Internet are sent in plaintext. This makes it possible for all Internet users to read a message and change the message. One can never be sure that a message passes over the Internet without being changed. This weakness can be eliminated by encrypting the message.
- Message delivery—Another e-mail weakness is that there are no guarantees for secure delivery. A message will ordinarily be delivered in a few seconds or minutes, but in some cases the delivery takes several hours if delivered at all. If one of the servers in the delivery chain is unavailable for some reason, messages can remain on that server until it is online again. Depending on how the e-mail system is configured, it ordinarily takes some time before the sender receives a message about the failure. Most e-mail systems have a certificate of posting function. However, lack of compatibility amongst different e-mail systems can result in missing feedback.
- Attachments—Most enterprises that use e-mail via the Internet allow mail to contain attachments. If those attachments are large, they will fill up the e-mail system and server in such a way that e-mail users are prevented from receiving other mail. To avoid this situation, the enterprise can put limits on how large the attachments are that the e-mail is allowed to receive and make guidelines for archiving and deletion of e-mails.
- Spam—An increasing problem is unwanted e-mails, called spam. This may be unwanted advertising and service offerings, including product offerings that may be embarrassing. This spam fills servers and steals time from the recipients. Spam is not regarded as a plain security problem, but can result in reduced availability of the IT systems.

2.3.3 WWW is a worldwide network of servers that offers information in plaintext, sound and pictures. Different kinds of services, such as financial services and trading are available to the international community. Access to WWW goes through a browser, such as Internet Explorer, Opera and others. WWW features are:

- Information quality—WWW contains an enormous amount of information; however, the information quality varies. There is a lack of superior control over the information that is placed on WWW. Every person who transfers information to WWW is responsible for quality assurance. Therefore, there is no guarantee of credibility, accuracy or that the information is up to date.
- Tracks—An Internet user leaves behind several tracks when he/she visits web sites, primarily the network address, but in some cases also the username. By accessing inappropriate sites on the Internet from an organisation computer and leaving tracks behind, the organisation can be associated with web sites, such as those offering pornography, extreme political movements and others. Therefore, many enterprises choose to block addresses to such web sites.
- Browser—There are many browsers available with different functionalities, strengths and weaknesses. New security weaknesses in browsers are disclosed frequently. Some of these weaknesses can cause serious problems for enterprises. Data criminals can create homepages that contain malicious code that exploits security weaknesses and executes unauthorised tasks on an organisation's PCs.
- Plug-ins—In the most used browsers, it is possible to install minor additional programs (plug-ins), which provide increased functionality, such as improved sound, extended video functionality or games. Programming errors in some plug-ins have made it possible for intruders to get access to data in IT systems.
- Cookies—Small pieces of information used by the browser and transferred to the hard disc for logging and documentation purposes, such as the date of the last visit on the WWW, what homepages were visited and what products were bought (if an e-marketplace is visited). E-marketplaces are often based on use of cookies. Cookies can also store passwords; however, the use of cookies represents no known security threats but can be regarded more as a privacy violation as long as web sites store the information about users and user activities. Whether to allow the use of cookies is a policy matter. In most

browsers, it is possible to choose whether to accept cookies. There is also freeware available that gives an opportunity to use cookies during Internet surfing, but removes user information by logoff.

2.3.4 FTP is a service that enables data transfer between computers. It is often used to download files from WWW. FTP has basically no security. Username and passwords are transmitted in plaintext over the network. When used, it is very important to configure the service correctly. FTP service characteristics include:

- Anonymous FTP—A service which allows outsiders to download data or programs from an enterprise server. For an enterprise that wants to offer this service, it is crucial to configure the systems correctly. If not, intruders can get access to enterprise data. The server can also be used to store illegal data or programs. In such cases, the user logs in with the username (anonymous or ftp) and password. However, few systems control whether the username, which is ordinarily an e-mail address, and password are correct.
- Active/passive communication—Unlike other services, FTP uses two gateways for communication. In addition, connection can be made in two ways—active or passive. In active mode, the user decides what gateway to use. In this mode it is possible to control and filter receiving data. If passive mode is used, the connected server decides what gateway to use. Passive mode is difficult for many firewalls to handle in a secure way.

2.3.5 News is a kind of a bulletin board where users can discuss any item. When a letter is sent to news, it is placed on the bulletin board with the author's name and address. The letter is often dispersed to different news servers all around the world. This makes it almost impossible to remove a letter after being sent to news. A letter sent from an organisation's computer can be regarded as the organisation's official view. It is also a risk that an employee could expose organisation secrets. It is possible to block access to news. This is a matter of organisational policy.

2.3.6 Telnet is a service that makes it possible to log on to other computers on the network. Telnet gives the user a character-based virtual terminal. During logon, the username and password are sent in plaintext. It is rather simple for intruders to read user information and use it for unauthorised access. To avoid this, one-time passwords and encryption can be used. It is also possible for hackers to intercept the terminal connection (session hijacking). After user logon, the hacker takes over the session with the user's accesses. This can be avoided by using encryption. Remote interactive access with SSH, remote x-windows VNC and Remote Desktop are expected to take over for Telnet as *de facto* methods of remotely accessing systems.

2.3.7 IRC and instant messaging are real-time conference systems. Users communicate by using a common area—a channel—where all users can participate in discussions. Many IRC/instant messaging programs have security weaknesses that enable intruders to obtain illegal access to an organisation's files. It is also possible for intruders to use those channels to spread viruses and to obtain access via "social engineering".

3 SECURITY MEASURES

3.1 Policy, Products and Follow-up

3.1.1 Secure Internet connections should be built upon the enterprise information security policy. It is important that there are guidelines to ensure correct and secure use of the Internet, and that security awareness is a major focus of leadership. If employees do not live up to security guidelines, the security measures will not work as expected. There should be procedures for authorisation and change control in place. In addition, the security guidelines should encompass ethical behaviour for use of the Internet.

3.1.2 There are many products on the market that can improve Internet security. To achieve the right level of security, it is necessary to implement several complementary products. Selection of products should be based upon a risk assessment.

3.1.3 It is of great importance that security measures are followed up. Operating instructions for monitoring and follow-up to security measures to ensure effectiveness and compliance with guidelines should be in place.

3.2 Firewalls

3.2.1 A firewall is the most common security measure used when establishing a connection from a local network to the Internet. A firewall is a combination of hardware and software that prevents any illegal penetration. The firewall should reflect the enterprise's security policy. Only authorised services should pass through it.

3.2.2 A firewall can be one of the following:

- Packet filtering routers—Examine packets of data entering or leaving a network.
- Application gateways—Apply security mechanisms to specific applications such as FTP or Telnet.
- Circuit level gateways—Supply security mechanisms when a TCP or UDP connection is established.
- Proxy servers—Intercept messages entering or leaving a network enabling the true IP address to be hidden.

The type of firewall deployed may be software-based or hardware-based, the latter being designed primarily for commercial environments, and it may employ a number of the techniques mentioned.

3.2.3 These firewalls deliver different kinds of security and require follow-up and maintenance.

3.2.4 There are two security concepts for data control through a firewall:

- Everything is fully restricted—Only services allowed by management pass through.
- No general restrictions—Only services considered high-risk by management are prevented.

3.2.5 The enterprise's security needs, request for user friendliness and capacity in the IT department should be considered when choosing a firewall solution. Configuration of the firewall should be correct and in compliance with the security policy before users can access the Internet.

3.3 One-time Password

3.3.1 There are many programs available that can be used to unveil passwords. Such programs are used by data criminals and hackers. Users often make passwords that are simple to guess and use for unauthorised purposes. However, even a good password that is hard to guess can be unveiled. Computers today are so powerful that it is possible to unveil even the most complex passwords. To prevent intruder access to an enterprise system, a possible solution is to use one-time passwords.

These can be generated either by a password generator or via a challenge/response system, which is based upon numbers punched on a unit similar to a calculator. One-time passwords should preferably be combined with encrypting software to make a secure solution.

3.4 Penetration Testing and Test Software

3.4.1 It is recommended to research currently known web application vulnerabilities due to the increasing complexity and severity of these vulnerabilities. There is a lot of software, both for sale and freeware, which can be used to test IT systems for different kinds of vulnerabilities/security weaknesses. Some of those are developed by serious persons or companies that want to contribute to a more secure Internet. However, the majority of those programs are developed by data criminals to break into enterprise systems. By using trusted penetration testing software, it is possible to test the quality of security measures in an enterprise's Internet connection.

3.5 Intrusion Detection and Prevention Systems

3.5.1 Intrusion detection systems (IDSs) are used to analyse local networks and business systems to disclose illegal attacks before any damage occurs. An IDS will detect any known attacks whilst they are in progress and send messages to the enterprise's IT personnel or security manager who can put security measures into effect. An IDS should be updated quickly after discovery of new threats and attacks.

3.5.2 Intrusion prevention systems (IPSs) are a concept unlike other security tools, which rely on signature files to identify an attack as (or after) it happens, intrusion prevention software predicts an attack before it can take effect. It does this by monitoring key areas of a computer system, and looks for "bad behaviour", such as worms, Trojans, spyware, malware and hackers. It complements firewall, antivirus and antispyware tools to provide complete protection from emerging threats. It is able to block new (zero-day) threats that bypass traditional security measures as it is not reliant on identifying and distributing threat signatures or patches.

3.6 Encryption

3.6.1 Data transferred over the Internet is, in principle, open to everyone. This means that unprotected sensitive data can be captured and used illegally. A method to ensure integrity and confidentiality of a system is encryption. Encryption can be used on different levels. The most secure solution is to encrypt on the application level, which means that confidentiality and integrity are maintained all the way to the end user. However, this solution is dependent upon compliant software between users.

3.7 Digital Signatures

3.7.1 By using digital signatures, message integrity can be maintained. This is especially useful in trading over the Internet. Digital signatures are based on a pair of keys, one private and one public key. The sender makes a fingerprint (copy) of the message that is being encrypted together with the private encryption key and the receiver's public key. The receiver reverses the process by decrypting the sender's public key and his/her own private key. This generates a new fingerprint that can be compared to the sender's fingerprint. If they are equal, nothing is changed.

3.8 Virtual Private Network (VPN)

3.8.1 VPN is a means to establish a secure communications channel between two or more computers over a shared, unsecured, physical network or networks. Computers can be physically connected in networks, but only those being members in the same virtual network can exchange data. The communication channels can be secured by encryption.

3.9 Antivirus Programs

3.9.1 Data virus is an increasing problem, especially after introduction of macro viruses. Data viruses are being spread through several sources, including e-mails, pirated copies of games and downloaded programs from the Internet. All enterprises that receive e-mail with attachments or permit employees to download from the Internet should have antivirus software on the servers and/or on PCs. It is of great importance that there are routines in place to keep antivirus software up to date.

3.10 Antispyware programs

3.10.1 Spyware differs from viruses and worms in that it does not ordinarily self-replicate. Like many recent viruses, spyware is designed to exploit infected computers for commercial gain. Typical tactics furthering this goal include delivery of unsolicited pop-up advertisements, theft of personal information (including financial information such as credit card numbers), monitoring of web-browsing activity for marketing purposes or routing of HTTP requests to advertising sites. To avoid this exposure, every enterprise should install antispyware programs that are designed to block or remove spyware.

3.11 Logging and Monitoring

3.11.1 The logging and monitoring of Internet traffic itself are not security measures, but are prerequisites to detecting attacks and maintaining security in networks and business systems. To be efficient, logging and monitoring should be carried out in communication nodes such as the firewall. Events that require follow-up should be based upon a risk assessment and enterprise policy. Logging results in large amounts of data, which is hard to follow-up manually. Therefore, it is practical to obtain a tool/software to filter, analyse and present relevant log data.

4. INTERNET USED FOR AN ENTERPRISE PRESENTATION CHANNEL

4.1 Internet Used as a Window

4.1.1 The Internet has been used as a window for an enterprise since the introduction of the WWW. This guideline will not deal with how to present an enterprise, but gives some reflections regarding what to consider before and after transmitting information to the WWW.

4.2 Before Transmitting Information to the WWW

4.2.1 It seems to be a must for most enterprises to be represented on the WWW. Information is often placed on home pages without paying attention to the security aspects. By giving detailed information about the business and employees, an enterprise is exposed to social engineering committed by data criminals. There are also examples of data criminals breaking into web servers to change the content on home pages.

4.2.2 Before an enterprise develops a home page, it should perform a need analysis as background material to decide what kind of information is appropriate to present and determine the level of risk that having that data present represents to the enterprise.

4.3 After Transmitting Information to the WWW

4.3.1 Home pages that are not updated soon lose common interest. Maintenance and development is crucial. Furthermore, the server should be followed up on a daily basis to detect potential illegal or unauthorised activities. If data criminals get access, the content of the home page can be changed in different manners. For instance, a change of telephone number to a competitor's number can result in lost sales for the owner of the home page. Through access to the WWW, it is also possible to exchange pirate copied software or use the server as storage for illegal information.

4.4 Internet as a Trade Channel

4.4.1 Trading products over the Internet (e-business) is a service that is growing all over the world. This trading activity, which includes payment, requires strict security measures. A consumer must be able to provide his/her credit card number to the vendor with confidence that it will not be misused. On the other hand, vendors must be confident that orders are real to avoid unnecessary costs or to be held economically responsible for misuse.

4.4.2 There are several solutions for secure trading over the Internet. Amongst the most common solutions are the Secure Sockets Layer (SSL) and Secure Electronic Transaction (SET) protocols.

4.5 Electronic Money

4.5.1 Trading via the Internet has increased the need for secure electronic money transactions. Many people are reluctant to expose their credit card number, and when transferring small amounts of money, it is not profitable to use credit cards. Therefore, several e-commerce companies have developed solutions to deal with electronic money. E-commerce trading chains consist of three parties: the customer, the vendor and the bank. Before a customer can use e-money, he/she has to download an electronic wallet from the bank. This wallet can be installed on a PC, a personal digital assistant (PDA) or a smartcard. After downloading, the money is ready for use. Digital signatures are used to secure the transactions.

4.6 Trusted Third Party (TTP)

4.6.1 Internet-based trading or exchange of enterprise critical data or information will ordinarily require traceability. To secure the trace integrity, third parties are being used to witness authenticity of the transaction. These are ordinarily big service providers within IT business, which use a technology called public key infrastructure (PKI). The main functions are authentication, encryption and digital signature.

4.6.2 During the last few years, solutions which enable an enterprise to manage its own security without engaging a third party have been launched.

5. PERFORMANCE OF AUDIT WORK/SECURITY REVIEW

5.1 Planning

5.1.1 The IS auditor should gain an understanding of the organisation's access and use of the Internet. The IS auditor should conduct a risk analysis of Internet access and use with respect to the organisation and its mission.

5.1.2 An audit programme should be developed, including the scope, objectives and timing of the audit. Reporting arrangements should be clearly documented in the audit programme. Consideration should be given to the nature and size of the organisation and its stakeholders. The IS auditor should gain an understanding of the organisation's mission and business objectives, the types of technical infrastructure and business critical data.

5.1.3 Also, an understanding of the organisational structure is needed, specifically of the roles and responsibilities of key staff, including the information managers and owners.

5.1.4 A primary objective of the audit planning phase is to understand the threats and risks that the organisation faces when connecting to the Internet.

5.2 Steps to Perform

5.2.1 The IS auditor should consider whether connecting to the Internet is based upon a total enterprise need assessment. The board and management should be aware of risks and what changes in threats mean for the enterprise to make the right decisions regarding use of the Internet. When defining the scope of the review, the IS auditor should also take into account factors such as the type of information collected, stored and used for various purposes within the organisation.

5.2.2 The IS auditor should determine whether the organisation has the following in place:

- An Internet policy
- A guideline for monitoring and follow-up network connection, firewalls, etc.
- An incident reporting procedure
- A guideline for homepage updates
- Training and awareness programmes

These, if available, should be assessed by the IS auditor to provide reasonable assurance that use of Internet is in accordance with policies and procedures.

5.3 Performing a Detailed Review

5.3.1 The IS auditor should assess the following administrative aspects:

- Management responsibility
- The purpose of giving access to the Internet
- Whether the enterprise has confidential/privacy data, which means that connection to the Internet should be restricted or not allowed
- The type of connection
- If there have been need assessments used as a basis for employee access
- Whether access is restricted to certain hours or time of day/week
- If there are any restrictions regarding where employees are given permission to surf/collect information
- If the enterprise sells products or services via the Internet, and whether payment is made via the Internet
- If the enterprise has the necessary competence, time and capacity to install, follow up and maintain an Internet connection

5.3.2 Risk assessment should cover the following as a minimum:

- Threats
- Changes in threats when connecting to the Internet
- Whether the existing information security policy covers the use of the Internet
- Whether the enterprise is interesting to data criminals or a target of industry espionage
- Consequences if internal/confidential information is exposed to intruders
- Cost if a security incident occurs
- Probability for a security incident to occur
- Security measures to be carried out to secure the Internet connections

5.3.3 Guidelines for use of the Internet should contain as a minimum:

- A connection to the security policy
- Documentation of services that are allowed
- Rules for acceptable use of those services and sanctions if rules are broken
- Description of procedures for network monitoring of compliance with laws and regulations
- Documentation of ethical attitudes
- Rules for sending and storing of e-mail
- Requirements for user training
- Potential agreements between collaborating partners
- An agreement that all employees sign to confirm that guidelines are read, understood and will be followed, which is important to prevent potential violations of laws regarding logging and monitoring of Internet traffic

5.3.4 Documentation for Internet operation should contain as a minimum:

- All technical equipment and infrastructure
- Rules for logging and monitoring
- Alarm setup
- Routines for logging and incident follow-up

5.3.5 Documentation of the Internet connection should contain as a minimum:

- Description of network perimeters
- Descriptions of access points
- Description of all modem connections
- Configuration of routers and potential proxy servers
- Configuration of firewalls

- Configuration of other security measures, such as encryption and digital signatures
- Description of secure storage of log files, for instance to write once read many (WORMs), external discs or tape
- Description of procedures to recreate log files

5.3.6 Documentation of routines for monitoring should contain as a minimum:

- Description of responsibility for administration and maintenance of the Internet connection, including back-up resources
- Review of log files from the firewall
- Review of transactions from current servers
- Review of log files from user activities
- Review of network statistics
- Following up on potential security incidents or attempts

5.4 Responsibilities

5.4.1 User responsibilities include:

- Complying with IS policy, guidelines and ethical standards
- Respecting existing laws and regulations in the countries where information is collected
- Never giving a password on the telephone or e-mail
- Never changing passwords by request via telephone or e-mail from an unknown person
- Never using the same username and password on the Internet as used on the local network
- Verifying data downloaded from the Internet before using it as a basis for business decisions, trading or payment, etc.

5.4.2 Responsibilities of IT management include:

- Maintaining and following up on Internet firewalls, routers, servers and other IT equipment in use. This includes responsibility to ensure that the correct version of system software and applications are properly installed and maintained. Furthermore, IT management should make sure that firewall logs are followed up on a daily basis and that configuration is in accordance with written guidelines.
- Being updated on threats and vulnerabilities in conjunction with systems and applications in use, a prerequisite for proper maintenance of the security level

5.4.3 Responsibilities of security management include:

- Restricting the person in charge of information security from having additional functions, such as IT operator, systems analyst or programmer
- Working out the guidelines for use of the Internet and giving information about acceptable and ethical use to the users, which is the security manager's main task
- Acting as a resource for top management within information security
- Reviewing logs from the firewall
- Reviewing reports from security systems
- Making sure that security measures are regularly tested
- Making sure that continuity and disaster plans cover enterprise services
- Following up on security incidents or attempts
- Reporting serious security incidents to management
- Being updated on threats and vulnerabilities in conjunction with systems and applications in use, as is the IT manager

5.4.4 Responsibilities of senior management include:

- Formulating an overall Internet policy
- Monitoring the policy and the related processes
- Providing adequate resources
- Empowering IT management to implement the policy

5.5 Technical Issues and Security Measures

5.5.1 Technical issues include:

- Security alarms and logging of unauthorised incidents should be activated in system software.
- The connection between the local network and the Internet should be protected through a firewall.
- Only those services allowed by management should pass through the firewall.
- The firewall should stop all non-allowed network protocols.
- The firewall should stop all access when an system error or disruption in production occurs.

5.5.2 Service related measures include:

- E-mail
  - Critical messages should be encrypted.

G33 General Considerations on the Use of the Internet cont.

  - Time critical messages should be followed up manually.
  - Attachments should be scanned to avoid damage from malicious code.
  - Passwords should not be sent by e-mail.
- WWW
  - When using Internet services, one should use usernames and passwords other than those used on the local network.
  - Information downloaded from the WWW should be verified and controlled before use.
  - Only an approved Internet browser should be used, and changes in configuration or installation of plug-ins should not be allowed.
  - All files downloaded from the Internet should be scanned for viruses or similar malicious code, such as spyware.
- FTP
  - All files downloaded from the Internet should be scanned for viruses or similar malicious code, such as spyware.
- News
  - Users should not be allowed to participate in “flame wars”.
  - Users should not be allowed to write articles which can give a negative image of the enterprise, employees, collaborating partners, vendors or competitors.
  - Information collected from news should be verified and controlled before use.
- Telnet
  - One-time passwords should be used, if possible.
- IRC/Instant messaging
  - IRC and instant messaging should only be allowed from a stand-alone PC
  - IRC and instant messaging should not be allowed to give internal enterprise information

5.5.3 Other security measures include:

- Logging on from a home office or other external logon should use a VPN connection with secure authentication, such as one-time password.
- Servers dedicated to external users should be installed in the DMZ.
- CGI scripts and other code used, which receive data from the Internet, should be quality assured and tested for errors and weaknesses.

6. EFFECTIVE DATE

6.1 This guideline is effective for all information systems audits beginning on 1 March 2006. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary*.

G34 Responsibility, Authority and Accountability

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S1 Audit Charter states, "The purpose, responsibility, authority and accountability of the information systems audit function or information systems audit assignments should be appropriately documented in an audit charter or engagement letter".

1.1.2 Standard S3 Professional Ethics and Standards states, “The IS auditor should adhere to the ISACA Code of Professional Ethics”.

1.2 Linkage to CobiT

1.2.1 High-level control objective M3 (*Obtain independent assurance*) states, “…obtaining independent assurance to increase confidence and trust among the organisations, customers and third-party providers”.

1.2.2 High-level control objective M4 (*Provide for independent audit*) states, “…providing for independent audit to increase confidence levels and benefit from best practice advice”.

1.2.3 Detailed control objective M4.1 (*Audit charter*) states, “A charter for the audit function should be established by the organisation’s senior management. This document should outline the responsibility, authority and accountability of the audit function. The charter should be reviewed periodically to assure that the independence, authority and responsibility of the audit function are maintained”.

1.3 CobiT Reference

1.3.1 Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT’s control objectives and associated management practices. To meet the requirement, the processes in CobiT most likely to be relevant, selected and adapted are classified below as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 Primary:

- M2—*Assess internal control adequacy.*
- M3—*Obtain independent assurance.*
- M4—*Provide for independent audit.*

1.3.3 Secondary:

- PO6—*Communicate management aims and direction.*
- PO7—*Manage human resources.*
- PO8—*Ensure compliance with external requirements.*
- DS1—*Define and manage service levels.*
- DS2—*Manage third-party services.*
- DS10—*Manage problems and incidents.*
- M1—*Monitor the process.*

1.3.4 The information criteria most relevant to responsibility, authority and accountability are:

- Primary: effectiveness, efficiency and confidentiality
- Secondary: availability, integrity and reliability

1.4 Purpose of the Guideline

1.4.1 With continual increase in system complexity and correspondingly ingenious cyberthreats, organisations are increasingly looking to professionals who have the proven skill, expertise and knowledge to identify, evaluate and recommend solutions to mitigate system risks and vulnerabilities. IS auditors play a crucial role in responding to rapidly changing information technology, its associated vulnerabilities and potential exposures to protect the organisation’s assets and assist in risk identification, evaluation and mitigation. IS auditors provide technical IT skills and expertise to the audit function—whether external or internal—and there is an ever-increasing need to maintain an adequate level of skill and knowledge in IT expertise as the technological sophistication in financial and operational environment increases. In the present era, where technology is the prime business driver or a key enabler to support business processes, organisations and their stakeholders are relying on the IS auditor to determine whether management is committed to ensure the safeguarding of assets; data integrity, effectiveness and efficiency; adherence to corporate policies; and compliance with legal, regulatory and statutory obligations.

1.4.2 ISACA’s IS auditing standards and CobiT clearly emphasise that the audit charter should accurately establish the IS auditors responsibility, authority and accountability to conduct audits.

1.4.3 It is in this context that there is a need for a guideline to provide guidance to IS auditors on their responsibility, authority and accountability on accepting to conduct audit assignments.

1.4.4 This guideline provides guidance in applying IS Auditing Standards S1 Audit Charter and S3 Professional Ethics and Standards. The IS auditor should consider this guideline in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

1.5 Guideline Application

1.5.1 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards and guidelines.

G34 Responsibility, Authority and Accountability cont.

2. RESPONSIBILITY

2.1 To the Profession

2.1.1 The IS auditor should be straightforward, honest and sincere in his/her approach to professional work.

2.1.2 The IS auditor should be independent of the auditee in attitude and appearance.

2.1.3 The IS auditor should adhere to the codes of professional ethics prescribed by his/her respective professional bodies, such as ISACA's Code of Professional Ethics

2.1.4 The IS auditor should conduct his/her activities in accordance with applicable auditing standards and generally accepted auditing practices applicable to the profession of IS auditing, such as ISACA's IS Auditing Standards, Guidelines and Procedures.

2.1.5 In instances where compliance is not achievable due to the circumstances of the audit environment, the IS auditor should disclose the fact of such non-compliance including the reason thereof and the effect on the audit of such non-compliance with applicable auditing standards in the audit report.

2.1.6 The IS auditor should uphold the dignity of the profession at all times.

2.1.7 The IS auditor should comply with applicable regulatory and statutory requirements.

2.1.8 The IS auditor should possess the required knowledge, competencies and skill to conduct accepted assignments.

2.1.9 The IS auditor should supervise all audit staff assigned to the IS audit, assure quality, comply with applicable standards and facilitate staff development.

2.1.10 The IS auditor should obtain and maintain sufficient and competent audit evidence in support of his/her conclusions and recommendations. In an audit of an information systems environment, some of the audit evidence may be in electronic form. The IS auditor should provide reasonable assurance that such audit evidence is adequately and safely stored and is retrievable in its entirety as and when required.

2.2 To the Auditee (Organisation)

2.2.1 The IS auditor should recognise, understand and assimilate the auditee's business objectives, goals and mission.

2.2.2 The IS auditor should understand the auditee's professional requirements of the IS auditor including, but not limited to, all independent requirements placed upon by the auditee.

2.2.3 Wherever appropriate, the IS auditor and auditee should mutually agree on the scope, objectives and terms of reference of the audit assignment.

2.2.4 The IS auditor should obtain sufficient understanding of management's attitudes, awareness and actions regarding internal controls and their importance to assess the appropriateness of the internal control environment.

2.2.5 The IS auditor should conduct a preliminary assessment of control risk relevant to activity under review. Audit objectives should reflect the results of this assessment. The IS auditor should document—in the audit working papers—the understanding obtained of the organisation's control systems and the assessment of control risk.

2.2.6 The IS auditor should use appropriate risk assessment techniques in developing the overall audit plan. When the control risk is assessed at a lower level, the IS auditor should also document the basis for the conclusions. In such an event, the IS auditor should obtain audit evidence through tests of control to support his/her assessment of control risk. The lower the assessment of control risk, the more audit evidence the IS auditor should obtain that IS/internal control systems are suitably designed and operating effectively.

2.2.7 Based on the results of the tests of control, the IS auditor should evaluate whether the internal controls are designed and operating as contemplated in the preliminary assessment of control risk. The IS auditor should consider the assessed levels of inherent and control risks in determining the nature, timing and extent of substantive procedures required to reduce audit risk to an acceptably low level.

2.2.8 The IS auditor should confirm the assessment of control risk based on results of substantive procedures and other audit evidence obtained during the conduct of the audit. In case of deviations from the prescribed control systems, the IS auditor should make specific inquiries to consider their implications. Where, on the basis of such inquiries, the IS auditor concludes that the deviations are such that the preliminary assessment of control risk is not supported; he/she should amend the same unless the audit evidence obtained from other tests of control supports that assessment. Where the IS auditor concludes that the assessed level of control risk needs to be revised, he/she should modify the nature, timing and extent of his/her planned substantive procedures.

2.2.9 The IS auditor should discuss with audit management and agree upon the audit plan, audit methodology, resources, time frame, and reporting requirements for the assignment. In planning the portions of the audit that may be affected by the IS environment, the IS auditor should obtain an understanding of the significance and complexity of the IS activities, appropriateness of stated controls and the availability and reliability of the data for use in the audit. This understanding would include such matters as:

- The information systems infrastructure [hardware, operating system(s) and application software used by the organisation, including changes, if any, therein since last audit]
- The significance and complexity of processing in each significant application
- Determination of the organisational structure of the organisation's IS activities and the extent of concentration or distribution of processing throughout the organisation, particularly, as they may affect segregation of duties
- Determination of the availability of data, reliability of available data, source documents, computer files and other audit evidence that may be required by the IS auditor and that may exist for only a short period or only in machine-readable form. Computer information systems may generate reports that might be useful in performing substantive tests (particularly analytical procedures).

2.2.10 The IS auditor should conduct the audit with due diligence and due professional care.

2.2.11 The IS auditor should have knowledge of key information technology risks and controls and available technology, such as computer assisted audit tools and other data analysis techniques, to perform his/her assigned work. Audits should be performed with proficiency and due professional care. The audit team collectively should possess or obtain the knowledge, skills and other competencies needed to perform their responsibilities.

2.2.12 The IS auditor should make management aware, as soon as practical and at an appropriate level of responsibility, of material weaknesses in the design or operation of the internal control systems that have come to the auditor's attention.
2.2.13 If the IS auditor believes that senior management has accepted a level of residual risk that may be unacceptable to the organisation, the IS auditor should discuss the matter with senior management. If the decision regarding residual risk is not resolved, the IS auditor should consider reporting the same to the board for resolution.
2.2.14 The IS auditor should respect the confidentiality of information acquired in the course of his/her work and should not disclose any such information to a third party without specific authority or unless there is a legal or professional duty to disclose it. The duty of confidentiality continues even after conclusion of the assignment and/or termination of the relationship between the IS auditor and the auditee.
2.2.15 The IS auditor should maintain an appropriate communication channel with the auditee. Communication should be accurate, objective, clear, concise, constructive, complete and timely. Results of the audit should be communicated to appropriate parties or authorities.
2.2.16 The IS auditor should submit a report in the appropriate form on completion of the audit. The report should include limitations, if any, on distribution and use of the results. The report should identify the organisation, the intended recipients and any restrictions on its circulation. The IS auditor should follow the reporting standards, policies and procedures of his/her respective audit organisations.
2.2.17 The IS auditor should be independent of the auditee at all times in attitude and appearance. The IS auditor's role is to audit an organisation's IS/internal policies, practices and procedures to assure that controls are adequate to achieve the organisation's mission. Although an IS auditor may be part of the organisation being audited, it is important and necessary that the IS auditor's independence be maintained.
2.2.18 In circumstance where the IS auditor is part of an organisation's control framework, he/she should provide reasonable assurance that he/she is not part of the team which is responsible for implementing specific IS/internal control procedures in the organisation under review.
2.2.19 The IS auditor should follow-up as appropriate and as required by the terms of assignment. If required, the IS auditor should also establish a follow-up process to monitor and determine that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

2.3 To the Stakeholders
2.3.1 The IS auditor should serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.
2.3.2 The IS auditor should disclose all material instances or events that have a direct bearing on the stakeholders' interests.
2.3.3 The IS auditor should disclose the true and correct state of affairs of the area under audit, as per scope and objectives of assignment.
2.3.4 The IS auditor should avoid misstatements and/or ambiguous statements, or statements leading to varied interpretations, in the report.
2.3.5 The IS auditor should disclose instances of loss of independence, if any, during the conduct of the audit.

2.4 Statutory and Regulatory
2.4.1 The IS auditor should keep abreast with the applicable laws, rules and regulations.
2.4.2 The IS auditor should review compliance with applicable statutory laws, rules, regulations and contracts and, where applicable, seek legal guidance.
2.4.3 The IS auditor should disclose information as required by law and, where appropriate, with the consent of the auditee
2.4.4 The IS auditor should use licensed tools and software in conducting audit assignments.

2.5 To Society
2.5.1 The IS auditor should support the education of the public and auditees in enhancing their understanding of IS security, control, assessing and managing risks, safeguarding IS assets, etc.
2.5.2 The IS auditor should support the education of the public and auditees on the uses and possible abuses of technology, control models, control objectives, generally accepted control practices, monitoring and assuring methodologies.
2.5.3 The IS auditor should support the education of the public and auditees on the precautions to be undertaken and preventive measures to be considered where transactions happen with the aid of technology.

3. AUTHORITY

3.4 Rights of IS Auditors
3.1.1 The IS auditor has the right to have an engagement letter or audit charter specifying the scope, objective and terms of reference of the audit.
3.1.2 The IS auditor has the right to access appropriate information and resources to effectively and efficiently complete the audit.
3.1.3 The IS auditor has the right to believe that management has established appropriate controls to prevent, deter and detect fraud unless the tests and evaluation carried on by the IS auditor prove otherwise.
3.1.4 The IS auditor has the right to call for such information and explanations deemed necessary and appropriate to permit objective completion of the audit.

3.1.5 The IS auditor has the right to retain the working files, documents, audit evidences, etc., obtained during the course of the audit, in support of his/her conclusions and to use the same as the basis of reference in case of any issues or contradictions.

3.5 Limitations

3.2.1 The IS auditor should have sufficient knowledge to identify the indicators of fraud but may not be expected to have the expertise of the person whose primary responsibility is detecting and investigating fraud.

3.2.2 The IS auditor should apply the due professional care and skill expected of a reasonably prudent and competent professional. However, due professional care does not imply infallibility.

3.2.3 The IS auditor should be alert to the significant risks that might affect objectives, operations or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

3.2.4 Where the IS auditor is not able to obtain required information, is restricted from accessing resources or is in any way restrained from carrying out his/her function, the IS auditor should escalate his/her concerns to appropriate senior levels in management. The IS auditor should conduct the audit in a professional manner.

3.2.5 Where the IS auditor has utilised the services of an external expert, the IS auditor should evaluate the usefulness and sufficiency of work performed by such external expert and also perform appropriate testing to confirm the findings of the external expert.

3.2.6 The IS auditor is not responsible for implementing corrective actions.

4. ACCOUNTABILITY

4.1 Professional Accountability

4.1.1 Conventional interpretation and ordinary discourse interpret accountability as a process of assigning blame and punishing wrongdoing. Professionally, this should be seen as a positive incentive—as an opportunity to demonstrate achievements and stewardship. In this view, accountability is an integral and indispensable part of establishing effective relationships for getting things done and owning responsibility.

4.1.2 The IS auditor's precise role and relationship varies with different organisations and the nature of the assignment. Therefore, it is important that there is clarity over whom the assignment serves and the purpose of the assignment. The auditor's relationship with each of the key parties should be determined and documented in the engagement letter with the auditee.

4.1.3 It is generally accepted in principle that the IS auditor should be objective and thus remain independent from organisation management. The board or management often seek greater reassurance about controls and other matters. It is management's responsibility to establish and maintain adequate internal control structure. In such circumstances, the IS auditor is accountable for the credibility of the submitted report.

4.1.4 Accountability can be established through due professional diligence, a proactive approach, transparency in the delivery of services, and reporting/providing credible and timely information to the concerned/recognised group.

4.1.5 Accountability is responsibility for performance against agreed-upon expectations both stated or implied.

4.1.6 The IS auditor should exercise due caution from disclosing information acquired in the course of his/her professional engagement to any person other than the organisation, without consent of the organisation or otherwise than as required by any statute for the time being in force. The IS auditor should always keep in view the various regulatory and statutory issues applicable to the organisation audited to provide reasonable assurance of the compliance with disclosure of information.

4.2 Professional Negligence

4.2.1 The IS auditor should not express an opinion without obtaining sufficient and competent information and possessing relevant audit evidence based upon generally accepted auditing practices.

4.2.2 The IS auditor should report to appropriate parties/authorities any material departure from procedures, policies and compliance matters that has come to his/her notice during the conduct of the assignment.

4.3 Restrictions

4.3.1 The IS auditor should not accept assignments if his/her independence will be impaired or perceived to be impaired. For example, if the IS auditor has a beneficial interest in the auditee organisation or is not independent of the auditee, he/she should not accept the assignment. Instances of beneficial interest may be indebtedness to or significant investment in the organisation.

4.3.2 The IS auditor should not allow any unauthorised person or firm to conduct IS audit assignments in his/her name.

4.3.3 The IS auditor should not solicit professional work by unfair means and not make payment of commission or brokerage for obtaining professional assignments.

4.3.4 The IS auditor should not advertise his/her professional accomplishments or services. In promoting themselves and their professional services, IS auditors should:

- Not use means which brings disrepute to the profession
- Not make exaggerated claims for the services offered, qualifications possessed or experience gained
- Not denigrate work of other IS auditors

4.3.5 The IS auditor should not seek professional work by unethical means.

5. EFFECTIVE DATE

5.1 This guideline is effective for all information systems audits beginning 1 March 2006. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

G35 Follow-up Activities

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S8 Follow-up Activities states, "After the reporting of findings and recommendations, the IS auditor should request and evaluate relevant information to conclude whether appropriate action has been taken by management in a timely manner".

1.1 Linkage to COBIT

1.2.1 High-level control objective M3 (*Obtain independent assurance*) states, "…obtaining independent assurance to increase confidence and trust amongst the organisations, customers and third-party providers".

1.2.2 High-level control objective M4 (*Provide for independent audit*) states, "…providing for independent audit to increase confidence levels and benefit from best practice advice".

1.2.3 Detailed control objective M4.8 (*Follow-up activities*) states, "Resolution of audit comments rests with management. Auditors should request and evaluate appropriate information on previous findings, conclusions and recommendations to determine whether appropriate actions have been implemented in a timely manner".

1.3 COBIT Reference

1.3.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the requirement, the processes in COBIT likely to be the most relevant selected and adapted are classified below as primary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 Primary:

- M3—*Obtain independent assurance*
- M4—*Provide for independent audit*

1.3.3 The information criteria most relevant to competence are:

- Primary: effectiveness, efficiency, confidentiality, integrity and compliance
- Secondary: availability and reliability

1.4 Purpose of the Guideline

1.4.1 The purpose of this guideline is to provide direction to IS auditors engaged in following up on recommendations and audit comments made in reports.

1.4.2 This guideline provides guidance in applying IS Auditing Standard S8 Follow-up Activities.

1.5 Guideline Application

1.5.1 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards and guidelines.

2. FOLLOW-UP ACTIVITIES

2.1 Definition

- Follow-up activities by IS auditors can be defined "as a process by which they determine the adequacy, effectiveness and timeliness of actions taken by management on reported engagement observations and recommendations, including those made by external auditors and others". A follow-up process should be established to help provide reasonable assurance that each review conducted by the IS auditors provides optimal benefit to the organisation by requiring that agreed-upon outcomes arising from reviews are implemented in accordance with management undertakings or that management recognises and acknowledges the risks inherent in delaying or not implementing proposed outcomes.

2.2 Management's Proposed Actions

2.2.1 As part of the IS auditor's discussions with the engagement organisation, the IS auditor should obtain agreement on the results of the engagement and on a plan of action to improve operations, as needed.

2.2.2 Management should provide an implementation/action date when each proposed action is to be completed.

2.2.3 When management's proposed actions to implement or otherwise address reported recommendations and audit comments have been discussed with or provided to the IS auditor, these actions should be recorded as a management response in the final report with a committed implementation date.

2.2.4 If the IS auditor and engagement organisation disagree about a particular recommendation or audit comment, the engagement communications may state both positions and the reasons for the disagreement. The organisation's written comments may be included as an appendix to the engagement report. Alternatively, the organisation's views may be presented in the body of the report or in a cover letter. Senior management (or the audit committee if one exists) should then make a decision as to which point of view they support. If senior management (or the audit committee) supports the view of the organisation in a particular case, the IS auditor need not follow-up with that particular recommendation, unless it is considered that the significance and level of effect of the observation has changed due to a change(s) in the IS environment (refer to section 2.4.3).

2.2.5 During some reviews, such as pre-implementation application system reviews, findings may be reported to the project team and/or management on an ongoing basis often in the form of issue statements. In these cases, actions to resolve issues raised should be monitored on an ongoing basis. If issue statement recommendations have been implemented, then "completed" or "implemented" can be recorded against the recommendation in the final report. "Completed" or "implemented" recommendations should be reported.

2.3 Follow-up Procedures

2.3.1 Procedures for follow-up activities should be established and should include:

- The recording of a time frame within which management should respond to agreed-upon recommendations
- An evaluation of management's response
- A verification of the response, if thought appropriate (refer to section 2.7)
- Follow-up work, if thought appropriate
- A communications procedure that escalates outstanding and unsatisfactory responses/actions to the appropriate levels of management
- A process for providing reasonable assurance of management's assumption of associated risks, in the event that remedial action is delayed or not proposed to be implemented

2.3.2 An automated tracking system or database can assist in the carrying out of follow-up activities.

2.3.3 Factors that should be considered in determining appropriate follow-up procedures are:

- Any changes in the IS environment that may affect the significance of a reported observation
- The significance of the reported finding or recommendation
- The effect that may result should the corrective action fail
- The degree of effort and cost needed to correct the reported issue
- The complexity of the corrective action
- The time period involved

2.3.4 If the IS auditor is working in an internal audit environment, responsibility for follow-up should be defined in the internal audit activity's written charter.

2.4 Timing and Scheduling of Follow-up Activities

2.4.1 The nature, timing and extent of the follow-up activities should take into account the significance of the reported finding and the effect if corrective action is not taken. The timing of IS audit follow-up activities in relation to the original reporting is a matter of professional judgement dependent on a number of considerations, such as the nature or magnitude of associated risks and costs to the organisation.

2.4.2 Agreed-upon outcomes relating to high-risk issues should be followed up soon after the due date for action and may be monitored progressively.

2.4.3 Because they are an integral part of the IS audit process, follow-up activities should be scheduled, along with the other steps necessary to perform each review. Specific follow-up activities and the timing of such activities may be influenced by the results of the review and may be established in consultation with line management.

2.4.4 In a particular report, the implementation of all the management responses may be followed up together even though the implementation dates committed to by management may be different. Another approach is to follow up individual management responses according to the due date agreed to with management.

2.5 Deferring Follow-up Activities

2.5.1 The IS auditor is responsible for scheduling follow-up activities as part of developing engagement work schedules. The scheduling of follow-ups should be based on the risk and exposure involved, as well as the degree of difficulty and the significance of timing in implementing corrective action.

2.5.2 There may also be instances where the IS auditor judges that management's oral or written response shows that action already taken is sufficient when weighed against the relative importance of the engagement observation or recommendation. On such occasions, actual follow-up verification activities may be performed as part of the next engagement that deals with the relevant system or issue.

2.6 The Form of Follow-up Responses

2.6.1 The most effective way to receive follow-up responses from management is in writing, as this helps to reinforce and confirm management responsibility for follow-up action and progress achieved. Also, written responses ensure an accurate record of actions, responsibilities and current status. Oral responses may also be received and recorded by the IS auditor and where possible approved by management. Proof of action or implementation of recommendations may also be provided with the response.

2.6.2 The IS auditor may request and/or receive periodic updates from management to evaluate the progress management has made to carry out its agreed-upon actions, particularly in relation to high-risk issues and remedial actions with long lead times.

2.7 Nature and Extent of Follow-up Activities

2.7.1 Normally, the IS auditor will request follow-up status from the organisation soon after the proposed implementation date of some or all of the agreed-upon actions has passed. This may involve reformatting the final report to give the organisation an area in the report to document the details of actions taken to implement recommendations.

2.7.2 The organisation will normally be given a time frame within which to respond with details of actions taken to implement recommendations.

2.7.3 Management's response detailing the actions taken should be evaluated, if possible, by the IS auditor who performed the original review. Wherever possible, audit evidence of action taken should be obtained. For example, procedures may have been documented or a certain management report produced.

2.7.4 Where management provides information on actions taken to implement recommendations and the IS auditor has doubts about the information provided or the effectiveness of the action taken, appropriate testing or other audit procedures should be undertaken to confirm the true position or status prior to concluding follow-up activities.

2.7.5 As a part of the follow-up activities, the IS auditor should evaluate whether unimplemented findings are still relevant or have a greater significance. The IS auditor may decide that the implementation of a particular recommendation is no longer appropriate. This could occur where application systems have changed, where compensating controls have been implemented, or where business objectives or priorities have changed in such a way as to effectively remove or significantly reduce the original risk. In the same way, a change in the IS environment may increase the significance of the effect of a previous observation and the need for its resolution.

2.7.6 A follow-up engagement may have to be scheduled to verify the implementation of critical/important actions.

2.7.7 The IS auditor's opinion on unsatisfactory management responses or action should be communicated to the appropriate level of management.

2.8 Acceptance of Risks by Management

2.8.1 Management is responsible for deciding the appropriate action to be taken in response to reported engagement observations and recommendations. The IS auditor is responsible for assessing such management action for appropriateness and the timely resolution of the matters reported as engagement observations and recommendations.

2.8.2 Senior management may decide to accept the risk of not correcting the reported condition because of cost or other considerations. The board (or the audit committee if one exists) should be informed of senior management's decision on all significant engagement observations and recommendations.

2.8.3 When the IS auditor believes that the organisation has accepted a level of residual risk that is inappropriate for the organisation, the IS auditor should discuss the matter with internal audit and senior management. If the IS auditor is not in agreement with the decision regarding residual risk, the IS auditor and senior management should report the matter to the board (or the audit committee, if one exists) for resolution.

2.9 External Audit Follow-up by an Internal IS Auditor

2.9.1 Follow-up responsibilities for ongoing internal audit activities should be assigned in the audit charter of the internal IS audit function, and for other audit assignments in the engagement letters.

2.9.2 Depending on the scope and terms of the engagement and in accordance with the relevant IS Auditing Standards, external IS auditors may rely on an internal IS audit function to follow-up on their agreed-upon recommendations.

3. CONSULTING

3.1 Consulting Type Engagements

3.1.1 Consulting type engagements or services can be defined as "advisory and related client service activities, the nature and scope of which are agreed upon with the client and which are intended to add value and improve an organisation's operations. Examples include counsel, advice, facilitation, process design and training."[1] The nature and scope of the engagement should be agreed before the engagement begins.

3.1.2 The IS auditor should monitor the results of consulting engagements to the extent agreed upon with the organisation. Varying types of monitoring may be appropriate for differing types of consulting engagements. The monitoring effort may depend on factors, such as, management's explicit interest in the engagement outcomes or the IS auditor's assessment of the project's risks and/or potential additional value to the organisation identified by the engagement.

4. REPORTING

4.1 Reporting of Follow-up Activities

4.1.1 A report on the status of agreed remedial actions arising from IS audit reports, including agreed recommendations not implemented, should be presented to the audit committee, if one has been established, or alternatively to the appropriate level of organisation management.

4.1.2 If during a subsequent engagement, the IS auditor finds that the action that management had purported as "implemented" had in fact not been implemented, this should be communicated to senior management and the audit committee if one is in place.

4.1.3 When all the agreed remedial actions have been implemented, a report detailing all the implemented/completed actions can be forwarded to senior management (or the audit committee, if one exists).

5. EFFECTIVE DATE

5.1 This guideline is effective for all information systems audits beginning 1 March 2006. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

[1] International Standards for the Professional Practice of Internal Auditing, Glossary, IIA

G36 Biometric Controls

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, 'IS audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met. During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.1.2 Standard S10 IT Governance states, 'The IS auditor should review and assess whether the IS function aligns with the organisation's mission, vision, values, objectives and strategies…The IS auditor should review and assess the effectiveness of IS resources and performance management processes'.

1.2 Linkage to COBIT

1.2.1 Control process AI1 Identify automated solutions states, 'Control over the IT process of identify automated solutions that satisfies the business requirement for IT of translating business functional and control requirements into an effective and efficient design of automated solutions by focusing on identifying technically feasible and cost-effective solutions is achieved by:

- Defining business and technical requirements
- Undertaking feasibility studies as defined in the development standards
- Approving (or rejecting) requirements and feasibility study results

And is measured by the:

- Number of projects where stated beliefs were not achieved due to incorrect feasibility assumptions
- Percent of feasibility studies signed off by the business process owner
- Percent of users satisfied with functionality delivered'

1.2.2 Control process AI3 Acquire and maintain technology infrastructure states, 'Control over the IT process of acquire and maintain technology infrastructure that satisfies the business requirement for IT of acquiring and maintaining an integrated and standardised IT infrastructure by focusing on providing appropriate platforms for the business applications in line with the defined IT architecture and technology standards is achieved by:

- Producing a technology acquisition plan that aligns to the technology infrastructure plan
- Planning infrastructure maintenance
- Implementing internal control, security and auditability measures

And is measured by the:

- Percent of platforms that are not in line with the defined IT architecture and technology standards
- Number of critical business processes supported by obsolete (or soon to be) infrastructure
- Number of infrastructure components that are no longer supportable (or will not be in the near future)'

1.2.3 Control process AI5 Procure IT resources states, 'Control over the IT process of procure IT resources that satisfies the business requirement for IT of improving IT's cost-efficiency and its contribution to business profitability by focusing on acquiring and maintaining IT skills that respond to the delivery strategy, an integrated and standardised IT infrastructure, and reducing IT procurement risk is achieved by:

- Obtaining professional legal and contractual advice
- Defining procurement procedures and standards
- Procuring requested hardware, software and services in line with defined procedures

And is measured by the:

- Number of disputes related to procurement contracts
- Reduced purchasing cost
- Percent of key stakeholders satisfied with suppliers
- Percent of platforms'

1.2.4 Control objective AI3.1 states, 'Produce a plan for the acquisition, implementation and maintenance of the technological infrastructure that meets established business functional and technical requirements and is in accord with the organisation's technology direction. The plan should consider future flexibility for capacity additions, transition costs, technical risks and the lifetime of the investment for technology upgrades. Assess the complexity costs and the commercial viability of the vendor and product when adding new technical capability'.

1.3 COBIT Reference

1.3.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices.

1.3.2 The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment. To meet the requirement, the processes in COBIT most likely to be relevant, selected and adapted are classified below as primary and secondary.

1.3.3 Primary:

- PO1—Define a strategic IT plan.

- PO3—Determine technological direction.
- PO5—Manage the IT investment.
- PO8—Manage quality.
- PO9—Assess and manage IT risks.
- PO10—Manage projects.
- AI1—Identify automated solutions.
- AI3—Acquire and maintain technology infrastructure.
- AI5—Procure IT resources.
- DS1—Define and manage service levels.
- DS3—Manage performance and capacity.
- DS4—Ensure continuous service.
- DS5—Ensure systems security.
- DS7—Educate and train users.
- M1—Monitor and evaluate IT performance.
- M2—Monitor and evaluate internal control.
- ME3—Ensure regulatory compliance.

1.3.4 Secondary:

- PO6—Communicate management aims and direction.
- AI6—Manage changes.
- DS9—Manage the configuration.
- DS10—Manage problems.
- DS11—Manage data.

1.3.5 The information criteria most relevant to biometric controls are:

- Primary—Effectiveness, efficiency and availability
- Secondary—Confidentiality, integrity and reliability

1.4 Purpose of the Guideline

1.4.1 The traditional means of identification and authentication—the keystones to access control—is based on 'something you know', such as a personal identification number (PIN) or password and 'something you have', such as smart cards or automated teller machine (ATM) cards. Apart from the need to rely upon ones memory either to memorise the password or to carry the card, both these approaches do not distinguish the person in a unique manner. Passwords and token-based systems have their drawbacks and often lead to bottlenecks, especially during crisis. With the advancement of technology, there is a paradigm shift toward a more reliable means of access control to 'something you are', i.e., biometric-based access controls.

1.4.2 Accuracy is the critical characteristic of a biometric access control system. Usually identification is a 'one-to-many' search of an individual's characteristics from a database of stored images, while authentication is a 'one-to-one' search to verify a claim to an identity made by an individual. A biometric is normally applied for identification in physical access controls and for authentication in logical access controls. The system fails if it is not able to separate an authentic person from an impostor. It is important that the incidence of either a false rejection (false negative) or a false acceptance (false positive) is low and at a rate considered acceptable to the organisation as a result of a cost/risk assessment.

1.4.3 With increased deployment of security architecture incorporating biometric technology, it has become imperative that the IS auditor be aware of the risks and countermeasures related to such technology. The IS auditor reviewing a system of biometric controls should have good insight into the technology, business process and control objective to ensure that the business objectives are achieved.

1.4.4 It is in this context that there is a need for a guideline to provide guidance to IS auditors who review biometric controls while carrying out audit assignments.

1.5 Guideline Application

1.5.1 This guideline provides guidance in applying IS Auditing Standard S6 Performance of Audit Work and S10 IT Governance.

1.5.2 The IS auditor should consider this guideline in determining how to achieve implementation of the previously mentioned standards, use professional judgement in its application and be prepared to justify any departure.

1.5.3 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards and guidelines.

2. BIOMETRIC CONTROLS

2.1 Introduction

2.1.1 The word 'biometric' is derived from the Greek words 'bio' and 'metric' meaning 'life measurement'. It is defined as the automated identification or verification of an individual based on physiological or behavioural characteristics. The science of biometrics exploits the advantage of uniqueness of an individual's physiological or behavioural characteristics.

2.1.2 Biometric controls refer to the use of individual's physiological or behavioural characteristics to design policies, procedures, practices and organisational structures to provide reasonable assurance that business objectives, with reference to identification and authorisation, are achieved and that undesirable events will be prevented or detected and corrected.

2.1.3 Typically biometric systems perform the functions listed in **figure 1**.

Figure 1—Typical Biometric System Functions	
Enrollment	The enrollment process requires the intended user to provide the system a biometric sample that will be digitally converted and stored in a repository as a reference template. Many biometric systems use multiple samples, and the average of all the templates is used in the creation of a reference template.
Data storage	Individual reference templates are stored in an accessible repository for verification of the user's biometrics during real-time access. Storage can be local in the biometric device, remote in a central repository, in portable tokens such as smart cards, or a combination of these methods.
Data acquisition	Data are acquired for identification and authentication of valid users to gain access. Data are acquired every time the user wishes to gain access.
Transmission	A transmission channel is used by the system to transmit the data acquired for the purpose of identification and authentication. This channel may be internal to the biometric system or external such as a local area network (LAN).
Signal processing	Signal processing or image processing involves the matching and validating of the data acquired with the data stored. The reference template stored in the repository is matched with the data acquired, and the result is based upon the quality of matching.
Decision	This is the function where a 'match' or 'no match' decision is made for allowing or denying access to the user.

2.2 Identification vs. Authentication

2.2.1 Biometrics is the automated process for identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.

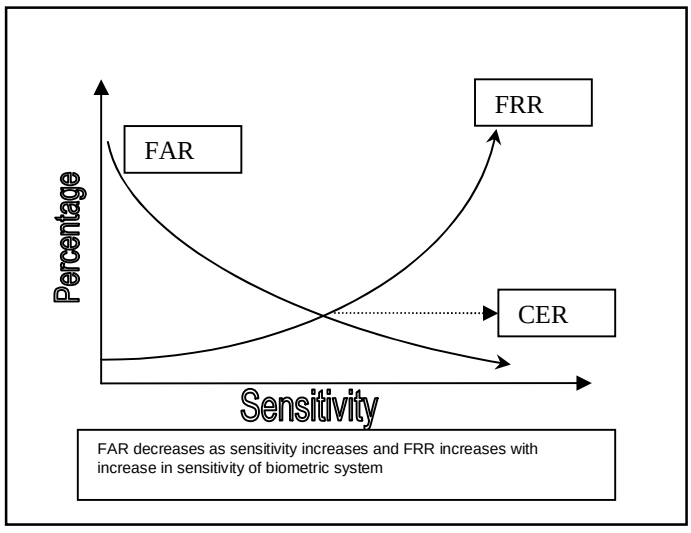
2.2.1 In biometrics, identification involves a one-to-many search of individual characteristics from the repository of data. Authentication in biometrics involves the one-to-one search to verify a claim to an identity made by the individual.

2.2.2 Typically, a biometric uses identification in physical controls and authentication in logical controls.

2.3 Performance Measures

2.3.1 Performance measures are designed to provide a baseline for help in evaluation of products. IS auditors should consider these measures in evaluating the performance of the biometric systems during the course of the audit assignment. The primary measures in biometric systems are as follows and shown in **figure 2**.

Figure 2—Sample Graph of FAR, FRR and CER (illustrative)



2.3.2 False rejection rate (FRR) or type I error—The measure of the percentage of times a valid subject has been falsely rejected by the system. FRR (%) = number of false rejections * 100/total number of unique attempts.

2.3.3 False acceptance rate (FAR) or type II error—The measure of the percentage of times an invalid subject has been falsely accepted by the system. FAR (%) = number of false acceptance * 100/total number of unique attempts.

2.3.4 Cross-over error rate (CER)—A measure representing the percent at which FRR equals FAR. This is the point on the graph where the FAR and FRR intersect. The cross-over rate indicates a system with good balance over sensitivity and performance.

2.3.5 Enrollment time—The time taken to initially enroll a new subject with a system by providing samples for creation of reference templates.

2.3.6 Failure to enroll rate (FTER)—Used to determine the rate of failed enrollment attempts. FTER = number of unsuccessful enrollments/total number of users attempting to enroll.

2.3.7 Throughput rate—The time taken by the system to validate transaction data with the data in repository to process the identification or authentication function. This is the rate at which enrolled subjects are processed for acceptance or rejection by the system.

2.4 Types of Biometric Systems

2.4.1 Biometric systems are broadly classified under two categories; one based on physiological characteristics, i.e., 'what we are' and the other based on behavioural characteristics, i.e., 'what we do'.

2.4.2 Various biometric systems based on physiological characteristics are listed in **figure 3**.

Figure 3—Biometric Systems Based on Physiological Characteristics	
Biometric System	**Data Enrollment/Acquisition**
Fingerprint	An image is obtained when the subject firmly presses his/her finger against a glass or polycarbonate plate.
Fingertip	Blood vessel pattern under the skin is captured.
Finger joint	Finger section between first and second joint is captured.
Hand geometry	Vertical and horisontal images are simultaneously captured by cameras to obtain a three-dimensional record of the length, width and height of the hand and fingers.
Retina scan	An image of the blood vessel pattern of the retina on the inside rear portion of the eyeball is captured by a camera.
Iris recognition	An image of the iris (coloured portion of the eye surrounding the pupil) is captured by a camera.
Wrist veins	The vein pattern on the wrist is captured.
Knuckle creases	Knuckle crease patterns are captured while grasping a bar.
Face recognition	Facial images are captured by high-quality cameras.
Facial thermograph	Heat patterns of the facial tissue are captured using thermal devices.

2.4.3 Various biometric systems based on behavioural characteristics are listed in **figure 4**.

Figure 4—Biometric Systems Based on Behavioural Characteristics	
Biometric System	**Data Enrollment/Acquisition**
Voice recognition	Voice is digitally converted into voiceprint and stored in binary numbers.
Keystroke dynamics	The subject's dwell time (length of time the key is held down) and flight time (time taken to move between keys) are measured.
Signature dynamics	The subject's signature is compared, and speed, pressure and timing during signature are monitored.

2.5 Data Storage

2.5.1 Reference templates should be stored in an accessible repository for easy retrieval and comparison.

2.5.2 Local storage within the biometric reader device enables quick availability of reference templates and faster matching and allows flexibility in deployment. However, the system will require re-enrollment upon system crash if not adequately supported by the backup and restore process.

2.5.3 Large organisations store reference templates in a central repository that allows users to enroll at central locations and be recognised by networked biometric devices. A central repository allows backup, restore and auditable features. Retrieval will be relatively slower, especially where the data size/volume is large.

2.5.4 Reference templates should be stored on smart cards where the user carries the biometric reference samples and the user is responsible for the privacy, confidentiality, availability and integrity of the reference template. Smart cards may also have additional security features, such as encryption and digital signatures to further secure the device.

2.5.5 Confidentiality and integrity of data should be managed so that personal information is protected from unauthorised access.

2.6 Risks and Controls in Biometric System

2.6.1 The IS auditor should be aware of the risks and control measures typical to the biometric system. The most common risks and countermeasures are listed in **figure 5**.

Figure 5—Common Biometric System Risks and Countermeasures		
Risks	**Examples**	**Possible Countermeasures**
Spoofing and mimicry attacks	Artificial finger used on fingerprint biometric device	Multimodal biometrics, vitality detection, interactive authentication
Fake template risk	Fake template stored in server	Encryption, intrusion detection system (IDS), smart cards
Transmission risk	Data intercepted during transmission during enrollment or data acquisition	Interactive authentication, rejection of identical signals, system integration
Cross-system risk	The same template used in different applications with different security levels	Hash functions, encoding algorithms
Component alternation risk	Malicious code, Trojan, etc.	System integration, well-implemented security policy
Enrollment, administration and system use risk	Data altered during enrollment, administration or system use	Well-implemented security policy
Noise and power loss risk	Flashing light to optical sensor, changing temperature or humidity of fingerprint	Well-implemented security policy
Power and timing analysis risk	Power analysis and differential power analysis garner data on biometric template.	Noise generators, low power consumption chips in biometric devices
Residual characteristic risk	Fingerprint remaining on the sensor copied by various means	Technology assessment, multimodal access

Figure 5—Common Biometric System Risks and Countermeasures		
Risks	**Examples**	**Possible Countermeasures**
Similar template/similar characteristics risk	An illegitimate user has a template similar to a legitimate user.	Technology assessment, multimodal access, calibration review
Brute-force attack risk	An intruder uses brute force to deceive the system.	Account lock after number of unsuccessful attempts
Injection risk	Captured digital signal injected into authentication system	Secure transmission; heat sensor activated scanner (warm body present); date/time stamps in digital representation of images
Users' rejection	The invasive nature of biometrics techniques could cause users to reject using the system.	Training and awareness of users and the selection of the least intrusive technique possible
Changes in physical characteristics	Some techniques depend on face or hand characteristics, but these human aspects change with the years.	Monitoring of CER
Cost of integration with other legacy systems	Coherence with other techniques used for legacy systems than have to be integrated	Cost-benefit analysis
Risk of loss of data	Hard disk/hardware failure	Data backup and restoration

3. AUDIT PROCEDURE

3.1 Selecting and Acquiring the Biometric System

3.1.1 The IS auditor should consider reviewing the following processes relating to selecting and acquiring a biometric system:

- The goals of installing the biometric system, and alignment of these goals to the business objectives of the organisation
- The study on the selection of the biometric system, based on risk analysis and asset classification, including consideration of privacy and legal matters
- The risk analysis impacts and mitigation plan
- The impact on business from the use of biometric controls
- The effect of biometric controls on employees, customers and business partners
- The return on investment for a biometric system vs. traditional access systems, such as user ID and password authentication
- The obsolescence of the biometric product
- The compliance of the product to industry and national/international standards
- The market analysis of product performance and supplier service support
- Vendor certification and product certification
- The intrusiveness of the system for data collection
- User acceptability within similar industry and in other industry/organisations
- Legal considerations and users' rights (privacy)

3.2 Operation and Maintenance of the Biometric System

3.2.1 The IS auditor should consider reviewing the following aspects relating to operation and maintenance of the biometric system:

- The biometric policy and its alignment to the security policy of the organisation
- The security confidentiality, integrity and availability (CIA) of biometric information, restricted access to data repository
- Monitoring the efficiency of the biometric system through analysis of data, such as enrollment time, success rates, failure rates, throughput time, down time, false positives, false negatives, mean time between failure (MTBF), mean time to repair (MTTR) and FTER
- The interface of the biometric system with other applications and systems (e.g., single sign-on)
- Interface with other biometric systems in the organisation
- Analysis of operation and maintenance cost
- Data storage capacity requirements
- Data security, backup and restore procedures
- Upgrade and patch management
- Destruction of user records after termination from the company
- Business continuity in case of biometric system failure and availability of standby systems/compensating controls
- Appropriate change control where role-based access is used

3.3 User Training and Acceptance

3.3.1 The IS auditor should consider reviewing the following aspects relating to user training and acceptance of the biometric system:

- Communication of biometric policy within the organisation
- Commitment to securing the biometric information and privacy of genuine users

- Commitment to relevant privacy and biometric laws and regulations
- Awareness by the users of the biometric authentication system
- Identification of owner roles and responsibility for the biometric system
- Identification of training needs, training schedule, help desk and support service
- Training on usage of the system, protection, and system and self hygiene
- Availability of documented training material and sign boards
- Acceptance by users of the system in the organisation
- Risk of uncooperative users to damage or sabotage the system

3.4 System Performance

3.4.1 The IS auditor should consider reviewing the following aspects relating to system performance of the biometric system:

- Interface of the system with applications
- Process for enrollment, re-enrollment and removal of users
- Subject and system contact requirements
- Testing, verification, validation and approval of the system
- Testing of access definition and administrator privileges
- Protection against tampering or sabotage
- Protection against compromise of data
- Backup of data
- Business continuity planning (BCP) in case of system failure and testing of BCP
- Periodic testing (e.g., brute force)
- Resistance to counterfeiting and reliability over prolonged usage

3.5 Application and Database Controls

3.5.1 The IS auditor should consider reviewing the following aspects relating to access controls and configuration settings of the biometric system:

- Platform security configuration settings, including restricting access to all biometric information of individuals to only those with a current and strict business need
- Intrusion detection controls
- Transaction controls
- Encryption of network, including lines
- Encryption of stored data in repository
- Change management (software and hardware)
- Database administration and maintenance
- Installation of hardware and software

3.6 Audit Trials

3.6.1 The IS auditor should consider reviewing the following aspects relating to audit trail of biometric system:

- Access log
- Activity log
- Change log
- Log of denial of access
- System downtime log

4. AUDIT CONSIDERATIONS

4.1 Historic Concerns Over Biometric System Use

4.1.1 The following are concerns that need to be addressed when considering the use of biometrics:

- Privacy concerns—Certain health events such as diabetes or strokes cause changes in the blood vessel pattern in the retina. Organisations using a retina-based biometric system may improperly obtain health information that may be used to the detriment of the system user. All laws and regulations regarding using and capturing physical characteristics must be considered prior to installing any biometric system.
- Intrusiveness of data collection—The user's sensitivity to intrusion into his/her personal space during a scan
- Perceived health maladies—Concern over contagious diseases by contact with a contaminated surface (e.g., fingerprint scanner)
- Skill to use the system—Certain users may not have the required skill (e.g., literacy or ability) to use the system or may suspect the actual performance of the system. Operating conditions (e.g., greasy hand, dusty areas) may hamper the performance of the system.

- Robustness of the system—Biometric technology is not foolproof and needs to overcome problems related to reliability of biometric applications. Impact of false rejections and acceptance, from both operational and reputation viewpoints, must be reviewed. Risk of tampering and sabotage by insiders also cannot be ruled out.
- Cost of deployment—Cost of deploying biometric devices on every access point may be expensive and may consume resources.
- Accuracy—The possibility of unauthorised users gaining access and authorised users being denied access exists.
- Resistance to change—There may be instances of users who are resistant to use biometric systems.
- Local regulatory and statutory requirements with respect to use of biometric systems and acceptability of system to the using community

5. EFFECTIVE DATE

5.1 This guideline is effective for all IS audits beginning on or after 1 February 2007. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary*.

References

IT Governance Institute, *Risk and Control of Biometric Technology*, USA, 2004

G37 Configuration Management Process

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, 'IS audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met. During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.2 Linkage to COBIT 4.1

1.2.1 Control process AI2 *Acquire and maintain application software* states, 'Control over the IT process of acquiring and maintaining application software that satisfies the business requirement for IT of aligning available applications in line with business requirements, and doing so in a timely manner and at a reasonable cost by focusing on ensuring that there is a timely and cost-effective development process is achieved by:

- Translating business requirements into design specifications
- Adhering to development standards for all modifications
- Separating development, testing and operational activities

'And is measured by:

- Number of production problems per application causing visible down time
- Percentage of users satisfied with functionality delivered'

1.2.2 Control process DS9 *Manage the configuration* states, 'Control over the IT process of manage the configuration that satisfies the business requirement for IT of optimising the IT infrastructure, resources and capabilities, and accounting for IT assets by focusing on establishing and maintaining an accurate and complete repository of asset configuration attributes and baselines, and comparing against actual asset configuration is achieved by:

- Establishing a central repository of all configuration items
- Identifying configuration items and maintaining them
- Reviewing integrity of configuration data

'And is measured by:

- Number of business compliance issues caused by improper configuration of assets
- Number of deviations identified between configuration repository and actual asset configurations
- Percent of licences purchased and not accounted for in repository'

1.2.3 Control objective DS 9.1 *Configuration repository and baseline* states, 'Establish a supporting tool and a central repository to contain all relevant information on configuration items. Monitor and record all assets and changes to assets. Maintain a baseline of configuration items for every system and service as a checkpoint to which to return after changes.'

1.2.4 Control objective DS 9.2 *Identification and maintenance of configuration* items states, 'Establish configuration procedures to support management and logging of all changes to the configuration repository. Integrate these procedures with change management and problem management procedures.'

1.2.5 Control objective DS 9.3 *Configuration integrity review* states, 'Periodically review the configuration data to verify and confirm the integrity of the current and historical configuration Periodically review installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements. Report, act on and correct errors and deviations.'

1.3 COBIT Reference

1.3.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices.

1.3.2 The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment. To meet the requirement, the processes in COBIT likely to be the most relevant selected and adapted are classified as:

- Primary:
  - PO9 *Assess and manage IT risks*
  - AI6 *Manage changes*
  - DS9 *Manage the configuration*
  - ME2 *Monitor and evaluate internal control*
- Secondary:
  - PO1 *Define a strategic IT plan*
  - PO3 *Determine technological direction*
  - PO6 *Communicate management aims and direction*
  - DS4 *Ensure continuous service*

1.3.3 The information criteria most relevant to configuration management are:

- Primary: Effectiveness
- Secondary: Efficiency, availability, reliability

1.3.4 The IT governance focus areas most relevant to configuration management are:

- Primary: Value delivery
- Secondary: Risk management

1.4 Purpose of the Guideline

1.4.1 Managing the configuration means providing reasonable assurance that the integrity of hardware and software configurations that requires establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimises production issues and resolves issues faster.

1.4.2 Modern businesses are organised as a set of core processes. Almost every organisation in the world is faced with increasing pressure for effectiveness and efficiency (i.e., higher quality requirements for products and services, increased revenue, cost reduction, new product development), a pressure for better, faster and cheaper enterprisewide system and network change control process that provides high quality software for the business owners. However, changing various components, such as desktop software, networks, middleware, system software for operating system and database, introduce significant risk should be managed.

1.4.3 This guideline is intended to aid the IS auditor in performing review of configuration management process. Primarily intended for IS auditors—internal as well as external auditors—this document can be used by other IS professionals with responsibilities for information system availability, data integrity and information confidentiality.

1.4.4 This guideline describes configuration management from a:

- Process flow
- Roles and responsibilities
- Asset tracking and tools
- Control and logging of changes
- Communication requirements including release management
- Metrics to be reported

1.5 Background and General Process Flow

1.5.1 The goal of the configuration management process is to:

- Manage and effectively control change to the enterprise IT systems, resources and networks while maintaining or improving system availability.
- Increasing accuracy of predications of effect and managing risks that changes can cause.
- Creating and maintaining a central repository of all configuration items and historical information of the effect from of changes to the baseline configuration (e.g., success or failure of specific types of changes especially in large scale and complex environments)
- Communicating the number of and types of changes planned in the short and long term. Thereby establishing a process that communicates the status and existence of changes to all affected parties.

1.5.2 Effective configuration management enables management to reduce the risk of requiring back-out due to inadequate preparation and/or incompatible changes affecting system availability and data processing integrity.

2. AUDIT CONSIDERATIONS

2.1 Typical Configuration Management Review Points

2.1.1 Depending upon the size and complexity of the organisation, the IS auditor should gather audit evidence of a configuration management control process. The IS auditor should obtain senior management expectations regarding configuration management. Typically, weak configuration management poses a significant threat to system availability and data integrity. Specifically, there is a high correlation between configuration changes to enterprise systems, resources and networks and critical system outages and/or poor data integrity and/or lack of confidentiality of organisation information.

2.1.2 The IS auditor should understand the configuration management policy and procedure that outlines communication requirements, including documentation requirements for changing software and hardware of individual component to the enterprise systems and networks.

2.1.3 The IS auditor should obtain a general understanding of all elements, including all software such as business application software, middleware, and database system software and hardware interrelationships and integration, that comprise the enterprise systems and networks. For example, the hardware type, model number and serial number for uniqueness identification.

2.1.4 The IS auditor should obtain all hardware and software information (model and serial number) from the IT asset tracking system or comparable information that is verified as complete. If this is not available, a complete inventory may need to be taken.

2.1.5 The IS auditor should understand the relevance of each component and how it fits together including the interrelationships with all other components.

2.1.6 Review of configuration management process typically includes:

- Verifying the establishment of central repository of all configuration items
- Identifying configuration items and maintaining configuration data
- Determining whether the repository contains all necessary information about components, interrelationships and events
- Determining whether the configuration data is aligned with vendor/service provider catalogues
- Determining whether there is a complete integration of interrelated processes, and organisation uses and updates configuration data in an automated fashion
- Providing reasonable assurance of the integrity of configuration data
- Verifying the existence of formal change request to the system including complete change documentation
- Determining whether a formalised method is consistently employed of identifying and categorising changes into levels of risk to the enterprise systems, resources and networks

- Determining audit evidence of risk assessments of the requested change as deemed necessary by the configuration management committee, or appropriate level of the management. Risk assessment should denote if the change is restricted to specific environments or networks and the potential number of business users affected and the criticality of the business information processing.
- Verifying business and IT management formal approval of results of the risk assessment (i.e., changes to firewall rule settings)
- Determining that there is controlled development or installation of vendor upgrade of the change in a development (i.e., systems engineer's sandbox)
- Testing resulting in a required unqualified sign-off of configuration changes in a test environment, which mirrors the production environment in infrastructure and business software, noted no effect on other elements of the enterprise systems, resources and networks
- Scheduling of changes based on coordination of other changes to minimise potential effect to the enterprise systems, resources and networks. This scheduling occurs through release management sub-process that controls batching of the software program elevations including synchronising of changes that minimises the effect on the business.
- Determining that the elevation of the change into the production processing environment is made in a controlled manner (off hours) where there is additional testing of the change in the live production processing environment (i.e., upgrade of database system software is evaluated by executing critical stored procedures and triggers with an evaluation of data integrity)
- Establishing repository of all assets, configuration attributes and baselines. Verify that a baseline of configuration items is kept as a checkpoint to return to after changes.
- Verifying the baseline report provides essential hardware and software data for repair, service, warranty, upgrade and technical assessment of each individual component
- Reviewing actual asset configuration for compliance with baselines in the repository and establish integrity of the configuration repository
- Determining whether rules are in place and enforced for preventing the installation and for detecting unauthorised software .
- Determining whether there is a system to forecast repairs and upgrades that also provides scheduled upgrades and technology refreshment capabilities
- Providing reasonable assurance of a linkage between the change management process and configuration management so that all aspect of changes are understood in the configuration review process

2.2 Roles and Responsibilities

2.2.1 The IS auditor should obtain a listing of roles and responsibilities that support configuration management. These roles and responsibilities should be embedded in job descriptions of IT management responsible for each IT component and the correlated scope. If this is not present, the IS auditor should investigate responsibility for configuration management (i.e., identification of the overall process owner).

2.2.2 Obtain and verify that management has identified resources to measure the number and nature of changes being made to the enterprise systems, resources and networks.

2.2.3 Accountability is established regarding 1st and 2nd tier support for configuration changes.

2.3 Assets Tracking and Tools

2.3.1 Assets should be tracked and individual assets should be monitored to protect them from theft, abuse or misuse.

2.3.2 Software should be labeled, inventoried and appropriately licensed. Library management software should be used to produce audit trails of program changes and to maintain program version numbers, creation-date information and copies of previous versions.

2.3.3 The IS auditor should obtain a listing of all authorised software, if possible, from the use of automated tools that scans all hardware devices including servers and desktops computers. This software provides critical details, such as:

- Hardware type and model number
- Software elements, including interface programs and controls to verify that Inter-operability
- Vendor software:
  - Version
  - Documentation of current vendor support requirements
  - Documentation of any customisation made from vendor provided baseline that could affect the interface with other software

2.3.4 The IS auditor should obtain an general understanding of the software acquisition controls used to verify that all software purchased is recorded in the IT asset-tracking system.

2.4 Control and Logging of Changes

2.4.1 Procedures should be in place to verify that only authorised and identifiable configuration items are recorded in the inventory upon acquisition. These procedures should also provide for the authorised disposal and consequential sale or destruction of configuration items.

2.4.2 Procedures should be in place to keep track of changes to the configuration (e.g., new item, status change from development to prototype). Logging and control should be an integrated part of the configuration recording system including reviews of change records.

2.5 Communication Requirements Including Release Management

2.5.1 Senior IT management with selected senior business management formed into a steering committee to evaluate high-risk configuration changes (i.e., business applications). Minutes should be documented including decisions regarding implementation of changes

2.5.2 The IS auditor should obtain audit evidence of a schedule of changes including a "release calendar" that denotes the dates and times

that various changes are elevated into the production-processing environment. Typically, the IS auditor should observe separation of elevation of changes, so computer operations can more essential identify system problems

2.5.3 Audit evidence of communication to business owners of significant configuration changes to be on notice to detect unusual system events.

2.6 Metrics to be Reported

2.6.1 All measurements including dashboards result from measuring the number and nature of changes being made to the enterprise, systems, resources and networks. Some typical instances for measurement:

- Average time period (lag) between identifying a discrepancy and rectifying it
- Number of discrepancies relating to incomplete or missing configuration information
- Percent of configuration items in line with service levels for performance, security and availability
- Number of deviations identified between configuration repository and actual asset configurations
- Percent of licences purchased and not accounted for in repository
- Percent of unauthorised licences vs. purchased licences in use
- Percent of business compliance issues caused by improper configuration of assets

2.6.2 Performance including service levels statistics that include response time, system uptime (availability), quality of data integrity, etc., are formally documented and circulated amongst IT management. Employee or contractor performance (in cases where IT department is outsourced) should be measured on this metrics.

2.6.3 For changes, ascertain if management measures the amount of lead-time and if it affects the success or failure of making non-disruptive changes by:

- When lead-time is important, identifying sensitive types and volumes of changes to reduce disruptions
- Determining a better method of identifying and categorising changes into levels of risk
- Verifying every record has technical and management accountability
- Establishing a process verifying records are reviewed for technical merit and business readiness in a consistent manner while allowing flexibility based on business needs

3. EFFECTIVE DATE

3.1 This guideline is effective for all information systems audits effective 1 November 2007.

G38 Access Controls

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S1 Audit Charter states, 'The purpose, responsibility, authority and accountability of the information systems audit function or information systems audit assignments should be appropriately documented in an audit charter or engagement letter'.

1.1.2 Standard S3 Professional Ethics and Standards states, 'The IS auditor should adhere to the ISACA Code of Professional Ethics'.

1.2 Linkage to Guidelines

1.2.1 G13 Use of Risk Assessment in Audit Planning states, 'The IS auditor should use the selected risk assessment techniques in developing the overall audit plan and in planning specific audits. Risk assessment, in combination with other audit techniques, should be considered in making planning decisions such as:

- The nature, extent and timing of audit procedures
- The areas or business functions to be audited
- The amount of time and resources to be allocated to an audit'.

1.3 Linkage to CobiT

1.3.1 The control process ME2 *Monitor and evaluate internal control* states: control over the IT process of monitor and evaluate internal control, which satisfies the business requirement for IT of protecting the achievement of IT objectives and complying with IT-related laws and regulations by focusing on monitoring the internal control processes for IT-related activities and identifying improvement actions, is achieved by:

- Defining a system of internal controls embedded in the IT process framework
- Monitoring and reporting on the effectiveness of the internal controls over IT
- Reporting control expectations to management for action

ME2 is measured by:

- Number of major internal control breaches
- Number of control improvement initiatives
- Number and coverage of control self-assessments

1.3.2 ME3 *Ensure compliance with external requirements,* which satisfies the business requirement for IT of ensuring compliance with laws, regulations and contractual requirements by focusing on identifying all applicable laws, regulations and contracts and the corresponding level of IT compliance and optimising IT processes to reduce the risk of non-compliance, is achieved by:

- Identifying legal, regulatory and contractual requirements related to IT
- Assessing the impact of compliance requirements
- Monitoring and reporting on compliance with these requirements

ME3 is measured by:

- Cost of IT non-compliance, including settlements and fines
- Average time lag between identification of external compliance issues and resolution
- Frequency of compliance reviews

1.3.3 ME4 *Provide IT governance*, which satisfies the business requirement for IT of integrating IT governance with corporate governance objectives and complying with laws, regulations and contracts by focusing on preparing board reports on IT strategy, performance and risks, and responding to governance requirements in line with board directions, is achieved by:

- Establishing an IT governance framework integrated into corporate governance
- Obtaining independent assurance over the IT governance status

ME4 is measured by:

- Frequency of board reporting on IT to stakeholders (including maturity)
- Frequency of reporting from IT to the board (including maturity)
- Frequency of independent reviews of IT compliance

1.4 CobiT Reference

1.4.1 Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of CobiT's control objectives and associated management practices. To meet the responsibility, authority and accountability requirement of IS auditors, the processes in CobiT most likely to be relevant, selected and adapted are classified below as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.4.2 The specific objectives or processes of CobiT that should be considered as primary when reviewing the area addressed by this guidance:

- PO1 *IS risk assessment*
- PO2 *Define the information architecture*
- PO9 *Assess and manage IT risks*
- DS5 *Ensure systems security*

- DS7 *Educate and train users*
- DS9 *Manage the configuration*

1.4.3 The specific objectives or processes of CobiT that should be considered as secondary when reviewing the area addressed by this guidance:

- PO6 *Communicate management aims and direction*
- PO7 *Manage IT human resources*
- AI1 *Identify automated solutions*
- AI2 *Acquire and maintain application software*
- AI3 *Acquire and maintain technology infrastructure*
- AI6 *Manage changes*
- DS1 *Define and manage service levels*
- DS2 *Manage third-party services*
- DS10 *Manage problems*
- DS12 *Manage the physical environment*
- ME1 *Monitor and evaluate IT performance*
- ME3 *Ensure compliance with external requirements*

1.4.4 The information criteria most relevant to responsibility, authority and accountability are:

- Primary: Effectiveness, efficiency and confidentiality
- Secondary: Availability, integrity and reliability

1.5 Purpose of the Guideline

1.5.1 In the actual interconnected world, organisations should protect their assets from unauthorised use, not only to protect its investments but also to protect information assets from the risks generated by the misuse of resources, intentionally or unintentionally. Actual technology implementations are diverse and complex (e.g., platforms, applications, utilities, operating systems, databases, e-mail utilities, security and audit tools, Internet, faxes) and all of them have to be protected from unauthorised use. Physical assets, such as buildings, equipment, telecommunications, photocopiers, cameras, file cabinets, general printing information and customer documentation must also be protected. Due to this diversity, it is critical to have one standard process to control access. This standard will operate as a baseline, customised to address the particular needs of the organisation.

1.5.2 This guideline provides guidance in applying IS auditing standards S1 and S3. The IS auditor should consider this guideline in determining how to achieve implementation of the above standards, use professional judgment in its application and be prepared to justify any departure.

1.6 Guideline Application

1.6.1 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards and guidelines.

1.7 General Categories of Access

1.7.1 Minimal access—User access only to the specific resources needed

1.7.2 Need to know basis—User access to the resources needed to perform the work for the organisation, not for personal interest

1.7.3 Owner—User responsible for the asset

2. GENERAL DEFINITIONS

2.1 Security Policy

2.1.1 A security policy is a high-level document that describes management's and organisations' responsibility and defines the security strategy to comply with business objectives. Standards and procedures should be written for complete implementation. Standards define 'what' should be done to comply with the policy and are intended for all audiences. Procedures describe 'how' it should be done and are intended for those who have to implement the policy (e.g., users, technology, vendors). These could be organised in separate documents or could be consolidated in an 'access control policy'.

2.1.2 There are many sources of information to consider when writing a security policy. Each organisation should assess the information in relation to its business, need for protection and culture, and adopt that which best meets its objectives. The policy should be written by business and security specialists and approved by high-level management or directors before it is communicated to and signed by all employees.

2.2 Criteria to Define Access Rules

2.2.1 In general, the criteria should be based on the principle of need-to-know. Each organisation must define a level of access appropriate for each group of employees, vendors, customers, regulators and auditors (e.g., role-based access). A complete inventory of information assets should be made, considering the importance of the information, vulnerability, existing security measures in the IT environment, including equipment where the information is processed and skills or special expertise of those managing the information (intellectual property). The physical assets or resources to protect include:

- Buildings including their power and security and other infrastructure items (e.g., uninterruptible power supply [UPS], generators, cameras)
- Data centres
- Telecommunication rooms (switches, hubs, routers, private automatic branch exchanges [PABXs], cables)
- Libraries (tapes, cartridges, zips)

- Vaults/fire proof safes
- Safety boxes and key boxes
- Faxes
- Photocopiers
- Telex
- Customer documentation
- Support documentation (regulatory)

2.2.2 Organisations should consider creating and periodically reviewing matrix of access roles to verify segregation of critical duties.

2.2.3 Logical assets or resources to protect include:

- Servers (i.e., web servers, application) and their operating systems
- Database systems or file systems
- Applications
- Utilities and tools
- Magnetic cards, keys, certificates and smart cards
- Servers, workstations and PABX
- Data in general
- E-mail (corporate accounts)
- Firewall/intrusion detection systems (IDS)
- Reports
- Audit logs
- Network (security perimeter)

2.3 Ownership and Responsibilities

2.3.1 The owner for each information (and IT-related physical) asset should be defined in a formal way with assigned responsibilities. The responsibilities should encompass the information owner's duty to make sure that principles and rules for access control are made, implemented and followed by the organisation.

2.4 Assets Classification

2.4.1 Asset classification should be based on the information type managed (e.g., restricted, confidential, internal, public).

2.5 Administration

2.5.1 The access control policy should clearly define responsibilities, roles and procedures for changes in employee status, such as changes in positions and tasks, transfer within department/information security administration (ISA). It is of great importance to establish a procedure to manage changes in user status and communicate changes to information owners, users, super users, supervisors or any person/department responsible for defining, granting/eliminating or changing entitlements/privileges. A security administrator should have the overall responsibility for security administration. The term 'entitlement' is interchangeable with access granted to users.

2.6 User Controls

2.6.1 A set of controls should be defined for controlling and monitoring user activities, e.g., blocking users after a number of consecutive failed logins and blocking or deleting inactive users after a defined period of inactivity. Successfully logged in user should be provided with number of failed attempts, successful login date and time.

2.7 Entitlement Review

2.7.1 Entitlement reviews should be done at least semi-annually to verify that owners/supervisors validate the user entitlements and the changes effected. The appropriateness of the 'procedure', which requires the performance of the entitlement review, should be evaluated at least annually to verify any changes in the environment (i.e., application, external network access) that could possibily result in the need for a more frequent entitlement review are considered.

2.8 Authorised Use and Penalties

2.8.1 The policy and supporting documents (i.e., standards, guidelines) should state, while addressing other risk attributes, that organisational resources can only be used for business purposes and not for personal benefits. There should be

penalties/sanctions in case of misuse or inappropriate use of business resources.

2.8.2 The policy should encompass the regulatory framework (corporate and local), including, privacy law, data protection or bank secrecy. Also, it should state which situations, such as participation in chain letters, downloading software from Internet, using personal software on CDs/diskettes or using organization-owned information for personal benefit, are prohibited.

2.9 Non-staff Personnel

2.9.1 The policy should state functions or transactions (e.g., security transactions, authorisation) not accessible by temporary consultants or third-party personnel. Access to these functions and transactions can be accomplished by network controls, but are not accessible via corporate e-mail, dial-in access, etc.

2.10 Accountability and Password Sharing

2.10.1 The policy should state clearly that each employee is responsible for the actions done with his/her password, even if it is demonstrated that the action was carried out by another individual using that password. Passwords should have expiration dates and systems should force automatic changes. Based on all previous elements, each organisation defines access requirements according to employee's/customer's current business needs and the legal environment.

2.11 Type of Access

2.11.1 Depending on its origin, access can be classified as local or remote. Local access originates inside the organisation where the resources are physically located. Remote access originates from other locations, such as home, and is typically used for emergency change control procedures or administrator scheduled operations. In this last case, special security measures should be considered, such as configuration and antivirus software, secure connection (virtual private networks [VPN], encryption, Secure Sockets Layer [SSL]) and daily control of remote activity from home desktops.

2.11.2 Wireless or mobile device use should be minimised (not used for critical process/information) and strictly controlled. Consider complexity and the skills needed to perform access when classifying access as technical/non-technical and structured/unstructured. This is very important for risk assessment analysis and occurrence probability determination.

2.12 Requisites

2.12.1 Access to information assets should be measured against identification, authentication, authorisation or non-repudiation.

2.12.2 The user should be identified to the resource, typically with a user identification (ID) (a string of numbers and characters not less than eight positions in length), ID card or physical ID, such as a person's voice, fingerprint or iris/retina (biometric).

2.12.3 The user should be authenticated by providing the resource with one secret item that demonstrates who he/she is. Depending on classification and risk evaluation, authentication can be made by static passwords, dynamic passwords or one-time passwords (tokens), biometrics, personal identification numbers (PINs)/trading partner identification numbers (TPINs). Authentication is accomplished by using 'something that you know', 'something that you have' or 'something that you are'. Security is stronger with a combination of factors, e.g., an automatic teller machine (ATM) that uses two-factor authentication—something that you know (PIN) and something that you have (card). As an example, an access control policy should include tables such as the following table.

	Technique			
Information classification, risk evaluation and application usage, and type of access	**PIN/TPIN**	**Static Passwords**	**One-time Passwords**	**Biometrics**
Public information, low risk, not transactional applications, internal access	S	D	D	D
Confidential information, medium risk, transactional applications and internal access	I	I	D	D
Restricted information, high risk, transactional applications and remote access (web)	I	I	S	D

Legend: S—Sufficient, I— Insufficient, D—Desired

2.12.4 If identification/authentication is approved, the system permits access to the specific resource in question. This is accomplished by different techniques depending on type of resource, for example:

- For buildings, rooms, vaults and data centres—User access cards, PINs and biometrics
- For customers documents, cabinets and faxes—User access keys, cards and supervisor memos
- Firewalls and proxies are equipment assets that allow access to other resources, and because they are very important, they should be given special protection. They should have both physical and logical protection such as only administrator role usage, change in configurations, and usage of alarms and logs. In all cases, each company must analyse its needs depending on what services (e.g., web services, e-mail, FTPs) are in use and follow standards/best practices recommendations (e.g., disable port 80). To achieve this objective, it is important that each company considers a vulnerability and threat management procedure, which includes the subscription of one or more security bulletins (i.e., CERT, SANS, Microsoft, National Institute of Standards and Technology [NIST]).
- IDSs/active defense systems (ADSs)/intrusion prevention systems (IPSs) are equipment and software that detect and analyse suspicious traffic; they must be configured to generate alarms/logs that need to be reviewed immediately. It is important to implement a process for the review of logs and alarms received, the analysis of which indicates changes of configurations depending on the risk of the threats.
- Application, operating system and database management system (DBMS) user profiles defined at the application/DBMS level. Each user is assigned a user privilege and this is placed on the access controls lists (ACL).
- End-user computing for Excel spreadsheets, Access tables and Fox/Dbase files, if they exist, should be protected with sheets passwords, user privileges, cell passwords, etc. It is recommended not to use these tools for critical processes because the security controls they provide (i.e., password protection) may not be as strong as those built into the applications/DBMS.

2.12.5 Non-repudiation is intended to verify that somebody who made a transaction cannot deny it. It is accomplished by digital signatures and logs.

2.13 Risk Assessment

2.13.1 Access Risk assessments should be performed on an ongoing basis according to the nature of threats and changes to the threat scenario.

2.13.2 Poor access control practices can lead to unauthorised disclosure of confidential information (confidentiality), unauthorised changes to data (integrity) or loss of continuity of business (availability). The consequences of not having appropriate access controls in place should be considered based on the value of the asset to the organisation from a quantitative perspective as well as a qualitative perspective, e.g., reputation loss, customer perceptions, inability to comply with obligations, compromises (contracts, service level agreements [SLAs]), regulatory effect (fines and penalties), financial effect, competitive loss and revenue/income loss. To minimise this risk, preventive controls should be implemented (according to policy) to reduce risk to a level that is acceptable to the business (residual risk). Detective controls are also required to secure the process.

2.13.3 The degree of trust required for a given system is determined by the value of the information assets and the *perceived risk* to those assets.

2.14 Risk Monitoring and Metrics

2.14.1 Access risk indicators should be defined by methodologies, such as control risk self-assessment. Some examples include:

- Number of external intrusion attempts (failed or succeed)
- Number of internal unauthorised attempts
- Number of security incidents caused by unauthorised access
- Number of entitlement reviews not in compliance
- Number of inadequate access request approvals

2.15 Specific Threats to Access

2.15.1 Organisations, depending on their products/services/applications, should analyse their exposure to social engineering, phishing, identity theft, denial-of-service attacks, web spoofing and cross-site scripting. Based on the potential threat exposure, they should consider special measures for web applications and infrastructure (e.g., web standards policy, ethical hacking).

2.15.2 The organisation should be prepared to react appropriately to a breach of access including unauthorised intrusion.

2.16 Preventive Controls

2.16.1 Preventive controls include:

- System access should be authenticated by the use of a strong password (rules for password length and complexity, change frequency, password sharing, etc.).
- Formal approval should be required by the business owner before access is granted to business information resources.
- An access control policy should be communicated to and signed by all employees considering regulatory requirements (corporate and local levels) and implementation of access controls techniques according to policy
- Staff agreements for correct use of resources (human resources) should be signed
- A programme to train, communicate and make staff aware of correct access and measures for non-compliance should be in place.
- Procedures should exist to define, approve process, revoke, eliminate, change, communicate, log and audit access, approved by owners and supervisors.
- User administration procedures, including daily controls over the administration function should be in place.
- All vendor-supplied user IDs, where there is no business need, should be removed.
- For those vendor-supplied user IDs with a business need, the initial default password changes should be required.
- Access control tools, such as audit tools, firewalls and IDs, should exist.
- A resource use policy, including employee penalties for incorrect use (e-mail, Internet), should be in place.
- Third-party access requirements (SLAs or contracts)
- Labelling procedures, depending on risk assessment considerations
- Restrictions on access for temporary employees (security functions, transaction authorisation)
- Elimination of all platform default access/users, wherever possible
- Restricting all production service accounts from log on by users
- Encryption, which is not an access control, reducing the effect of unauthorised access
- Procedures to define access to physical resources, such as file cabinets, faxes, vaults, documents and their requirements on retention and protection
- Application of segregation of duties—dividing access to critical data between two or more persons to reach a level of mutual control
- PIN/TPIN/secure Internet password (HPIN), tokens, biometrics, user profiles, privileges, session time out, cable lock, anti-virus, anti-spyware

2.17 Detective Controls

2.17.1 Detective controls include:

- Entitlement review procedures, including escalation for non-compliance situations, and logging and review of vendor, customers, regulators and auditors.

- Activities of the privileged or superuser login account should be closely monitored and reviewed by senior computer security management.
- A security incident procedure, including roles and responsibilities and escalation procedures, should exist to manage inadequate access/abuse of resources, suspicious activity and hackers
- Audit/quality assurance reviews of entitlements, high-privilege users, functional users, default users, special groups/roles, firewall/IDS configurations, alerts and logs should be in place.
- Self-assessment methodology should be deployed to complement internal audit reviews. For example, a set of controls are integrated to the business processes and executed by each area with a frequency according to risk.
- An annual penetration test assessment should be made that includes networks, people, resources and business processes, where appropriate.
- The logs containing non-approved activities should be logged and reviewed.

2.18 Compensating Controls

2.18.1 Compensating controls should be considered where detective or preventive controls are insufficient.

2.18.2 For all of these indicators, a value trigger should be defined that permits the security manager to analyse the causes of these problems and define the management action plan to mitigate/resolve the issues (e.g., to reinforce training and to buy security tools).

2.19 Administration Access Procedure

2.19.1 Depending on local procedures, platforms, utilities and the design of access administration tools, this task could vary in organisations but in all cases should include:

- Formally documented access request for all actions (e.g., additions, deletions, resets and profiles changes) with adequate rationales and the owner's approvals should be required.
- When the administration process is manual (by form or e-mail), the user administrator that receives the request should check that approvals on the request are correct. In some cases this process has been automated through an application that contains the owner/supervisor of each resource/area and implements one automatic workflow to obtain approvals.
- The time frame for processing of each user administration operation should be defined and agreed to by the business (e.g., SLA, statement of work). For example, a user reset for critical applications must be responded to according to the SLA or in the appropriately defined time period.
- The process should define clearly the way to deliver passwords to users for additions or resets. In some cases this is automated through the application and the administrator never knows the user password. Also, it is desirable that when passwords are generated (i.e., during the addition or reset of user transactions), they should only be known to the account owner and stored with encryption, as they should be considered restricted information.
- The process to deliver PINs/TPINs to employees/customers should use a different delivery channel than the item (cards, tokens) and they should be inactive until they reach the owner who can activate them.
- A control should exist to verify that any password/PIN/TPIN is destroyed after some time period if it does not reach the owner.

2.20 Controls Over Information Security Administration

2.20.1 Activities include:

- All ISA activities should be recorded in audit logs.
- All user administration functions should be segregated from any other activities (i.e., system administration, business transactions and developer activity); otherwise, inappropriate segregation of duties will lead to conflicts of interest.
- One independent party should control all ISA activities in 24 hours or should implement maker/checker dual control to verify that only required actions are processed.
- All privileged users (administrators, DBAs) should be monitored and have a tighter control process for justification, documentation and approval.

2.21 Controls over User Activities

2.21.1 Controls over user activities include:

- Repeated failed log in attempts should be identified and investigated.
- Any blocked or suspended user ID (three or more consecutives failed attempts) should be investigated to verify that the user is the correct owner of the user ID and not an unauthorised person trying to discover passwords.
- Inactive users should be monitored and corrective action should be taken depending on the period, e.g., blocking of 60-day inactive users and deletion of 90-day inactive users.
- Activity carried out by default users (e.g., guest, administrators, owner, root) or contractors should be monitored on a daily basis. It is recommended to use security tools for this task.
- Access to data should be for a limited time period during the day, week, month or year.

2.22 Considerations to Monitor Access

2.22.1 Controls over user activities include:

- Access to critical accounts, log files, data files and databases should be monitored.
- Periodically, logs should be reviewed to monitor activities of privileged users and failed access attempts.
- E-mail use should be monitored due to the abuse that could lead to legal, privacy and ethical issues.

- The usage of privileged (system) log in accounts should be monitored and justified. Whenever possible, such users should have their own logon IDs and be assigned privileged authority (SysAdmin account) rather than use a generic ID, as it may be shared.
- For vendor-supplied security products, such as for network and server intrusion detection, and the associated logs should be reviewed daily, and alerts should be managed accordingly.

3. AUDIT PROCESS

3.1 Planning

3.1.1 An audit programme should be developed based on the organisation's risk assessment and risk management strategy, including the scope, objectives and timing of the audit. Reporting arrangements should be clearly documented in the audit programme. Consideration should be given to the nature and size of the organisation and its stakeholders. The IS auditor should gain an understanding of the organisation's mission and business objectives, the types of technical infrastructure, and business critical data.

3.1.2 An understanding of the organisational structure is needed, specifically of the roles and responsibilities of key staff, including the information managers, owners and supervisors.

3.1.3 A primary objective of the audit planning phase is to understand the threats and risks that the organisation faces when the access is incorrectly defined, approved, assigned, used or controlled.

3.1.4 Formal risk assessment methodologies should be employed to define the scope of the review with emphasis on high-risk areas.

3.1.5 Appropriate sampling techniques should be considered in the planning of the audit to quantify the results of testing, if applicable.

3.1.6 All previous audit reports should be reviewed and the level of resolution should be assessed on each issue according to the management action plan.

4. PERFORMANCE OF WORK

4.1 Audit Tasks

4.1.1 The IS auditor should consider reviewing the:

- Adherence to aforementioned preventative and detective controls, where applicable
- Organisational chart and job descriptions of all personnel with security responsibilities
- Roles associated with access to information resources to determine that they are created commensurate with current business duties
- Access authorities granted to employee accounts, including those associated with the information technology group, to determine that they are periodically validated to verify a continued business need exists
- Logon accounts assigned to employees that have been terminated to determine that they are removed as soon as possible
- Policies, criteria and process implementations to verify completeness, accuracy, updating and compliance evidence
- Approval procedure, responsibilities definition and their acceptance for security-related functions (e.g., information owners, business process owners, application owners)
- Asset inventory with classification and risk evaluations
- ISA logs and daily controls, especially for high-privilege users
- Detection, communication, escalation and resolution procedures for security incidents and their metrics during the period subject to review. Employees should be interviewed randomly to assess their awareness of the security incident procedure.
- Awareness and training programme and associated metrics
- ISA operating procedures
- Evidence of security incidents reporting, escalation and resolution of the period (if exists), lessons learned and the implemented action plan
- Justification and approvals of administrator activity and functional users rationale
- Reports from risk and vulnerability assessments
- Employee agreements and clauses signed as part of human resources procedures, typically when the working relationship begins
- Contracts signed with temporary personnel
- Reports of platform configurations (e.g., servers, desktops, host)
- Evidence of the entitlement review process for the period under review
- Firewall/IDS/IPS configuration reports
- Firewall/IDS/IPS logs for one spot
- Specific standards/guidelines (i.e., firewall, web applications)
- Service level contracts/agreements with shared/third-party service providers.

5 REPORTING

5.1 Report Generation and Follow-up

5.1.1 The draft audit report should be generated and discussed with relevant personnel. Only include those issues supported by clear evidence.

5.1.2 The report should be finalised following ISACA guidelines and presented to management with recommendations to resolve/improve issues and follow-up options.

5.1.3 Follow-up activities, action plans, responsibilities, target dates, and resources and priorities given by senior management should be agreed upon.

6. EFFECTIVE DATE

6.1 This guideline is effective for all IS audits beginning 1 February 2008.

G39 IT Organisation

1. BACKGROUND

1.3 Linkage to Standards

1.1.1 Standard S10 IT Governance states, 'The IS auditor should review and assess whether the IS function aligns with the organisation's mission, vision, values, objectives and strategies. The IS auditor should review whether the IS function has a clear statement about the performance expected by the business (effectiveness and efficiency) and assess its achievement'.

1.2 Linkage to COBIT

1.2.1 PO1 *Define a strategic IT plan* states, 'control over the IT process of *Define a strategic IT plan* that satisfies the business requirement for IT of sustaining or extending the business strategy and governance requirements while being transparent about benefits, costs and risks by focusing on incorporating IT and business management in the translation of business requirements into service offerings, and the development of strategies to deliver these services in a transparent and effective manner'.

1.2.2 PO4 *Define the IT processes, organisation and relationships*) states, 'control over the IT process of *Define the IT processes, organisation and relationships* that satisfies the business requirement for IT of being agile in responding to the business strategy while complying with governance requirements and providing defined and competent points of contact by focusing on establishing transparent, flexible and responsive IT organisational structures and defining and implementing IT processes with owners, roles and responsibilities integrated into business and decision processes'.

1.2.3 PO5 *Manage the IT investment* states, 'control over the IT process of *Manage the IT investment* that satisfies the business requirement for IT of continuously and demonstrably improving IT's cost-efficiency and its contribution to business profitability with integrated and standardized services that satisfy end user expectations by focusing on effective and efficient IT investment and portfolio decisions, and by setting and tracking IT budgets in line with IT strategy and investment decisions'.

1.2.4 ME4 *Provide IT governance* states, 'control over the IT process of *Provide IT governance* that satisfies the business requirement for IT of integrating IT governance with corporate governance objectives and complying with laws and regulations by focusing on preparing board reports on IT strategy, performance and risks, and responding to governance requirements in line with board directions'.

1.2.5 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the responsibility, authority and accountability requirement of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified below as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.7 The following specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance are secondary:

- PO2 *Define the information architecture*
- PO3 *Determine the technological direction*
- PO6 *Communicate management aims and direction*
- PO7 *Manage IT human resources*
- PO8 *Manage quality*
- PO9 *Assess and manage IT risks*
- PO10 *Manage projects*
- DS1 *Define and manage service levels*
- DS2 *Manage third-party services*
- DS3 *Manage performance and capacity*
- DS6 *Manage and allocate costs*
- DS7 *Educate and train users*
- DS8 *Manage service desk and incidents*
- DS9 *Manage the configuration*
- DS10 *Manage problems*
- DS12 *Manage the physical environment*
- DS13 *Manage operations*
- AI2 *Acquire and maintain application software*
- AI3 *Acquire and maintain technology infrastructure*
- AI6 *Manage changes*
- ME1 *Monitor and evaluate IT performance*

1.2.8 The information criteria most relevant to the IT organisation:

- Primary: Effectiveness and efficiency
- Secondary: Confidentiality, availability, integrity, compliance and reliability

1.5 Purpose of the Guideline

1.3.1 Structure can be a distinct enabler or inhibitor of organisational effectiveness but it alone will not determine organisational success. There is no one right structure, because no two organisations are exactly alike. All IT organisations serve similar purposes and have similar accountabilities, but their profiles, management systems, processes, constraints, strengths and weaknesses make each IT organisation unique. There are, however, certain attributes for verifying an optimised IT organisational structure.

1.3.2 This guideline provides guidance in applying IS Auditing Standard S10 IT Governance. The IS auditor should consider this guideline in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

1.4 Guideline Application

1.4.1 When applying this guideline, the IS auditor should consider it in relation to other relevant ISACA standards and guidelines.

2. THE IT ORGANISATION

2.1 Types of Organisations

2.1.1 The boundaries of today's organisations are more flexible and dynamic and, in most cases, more extensive. Organisations and industries realise that they must start focusing on whole processes, including those that transcend the physical walls of the organisation. They must reach out to business partners, suppliers and customers. Accurate, appropriate and timely information is the indispensable component in the new economy or what is commonly referred to as the extended enterprise. Information/knowledge-sharing activity amongst stakeholders of the extended enterprise is a key success factor in delivering workable enterprise governance. An overall competitive strategy must drive an effective knowledge management strategy and leadership. An organisation must build an appropriate information organisation to provide the information required by senior management in decision making, while maintaining an appropriate level of control over it.

2.2 IT Alignment

2.2.1 There is no one-size-fits-all approach for maximising the alignment of IT with the business and all of its components. Much depends upon the nature of the business, its size, its markets, its dependence upon IT, its leadership style and its culture. Additional factors that help dictate the organisation's alignment components and structure include the in-house IT capabilities, the dependence upon outsourcing, the nature of that outsourcing and the overall governance structure.

2.2.2 In recent years, IT has moved from providing largely back-office support to becoming the prime facilitator and enabler of the total business. Without proper alignment of IT, it is unlikely that any enterprise will achieve and sustain long-term success through the delivery of value to its stakeholders. The alignment of IT with the overall strategy of the enterprise does not happen by accident. It requires full and active involvement from many levels and activities within the enterprise, and active and focused management. It is a continuous effort and requires world-class skills and expertise, either in-house or outsourced. Risk taking, but with appropriate risk management is required along with strong and demonstrable governance.

2.2.3 Proper governance over the achievement of IT alignment requires leadership and commitment from the highest levels of the enterprise. This requires the proactive engagement of the chief executive officer and board. This requires the board to take responsibility for:

- Ensuring that IT strategy is aligned with business strategy
- Ensuring that IT delivers against the strategy
- Directing IT strategy to balance investments appropriately amongst systems that support the enterprise as it is, transform the enterprise or grow the enterprise

2.3 IT Strategic Plan

2.3.1 An organisation should establish an IT strategy committee at the board level. This committee should verify that IT governance, as part of corporate governance, is adequately addressed, advises on strategic direction and reviews major investments on behalf of the full board.

2.3.2 The IT strategy committee should create an IT strategic plan that defines, in co-operation with the relevant stakeholders, how IT will contribute to the enterprise's strategic objectives (goals) and related costs and risks. It includes how IT will support IT-enabled investment programmes and operational service delivery. The plan defines how the objectives will be met and measured and receives formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements.

2.3.3 The strategic plan should be sufficiently detailed to allow the definition of tactical IT plans. A portfolio of tactical IT plans that are derived from the IT strategic plan should be created. These tactical plans describe required IS initiatives, resource requirements, and how the use of resources and achievement of benefits will be monitored and managed. The tactical plans should be sufficiently detailed to allow for the definition of project plans. The set tactical IS plans and initiatives should be actively managed through analysis of project and service portfolios. This ordinarily encompasses balancing requirements and resources on a regular basis, comparing them to achievement of strategic and tactical goals and the expected benefits, and taking appropriate action on deviations.

2.4 IT Steering Committee

2.4.1 An IT steering committee (or equivalent) composed of executive, business and IT management should be established to:

- Determine prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and prioritieTrack status of projects and resolve resource conflicts
- Monitor service levels and service improvements

2.4.2 The IT steering committee in its strategy implementation oversight role should have amongst its members at least one board member (sitting as the chair) supported by heads of operational and support departments, the chief information officer (CIO) and chief technical officer (or equivalent) together with other key contributors including legal, audit, finance, etc. Its discussions will be at a greater level of detail than would be expected of the IT strategy committee, and it will be expected to provide a great deal of input to the strategy committee's higher-level deliberations, for example, including recommendations on:

- The annual level of IT spending
- Alignment of the enterprise's IT architecture with business goals
- Portfolio management, including approval of projects plans for significant IT-related business investments
- Monitoring project plans and verifying that internal and external changes are appropriately factored into the updated plans
- The acquisition and divestment of IT-related resources
- Monitoring conflicts for IT resources based upon clearly articulated business priorities
- Communicating strategic goals to project teams through its representation of the operating and support departments
- Formulating plans for, and overseeing the results from, the IT dashboard, IT balanced scorecard or other key metrics
- Communicating the value of IT to all stakeholders. This may be done through articles on the corporate intranet or staff publications and, more importantly, to stakeholders and external analysts through the corporate web site or stakeholder communications.

2.5 Organisational Placement of the IT Function and Supporting Functions

2.5.1 The IT function should be placed in the overall organisational structure with a business model contingent on the importance of IT within the enterprise. Specifically, its criticality to business strategy and the level of operational dependence on IT should be considered. The reporting line of the CIO should be commensurate with the importance and potential benefits of IT within the enterprise.

2.6 IT Organisational Structure

2.6.1 An internal and external IT organisational structure should be established that reflects business needs. In addition, a process should be put in place for periodically reviewing the IT organisational structure to adjust staffing requirements and sourcing strategies to meet expected business objectives and changing circumstances.

2.6.2 An IT organisation should be defined taking into consideration requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision. This organisation should be embedded into an IT process framework that verifies transparency and control as well as the involvement of senior executives and business management.

2.6.3 An IT strategy committee should verify board oversight of IT and one or more steering committees, in which business and IT participate, should determine prioritisation of IT resources in line with business needs. Processes, administrative policies and procedures need to be in place for all functions, with specific attention to control, quality assurance, risk management, information security, data and systems ownership, and segregation of duties. To verify timely support of business requirements, IT should be involved in relevant decision processes.

2.6.4 An IT process framework should be put in place to execute the IT strategic plan. This framework should include an IT process structure and relationships (e.g., to manage process gaps and overlaps), ownership, maturity, performance measurement, improvement, compliance, quality targets and plans to achieve them. It should provide integration amongst the processes that are specific to IT, enterprise portfolio management, business processes and business change processes. The IT process framework should be integrated in a quality management system and the internal control framework.

2.7 Roles and Responsibilities

2.7.1 Roles and responsibilities for all personnel in the organisation in relation to IS should be defined and communicated to allow sufficient authority to exercise the role and responsibility assigned to them. Role descriptions should be created and updated regularly. These descriptions should delineate both authority and responsibility, include definitions of skills and experience needed in the relevant positions, and are suitable for use in performance evaluation. Role descriptions should contain the responsibility for internal control.

2.8 Responsibility for IT Quality Assurance

2.8.1 Responsibility for the performance of the quality assurance function should be assigned, and the quality assurance group should be provided with appropriate quality assurance systems, controls and communications expertise. The organisational placement and the responsibilities and size of the quality assurance group should satisfy the requirements of the organisation.

2.9 Process Outsourcing

2.9.1 In most enterprises, the bulk of IT spending is devoted to operations and user support. Although in-house IT departments can provide these services, top executives are increasingly aware that service providers, both local and offshore, offer value and often a more disciplined approach to customer service.

2.9.2 With the increasing strategic importance of IT, the expectations of top executives in relation to IT have increased. Due to this situation, new and creative uses of outsourcing, which keep a balance with the internal organisation, have arisen. In many cases, the internal IT organisation is committed to delivering everyday services, such as user support, data centre operations and applications development, whilst contributing to strategy or leading innovation is left to external consultants (that can be seen as specialised and flexible). These tendencies may sometimes be supported by top executives due to increasing work supporting regulation. Because of the time it takes to change IT systems, the proportion of deficiencies in compliance attributed to the IT organisation will increase, exacerbating these tendencies, focusing internal resources even more to resolve these issues. Top executives recognise the need for advice about the strategic use of IT, and if they cannot get it from the IT organisation, they will go elsewhere. The use of third-party suppliers and consultants to give advice may risk a lack of objectivity, as they may recommend their own products and services for both strategic and routine activities. If the IT organisation cannot deliver strategic advice, it may lose the opportunity even to deliver routine services. Process outsourcing could also be the result of a management decision to focus on its core activities and because it is more cost-effective to outsource the IT process vs. using in-house expertise.

2.10 IT Infrastructure and Computer Operations

2.10.1 Complete and accurate processing of data requires effective management of data processing and maintenance of hardware. This process includes defining operations' policies and procedures for effective management of scheduled processing, protection of sensitive output, monitoring infrastructure and preventive maintenance of hardware. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.

2.10.2 Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel. A good preventive maintenance schedule also helps ensure the normal running of equipment.

2.10.3 Verifying the integrity of hardware and software configurations requires establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimises production issues and resolves issues faster.

2.10.4 Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the business can address root causes (such as poor user training) through effective reporting.

2.10.5 The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, offsite backup storage and periodic continuity plan training. An effective continuous service process minimises the probability and effect of a major IT service interruption on key business functions and processes.

2.10.6 The need to manage performance and capacity of IS resources requires a process to periodically review current performance and capacity of IS resources. This process includes forecasting future needs based on workload, storage and contingency requirements. This process provides assurance that information resources supporting business requirements are continually available.

2.10.7 Effective communication between IS management and business customers regarding services required is enabled by a documented definition and agreement of IS services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IS services and the related business requirements.

2.11 Operations Procedures and Tasks

2.11.1 Standard procedures for IT operations should be defined, implemented and maintained and the operations staff should be familiar with all tasks assigned to them. Operational procedures should cover shift handover (i.e., formal handover of activity, status updates, operational problems, escalation procedures, reports on current responsibilities) to verify continuous operations. Also, procedures to monitor the IT infrastructure and related events should be defined.

2.12 Application Development

2.12.1 Application systems could be acquired/developed through various modes, including:

- Custom development using internal resources
- Custom development using fully or partly outsourced resources located onsite or offsite (locally or at an offshore location)
- Vendor software packages implemented as-is with no customisation
- Vendor software packages customised to meet the specific requirements

At times, large complex applications (which may include enterprise resource planning systems) may involve a combination of the above.

2.13 Contract Adherence of the IT Function Utilising an Outsourcing Arrangement

2.13.1 A large number of IT services from IT help desk to IT operations can be outsourced to third-party providers. The need to

assure that services provided by third parties meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises business risk associated with non-performing suppliers.

2.14 Procedures Regarding Third Parties

2.14.1 All third-party supplier services should be identified and categorised according to supplier type, significance and criticality. Formal documentation of technical and organisational relationships covering the roles and responsibilities, goals, and expected deliverables should include credentials of representatives of these suppliers. The third-party relationship management process for each supplier should be formalised. The relationship owners must liaise on customer issues and verify the quality of the relationship based on trust and transparency, for example, through service level agreements (SLAs). When a new third-party supplier service is being entered into, the service provider's ability to enhance and adapt its services to reflect business changes should be considered.

2.14.2 A process should be established to monitor service delivery to verify that the supplier is meeting current business requirements and is continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.

2.15 Responsibility for Risk, Security and Compliance

2.15.1 Ownership and responsibility for IT-related risks should be embedded within the business at an appropriate senior level. Roles for managing critical IT risks including the specific responsibility for information security, physical security and compliance should be defined and assigned. Risk andsecurity management responsibilities should be established at the enterprise level to deal with

Organisation wide issues. Additional security management responsibilities may need to be assigned at a system-specific level to deal with related security issues. Direction or guidelines should be obtained from (via consultation with) senior management on the appetite for IT risk and approval of any residual IT risks.

2.16 Personnel Recruitment and Retention

2.16.1 Staffing requirements should be evaluated on a regular basis or upon major changes to the business, operational or IT environments to verify that the IT function has a sufficient number of competent IT staff. Staffing should take into consideration co-location of business/IT staff cross-functional training, job rotation and outsourcing opportunities.

2.16.2 Key IT personnel should be defined and identified, and overreliance on them should be minimised. A plan for contacting key personnel in case of emergency should be established. Also, policies and procedures should be defined and implemented for controlling the activities of consultants and other contract personnel by the IT function to assure the protection of the organisation's information assets and meet agreed contractual requirements. Key performance indicators should be included to help verify that staff is performing to expectations.

3. AUDIT PROCESS

3.1 Planning

3.1.1 An audit programme should be developed based on the organisation's risk assessment and risk management strategy, including the scope, objectives and timing of the audit. Reporting arrangements should be clearly documented in the audit programme. Consideration should be given to the nature and size of the organisation and its stakeholders. The IS auditor should gain an understanding of the organisation's mission and business objectives, the types of technical infrastructure, and business critical data.

3.1.2 Risk assessment methodologies should be used to define the scope of the review, focusing on high-risk areas.

3.1.3 Any previous audit reports should be reviewed, and the level of resolution should be assessed on each issue according to the management action plan.

3.1.4 The IS auditor should obtain information on the IT organisation including:

- The roles and responsibilities of key staff, including the information managers, owners and supervisors
- Senior management steering roles and responsibilities
- Organisational objectives and long- and short-range plans
- Setting the enterprise strategic directions
- IT objectives and long- and short-range plans
- Status reports and minutes of planning/steering committee meetings
- Information architecture model
- Policies and procedures relating to the IT organisation and relationships
- Position descriptions, training and development records
- Contracts with third-party service providers
- Determining whether the enterprise has developed the skills and IT infrastructure required to meet the strategic goals set for the enterprise

3.1.5 The IS auditor should identify and obtain a general understanding of the processes that enable the IT organisation to perform the functions listed in section 4.1.1, including the communication channels used to set goals and objectives to lower levels (top-down) and the information used to monitor its compliance (bottom-up).

3.1.6 The IS auditor should obtain information on the organisation's IS strategy (whether documented or not), including:

- Long- and short-range plans to fulfil the organisation's mission and goals
- Long- and short-range strategy and plans for IT and systems to support those plans
- An approach to setting IT strategy, developing plans and monitoring progress against those plans
- An approach to change control of IT strategy and plans
- An IT mission statement and agreed goals and objectives for IT activities
- Assessments of existing IT activities and systems

3.2 IS Audit Objectives

3.2.1 The objectives of an audit of the IT organisation may be affected by the intended audience's needs and the level of dissemination intended. The IS auditor should consider the following options in establishing the overall objectives of the audit:

- Reporting on the IT organisation and/or its effectiveness
- Whether IT initiatives support the organisation mission and goals
- Evaluation of alternate strategies for applications, technology and the organisation

3.2.2 The detailed objectives for an IS audit of the IT organisation ordinarily depends upon the framework of internal control exercised by top-level management. In the absence of any established framework, the COBIT framework should be used as a minimum basis for setting the detailed objectives.

3.3 Scope of the Audit

3.3.1 The IS auditor should include in the scope of the audit the relevant processes for planning and organising IT activity and the processes for monitoring that activity.

3.3.2 The scope of the audit should include control systems for the use and protection of the full range of IT resources defined in the COBIT framework. These include:

- Data
- Application systems
- Technology
- Facilities
- People
- IT governance

3.4 Staffing

3.4.1 The IS auditor should provide reasonable assurance that the staff used to perform this review includes persons of appropriate seniority and competence.

4. PERFORMANCE OF AUDIT WORK

4.1 Review of the IT Organisation and the Strategic Planning Process

4.1.1 In reviewing the IT organisation and relationships, the IS auditor should consider whether the IT organisation has the right mix of staff and skills, with roles and responsibilities defined and communicated and aligned with business. The IS auditor may include in the review whether:

- Policy statements and communications from senior management verify the independence and authority of the IT function
- Membership and functions of the IT planning/steering committee have been defined and responsibilities identified
- The IT planning/steering committee charter aligns the committee's goals with the organisation's objectives and long- and short-range plans and the IT objectives and long- and short-range plans
- The CIO reporting line is commensurate with the importance of the function in relation with the business of the enterprise and follows the trends of the enterprise industry and its market
- Policies address the need for evaluation and modification of organisational structure to meet changing objectives and circumstances
- Senior management verifies that roles and responsibilities are carried out
- Policies exist outlining roles and responsibilities for all personnel within the organisation with respect to information systems, internal control and security
- A quality assurance function and policies exists for the IT organisation
- Policies and procedures exist covering data and system ownership for all major data sources and systems
- Policies and procedures exist describing supervisory practices to verify that roles and responsibilities are appropriately exercised and all personnel have sufficient authority and resources to perform their roles and responsibilities

- Segregation of duties exist between systems development and maintenance, systems development and operations, systems development/maintenance and information security, operations and data control, operations and users, and operations and information security
- IT staffing and competence is maintained to verify its ability to provide effective technology solutions
- Appropriate roles and responsibilities exist for key processes, including system development life cycle activities, information security, acquisition and capacity planning
- Appropriate and effective key performance indicators and/or critical success factors are used in measuring results of the IT function in achieving organisational objectives
- IT policies and procedures exist to control the activities of consultants and other contract personnel, and thereby verify the protection of the organisation's assets
- Procedures are applicable to contracted IT services for adequacy and consistency with organisation acquisition policies
- Processes exist to coordinate, communicate and document interests both inside and outside the IT function
- Policies and procedures are in place to guarantee the delivery of services by the IT function is cost justified and in line with industry costs
- Organisational hiring and termination procedures including background checks

4.1.2 In reviewing the IT strategic planning process, the IS auditor should consider whether:

- There is a clear definition of IT mission and vision
- There is a strategic IT planning methodology in place
- The methodology correlates business goals and objectives to IS business goals and objectives
- This planning process is periodically updated (at least once per year)
- This plan identifies major IS initiatives and resources needed
- The level of the individuals involved in this process is appropriate

4.1.3 In reviewing the processes used to administer the current systems portfolio, the IS auditor should consider the coverage of organisational strategic and support areas by the current systems. The IS auditor may include in the review whether:

- The overall coverage of the policies issued providing the strategic areas defined by the business strategic planning process
- The process followed by top-level management to elaborate, communicate, enforce and monitor the policy compliance
- Documented policies exist on the following as appropriate: security, human resources, data ownership, end-user computing, intellectual property, data retention, system acquisition and implementation, outsourcing, independent assurance, continuity planning, insurance, and privacy
- The definition of roles and responsibilities of the people (e.g., data owners, IT management, executive management) involved in the processes under review are appropriate to support those processes
- The people involved in the processes under review have the skills, experience and resources needed to fulfil their roles
- The appropriate level of involvement of internal audit has been provided (if the organisation has internal audit resources)
- The position in the organisation of IT specialist staff or functions is appropriate to enable the organisation to make the best use of IT to achieve its business objectives
- The organisation and management of IT specialists, and non-specialists with IT responsibilities, are adequate to address the risks to the organisation of error, omissions, irregularities or illegal acts

5. REPORTING

5.1 Report Generation and Follow-up

5.1.1 The draft audit report should be generated and discussed with relevant personnel. Only those issues supported by clear audit evidence should be included. Recommendations developed for remediation should be discussed with appropriate personnel representing management.

5.1.2 The report should be finalised following ISACA guidelines and presented to management with recommendations to resolve/improve issues and follow-up options.

5.1.3 Follow-up activities, action plans, responsibilities, target dates, resources and priorities given by senior management should be agreed upon.

6. EFFECTIVE DATE

6.1 This guideline is effective for all IS audits beginning 1 May 2008.

G40 Review of Security Management Practices

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S1 Audit Charter states, 'The purpose, responsibility, authority and accountability of the information systems audit function or information systems audit assignments should be appropriately documented in an audit charter or engagement letter'.

1.1.2 Standard S3 Professional Ethics and Standards states, 'The IS auditor should adhere to the ISACA Code of Professional Ethics'.

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To review security management practices by IS auditor, the processes in COBIT most likely to be relevant, selected and adapted are classified below as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.2 The primary specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance are:

- PO2 *Define the information architecture*
- PO9 *Assess and manage IT risks*
- DS5 *Ensure systems security*
- DS7 *Educate and train users*
- ME2 *Monitor and evaluate internal control*
- ME3 *Ensure compliance with external requirements*
- ME4 *Provide IT governance*

1.2.3 The secondary specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance are:

- PO6 *Communicate management aims and direction*
- PO7 *Manage IT human resources*
- DS1 *Define and manage service levels*
- DS2 *Manage third-party services*
- DS9 *Manage the configuration*
- DS10 *Manage problems*
- DS12 *Manage the physical environment*
- AI1 *Identify automated solutions*
- AI2 *Acquire and maintain application software*
- AI3 *Acquire and maintain technology infrastructure*
- AI6 *Manage changes*
- ME1 *Monitor and evaluate IT performance*

1.2.4 The information criteria most relevant to responsibility, authority and accountability are:

- Primary: Effectiveness, efficiency and confidentiality
- Secondary: Availability, integrity and reliability

1.3 Purpose of the Guideline

1.3.1 Information is a most valuable asset in business. Information is increasingly vital for competitive success, and essential for economic survival. In the actual interconnected world, organisations should protect their information assets from unauthorised use, not only to protect its investments but also to protect information assets from the risks generated by the misuse of resources, intentionally or unintentionally. Such protection of information assets can be achieved only by implementing formal, detailed information security management framework in an enterprise. This guideline provides detailed guidance to assess and conclude on the design and operating effectiveness of the information security management practices implemented by management.

1.4 Guideline Application

1.4.1 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards and guidelines.

1.5 Definitions

1.5.1 Information is an asset that has value to any organisation that needs to be protected suitably. Information can be in any form, including paper, stored electronically in any electronic media, or transmitted by means suitable to the media.

1.5.2 Information security is a set of measures that are in place ensure that only authorised users (confidentiality) have access to accurate and complete information (integrity) when required (availability).

1.5.3 An information security management system (ISMS) is an overall management system, based on a business-risk approach to establish, implement, operate, monitor, review, maintain and improve information security. The organisational structure to implement security management practices includes policies, planning activities, responsibilities, procedures, processes and resources.

1.5.4 ISO 27001 *Information Security Management—Specification with Guidance for Use* is the replacement for BS7799-2. It is intended to provide the foundation for third-party audit and is harmonised with other management standards, such as ISO/IEC 9001:2000 and 14001:2004.

2. SECURITY MANAGEMENT PRACTICES IMPLEMENTATION

2.1 Planned Approach

2.1.1 Enterprise's that consider adoption of an ISMS should follow a processed approach for the implementation of the security management practices. Such implementation of security management practices should include all activities such as establishing, implementing and operating, monitoring and reviewing and maintaining and improving the ISMS. The organisation may choose to

adopt the Plan, Do, Check and Act (PDCA) model to implement the framework.

2.2 Establish Security Management Practices

2.2.1 The IS auditor should verify whether the enterprise has documented and implemented the information security policies and procedures relevant to manage the risks identified through a proper risk assessment process and improve information security performance, ensure compliance with organisation policies, and achieve its objectives.

2.3 Implement and Operate Security Management Practices

2.3.1 The IS auditor should verify whether the enterprise has identified appropriate controls, responsibilities and prioritisation of information security risks and has implemented all controls needed to address the risks and related objectives to protect information security. In addition, the IS auditor should verify whether the personnel have appropriate training and awareness programmes related to information security to implement and operate the security management practices. Also, the IS auditor should verify whether the enterprise has appropriate processes in place to operate the controls as intended including measures to detect and respond to security incidents.

2.4 Monitor and Review Security Management Practices

2.4.1 The IS auditor should verify whether the organisation has procedures to monitor the effectiveness and efficiency of the security management practices.

2.5 Maintain and Improve Security management Practices

2.5.1 The IS auditor should verify whether the enterprise has a process to ensure that management performs a review of the ISMS on a periodic basis to confirm its continuing applicability, adequacy, effectiveness and efficiency. Also, the IS auditor should verify whether the enterprise has a process to act upon the results and recommendations resulting from such periodic review and a continuous process to improve the effectiveness of ISMS.

3. REVIEW OF SECURITY MANAGEMENT PRACTICES

3.1 Security Management Practices

3.1.1 The IS auditor should verify whether the enterprise has a set of security management practices including policies, practices, procedures, security organisation, and security roles and responsibilities. The IS auditor should verify if the security management practices were established by the enterprise after identifying the security requirements through the risk assessment process and also with an understanding toward legal, statutory and regulatory requirements related to information protection and to meeting the information processing requirements needed for an enterprise.

3.2 Information Security Organisational Structure

3.2.1 The IS auditor should verify if the enterprise has set a clear security policy direction as a commitment to implementing security management practices by publishing and communicating a detailed information security policy that is approved by management.

3.2.2 The IS auditor should verify if the Information security policy includes, at minimum, the following:

- Definition of information security, objectives and scope
- Management's intent, in the form of a security policy statement, to implement security management practices
- A list of security policies, principles, standards and compliance requirements
- Information security management structure and related responsibilities
- Supporting documents in implementing security management practices such as more detailed policies and procedures

3.2.3 The IS auditor should verify whether the enterprise has documented and implemented ongoing training and awareness programmes to communicate the information security policy to the entire enterprise.

3.2.4 The IS auditor should verify whether the enterprise has documented and implemented a process to periodically evaluate the information security policy to ensure the effectiveness and applicability of the security policies.

3.2.5 The IS auditor should verify whether the enterprise has defined the responsibilities for implementation of security management practices, continuous evaluation, monitoring and improvement and to facilitate resourcing and implementing the security controls to achieve information security.

3.2.6 The IS auditor should verify whether the enterprise has a process for reviewing new information processing facilities prior to approving the implementation.

3.3 Third-party Access to Information and Outsourcing

3.3.1 The IS auditor should verify whether the enterprise has implemented appropriate access controls processes to prevent unauthorised access or misuse of information by third parties. Such controls should have been implemented prior to providing access to third parties.

3.3.2 The IS auditor should verify whether the enterprise has incorporated all control requirements, such as:

- Confidentiality and integrity
- Acceptable use
- Legal requirements, if any
- Arrangements for ensuring awareness of security responsibilities by all parties
- Controls to ensure integrity and confidentiality of the enterprise's business assets
- Physical and logical security requirements
- Outsourcing services availability
- Background screening of employees
- Auditing outsourced facilities, the right for which should be included within the contract with any third parties

3.4 Asset Classification and Control

3.4.1 IS auditor should verify whether the enterprise has identified owners and assigned accountability for all information assets, for protection of the assets. Such an asset ownership and accountability process should include an inventory of assets to help decide

several protection measures, including insurance and financial management, apart from defining protection mechanisms. Also, the IS auditor should verify if the assets in the enterprise include the following categories:

- Information assets (e.g., databases, data files, the business continuity plan, network diagram and security architecture)
- Software assets (e.g., application and system software, tools and utilities, and relevant licences)
- Physical assets (e.g., computer and communications equipment and electronic media)
- Services (e.g., general utilities, heating and lighting)

3.4.2 The IS auditor should verify whether the enterprise has classified all information assets based on their sensitivity and criticality to the business; value of information, including legal requirements to protect and retain; and the impact on the business upon losing the information or its integrity or non-availability.

3.4.3 The IS auditor should verify whether the enterprise has labelled all classified information assets and defined appropriate handling procedures including procedures to copy, store, transmit by various means and destroy. Such labelling can be by physical or electronic. Also, the IS auditor should verify whether appropriate monitoring procedures have been introduced to ensure that information classification, labelling and handling processes are appropriately implemented.

3.5 Personnel Security

3.5.1 The IS auditor should verify whether the enterprise has:

- Addressed the security responsibilities at the recruitment stage, including defining security job responsibilities within the job descriptions
- Introduced practices to perform security screening of all employees, especially for sensitive jobs
- Required confidentiality or non-disclosure agreements to be signed by employees or any third party
- Specified the responsibility for information security under the terms and conditions of employment

3.5.2 The IS auditor should verify whether the enterprise has an appropriate training programme on security policies and procedures to provide training to all employees and non-employees, as appropriate. The IS auditor should also verify, at least on a sample basis, with select users within the organisation, whether the users are aware of all security procedures and know how to adhere to these procedures to minimise the possibility of security risks.

3.5.3 The IS auditor should verify whether the enterprise has:

- Documented and implemented reporting and incident response procedures
- Communicated and trained the entire enterprise regarding the security reporting and incident response procedures
- Required users to report security weaknesses identified in information systems to take appropriate remediation action
- Documented and implemented procedures for reporting software malfunctions
- Introduced appropriate incident-reporting functionalities that would enable management to identify recurring incidents and enhance security control requirements accordingly
- Documented and implemented a formal disciplinary process for employees who have committed a security breach

3.5.4 The IS auditor should verify whether the enterprise has proper procedures in place to collect evidence. Such procedures should include follow-up actions against a person or enterprise after an information security incident involves legal action (either civil or criminal) in order to collect, retain and present (as needed) appropriate evidence, as laid down in the relevant jurisdiction(s).

3.5.5 The IS auditor should verify whether the enterprise has a formal process for termination of employment in case of actions to be taken due to security breach. Such formal processes should include:

- Circumstances in which termination of employment would occur and responsibility for deciding terminations
- Requirement that all employees, contractors and third parties return all of the enterprise's assets in their possession upon termination of their employment, contract or agreement
- Removal (or adjusted upon change) of access rights of all employees, contractors and third parties to information and information processing facilities upon termination of their employment, contract or agreement

3.6 Physical Security

3.6.1 The IS auditor should verify whether the enterprise has introduced appropriate security controls to secure the office buildings from physical security threats. Such controls include:

- Security perimeters to protect areas that contain information and information processing facilities
- Appropriate entry procedures to secure areas to allow authorised personnel only
- Physical security for offices, rooms and facilities
- Physical protection against damage from nature or man-made disasters
- Physical protection for working in secure areas
- Physical access controls to network closets (including telecom closets)
- Segregation of physical locations and access areas such as loading and unloading sections where potential for unauthorised access exists to information processing facilities

3.6.2 The IS auditor should verify whether the enterprise has adequately implemented physical security controls to prevent loss, damage or compromise of assets and interruption to business activities. Such controls include:

- Protection of all equipment, including telecom and network equipment, to reduce risks from environmental threats and hazards and opportunities for unauthorised access
- Proper maintenance of supporting utilities to ensure that disruptions are not caused to the equipment by their failures
- Protection of power and telecommunications cabling carrying data or supporting information services from interception or damage
- Proper maintenance of equipment to ensure its continued availability and integrity
- Proper protection measures for offsite equipment, taking into account the different risks of working outside the enterprise's premises
- Controls to ensure that any sensitive data and licensed software within any equipment or storage media has been removed or securely overwritten prior to disposal
- Prior to disposal of access devices, such as access cards or tokens, remove sensitive information
- Proper authorisation requirements for equipment, information or software prior to taking them offsite

3.7 Communications and Operations Management

3.7.1 The IS auditor should verify the following while reviewing the operational procedures of the enterprise:

- Operating procedures should be documented, maintained and made available to all users who need them.
- Changes to information processing facilities and systems should be controlled.
- Duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the enterprise's assets.
- Development, test and operational facilities should be separated to reduce the risk of unauthorised access or changes to the operational system.
- Security controls, service definitions and delivery levels included in the third-party service delivery agreement should be implemented, operated and maintained by the third party. The services, reports and records provided by the third party should be regularly monitored, reviewed and audited.

3.7.2 The IS auditor should verify whether the enterprise has documented and implemented:

- Procedures to monitor, tune and project the future capacity requirements for all information resources to ensure the required system performance
- Acceptance criteria for new information systems, upgrades and new versions, including performing suitable tests of the system(s) during development and prior to acceptance

3.7.3 The IS auditor should verify whether the enterprise has the following in place to protect against malicious software:

- Controls for detection, prevention and recovery to protect against malicious code and appropriate user-awareness procedures. Such protection measures could include installation of antivirus software and software that could detect and remove spyware and adware
- Controls to ensure authorisation of use of mobile code, appropriate configuration to ensure that the authorised mobile code operates according to a clearly defined security policy, and controls to prevent unauthorised mobile code from executing

3.7.4 The IS auditor should verify whether the enterprise has documented and implemented routine procedures to execute the agreed-upon backup strategy: test for recovery as needed for timely restoration, logging backup failures and remediation; monitor the equipment environment as needed. Such procedures should include backing up of information, operator logs and fault logging.

3.7.5 The IS auditor should verify whether the enterprise has established appropriate controls to manage and protect networks, in order to be protected from threats and to maintain security for the systems and applications using the network, including information in transit. The IS auditor should verify whether the network services agreement, whether the services are in-house or outsourced, should include security features, service levels and management requirements of all network services. Protection measures could include installation of firewalls and scanning of the networks, including penetration testing as needed.

3.7.6 The IS auditor should verify whether the enterprise has established the following formal procedures for:

- Disposal of media securely and safely when no longer required
- Handling and storage of information to protect this information from unauthorised disclosure or misuse
- Protection of system documentation against unauthorised access

3.7.7 The IS auditor should verify whether the enterprise has established the following:

- Formal exchange policies, procedures and controls to protect the exchange of information through the use of all types of communication facilities
- Agreements for the exchange of information and software between the organisation and external parties
- Protection of media containing information against unauthorised access, misuse or corruption during transportation beyond the enterprise's physical boundaries

3.7.8 The IS auditor should verify whether the enterprise has established the following:

- Policies and procedures to protect information associated with the interconnection of business information systems
- Appropriate protection measures for information involved in electronic messaging
- Appropriate protection measures to protect information involved in electronic commerce passing over public networks, from fraudulent activity, contract dispute, and unauthorised disclosure and modification
- Protection to ensure that online transactions are transmitted completely and that misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay does not occur
- Protection to ensure the integrity of information available on a public system

3.8 Access Controls to Information Assets

3.8.1 The IS auditor should verify whether the enterprise has a documented access-control policy based on business and security requirements for access.

3.8.2 The IS auditor should verify whether the enterprise has documented and implemented a formal user registration and de-registration procedure for granting and revoking access to all information systems and services. Such process should include: a) restricted and controlled allocation and use of privileges, b) review of users' access rights at regular intervals and c) timely revocation of access.

3.8.3 The IS auditor should verify whether the enterprise has documented and implemented controls to ensure that:

- Information users are required to follow good security practices in the selection and use of passwords
- Those with administrator/privileged access have stronger passwords and change their passwords more regularly (while stronger passwords are best practice for all users)
- Information users have ensured that unattended equipment has appropriate protection
- Information users have adopted a clear-desk policy for papers and removable storage media and a clear-screen policy for information-processing facilities

3.8.4 The IS auditor should verify whether the enterprise has documented and implemented the following related to network access control:

- Appropriate authentication and authorisation methods to control access by remote users
- Controlled physical and logical access to diagnostic and configuration ports
- Segregated groups of information services, users and information systems on networks. This should include appropriate restrictions for shared networks, especially those extending across the enterprise's boundaries, to ensure that the capability of users to connect to the network is in line with the access-control policy and requirements of the business applications.
- Routing controls to ensure that computer connections and information flows do not breach the access control policy of the

business applications

3.8.5 The IS auditor should verify whether the enterprise has documented and implemented the following to protect access to the operating system:

- Secure logon procedure for access to operating systems
- Unique identifier (user ID) for all users within the enterprise for individual use only, and a suitable authentication technique to substantiate the claimed identity of a user
- Interactive system for managing passwords and to ensure quality passwords
- Controls to restrict access to utility programmes that might be capable of overriding system and application controls
- Controls to shut down inactive sessions after a defined period of inactivity
- Restrictions on connection times to provide additional security for high-risk applications

3.8.6 The IS auditor should verify whether the enterprise has documented and implemented the following to protect access to the applications:

- Access to information and application system functions by users and support personnel provided in accordance with the defined access-control policy
- Dedicated (isolated) computing environment for protecting sensitive applications

3.8.7 The IS auditor should verify whether the enterprise has documented and implemented the following to monitor system access and use:

- A formal policy and appropriate security measures to protect against the risks of using mobile computing and communication facilities
- Audit logs to record user activities, exceptions, and information security events and procedures to maintain the logs for an agreed-upon period to assist in future investigations and access control monitoring
- Procedures to monitor use of information processing facilities and to review the results of the monitoring activities
- Controls to protect logging facilities and log information against tampering and unauthorised access
- Procedures to log system administrator and system operator activities and monitor the activities of the IT administrators on a regular basis
- Procedures to log, analyse and act upon faults
- Synchronisation of clocks of all relevant information processing systems within the enterprise or security domain to an agreed-upon accurate time source

3.8.8 The IS auditor should verify whether the enterprise has completed the following:

- A formal assessment of threats and vulnerabilities, from internal or external attacks, and their impact on the enterprise's network, information systems and applications
- Implementation of an intrusion detection mechanism for timely identification of any intrusions within the enterprise's network
- Adequate procedures to apply security patches and other patches required for the system without compromising the current security level of the information systems
- Preventive, detective and corrective plans for any security incidents

3.9 Systems Development and Maintenance Documentation and Implementation

3.9.1 The IS auditor should verify whether statements of business requirements for new information systems, or enhancements to existing information systems, specify the requirements for security controls, including:

- Access controls to application systems
- Validation requirements for data inputs to applications to ensure that these data are correct and appropriate
- Validation checks within applications to detect any corruption of information through processing errors or deliberate acts
- Requirements for ensuring authenticity and protecting message integrity in applications
- Validation of data output from an application validated to ensure that the processing of stored information is correct and appropriate to the circumstances

3.9.2 The IS auditor should verify whether the enterprise has documented and implemented a policy on the use of cryptographic controls for the protection of information. Such controls should include key management to support the enterprise's use of cryptographic techniques.

3.9.3 The IS auditor should verify whether the enterprise has established procedures to control the installation of software on operational systems and access to program source code.

3.9.4 The IS auditor should verify whether the enterprise has established formal change control procedures. Such procedures should include:

- Review and test of business critical applications when operating systems are changed to ensure that there is no adverse impact on organisational operations or security.
- Limit and control modifications to software packages to necessary changes.
- Monitor outsourced software development.
- Input processes to obtain timely information about technical vulnerabilities of the information systems being used, including a process to evaluate the exposure to such vulnerabilities, and introduce appropriate measures to address risk**.**

3.9.5 The IS auditor should perform a post-implementation review of the system, after it has been developed and implemented, to assess if the system meets the business and control requirements. The IS auditor in some cases, can also perform a pre-implementation review of the system, prior to the system implementation, to identify weaknesses or control improvements for timely remediation.

3.10 Business Continuity Management

3.10.1 The IS auditor should verify whether the enterprise has established the following:

- A managed process for business continuity throughout the organisation to address the information security requirements needed for the enterprise's business continuity
- A process to identify events that can cause interruptions to business processes, along with the probability and impact of such interruptions and their consequences for information security. This should include disaster incident response management and related procedures.
- Plans to maintain or restore operations and ensure availability of information, at the required level and in the required time

scales, following interruption to, or failure of, critical business processes
- A single framework of business continuity plans to ensure that all plans are consistent, consistently address information security requirements, and identify priorities for testing and maintenance
- A test and regular update of all business continuity plans to ensure that they are up to date and effective. Where appropriate, the IS auditor can observe management's testing process of the business continuity plan.
- Plans to provide training/awareness specifically on responsibilities for those identified to be involved in the business continuity process within the enterprise

3.11 Compliance

3.11.1 The IS auditor should verify whether the enterprise has:
- Defined, documented, and kept up to date all relevant statutory, regulatory and contractual requirements and the enterprise's approach to meet these requirements for each information system and the enterprise as a whole.
- Implemented appropriate procedures to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products
- Protected important records from loss, destruction and falsification in accordance with statutory, regulatory, contractual and business requirements
- Implemented data protection and privacy controls as required in relevant legislation, regulations, and, if applicable, contractual clauses
- Implemented controls to deter users from using information processing facilities for unauthorised purposes
- Implemented controls to require that all software installed in the enterprise be either licensed or open source
- Implemented cryptographic controls in compliance with all relevant agreements, laws and regulations

3.11.2 The IS auditor should verify whether the enterprise has established a process to confirm that the:
- Managers have ensured that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards
- Information systems are regularly checked for compliance with security implementation standards

3.11.3 The IS auditor should verify whether the enterprise has established a process to ensure that the
- Audit requirements and activities involving checks on operational systems are planned and agreed-upon to minimise the risk of disruptions to business processes
- Access to information systems audit tools is protected to prevent any possible misuse or compromise

4 AUDIT PROCESS

4.1 Planning

4.1.1 The IS auditor should prepare an audit program for reviewing the security management practices of the enterprise based on the enterprise's risk assessment and risk management strategy, including the scope, objectives and timing of the audit. Reporting arrangements should be clearly documented in the audit programme. Consideration should be given to the nature and size of the enterprise and its stakeholders. The IS auditor should gain an understanding of the enterprise's mission and business objectives, enterprise information assets, technology infrastructure, and security management practices.

4.1.2 An understanding of the organisational structure is needed, specifically of the roles and responsibilities of key staff responsible for creating, communicating and monitoring security management practices and their compliance within the company. Other key staff members include information managers, owners and supervisors.

4.1.3 A primary objective of the audit planning phase is to understand the security-related threats and risks that the enterprise faces to arrive at audit objectives and to define the scope of the review with an emphasis on high-risk areas.

4.1.4 Appropriate sampling techniques should be considered in the planning of the audit to quantify the results of testing, if applicable.

4.1.5 A previous audit report should be required and the level of resolution should be assessed on each issue according to the management action plan.

5. PERFORMANCE OF WORK

5.1 Audit Tasks

5.1.1 The IS auditor should perform a detailed and independent review of the security management practices and their implementation, to provide assurance that the enterprise security management objectives are appropriately achieved.

5.1.2 The IS auditor should review all aspects of the security management practices as outlined in this guideline to provide such assurance

6. REPORTING

6.1 Report Generation and Follow-up

6.1.1 The draft audit report should be generated and discussed with relevant personnel. Only include those issues supported by clear evidence

6.1.2 The report should be finalised following ISACA guidelines and presented to management or the governance board, if available and appropriate, with recommendations to resolve/improve issues and follow-up options. Specifically, for sensitive security deficiencies, distribution of the report should be restricted to the governance board or appropriate level of management

6.1.3 Follow-up activities, action plans, responsibilities, target dates, resources and priorities given by senior management and/or the governance board should be agreed upon.

7. EFFECTIVE DATE

7.1 This guideline is effective for all IS audits beginning on or after 1 December 2008.

G41 Return on Security Investment (ROSI)

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S10 IT Governance states the IT audit and assurance professional should review:

- And assess whether the IT function aligns with the enterprise's mission, vision, values, objectives and strategies
- Whether the IT function has a clear statement about the performance expected by the business (effectiveness and efficiency) and assess its achievement
- And assess the effectiveness of IT resources and performance management processes

1.2 Linkage to COBIT

1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the return on security investment (ROSI) requirements of IT audit and assurance professionals, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.2.1 Primary IT processes are:

- PO1 *Define a strategic IT plan*
- PO3 *Determine technology direction*
- PO5 *Manage the IT investment*
- PO9 *Assess and manage IT risk*
- DS3 *Manage performance and capacity*
- DS6 *Identify and allocate costs*
- ME1 *Monitor and evaluate IT performance*
- ME4 *Provide IT governance*

1.2.3 Secondary IT processes are:

- PO6 *Communicate management aims and direction*
- AI1 *Identify automated solutions*
- AI5 *Procure IT resources*
- ME3 *Ensure regulatory compliance*

1.2.4 The information criteria most relevant to ROSI are:

- Primary—Effectiveness, efficiency and availability
- Secondary—Confidentiality, integrity and reliability

1.3 Purpose of the Guideline

1.3.1 Enterprises are increasingly finding it challenging to make a case to invest in IT security. Clearly defining ROSI is critical for enterprises to attain business objectives. To obtain a reasonably accurate estimation of ROSI, the enterprise needs to determine its security requirements and the most appropriate measure of ROSI, and establish metrics to collect information to measure ROSI. Business operations today recognise the significance of security measures as well as the risks and consequences involved in ignoring the impact of security to business operations. Decision makers are required to quantify, review and modify security metrics periodically to ensure effectiveness of the security measure. Additionally, internal, external and regulatory compliance require maintaining continuous improvement of security goals.

1.3.2 Enterprises cannot afford to ignore the value propositions of security metrics to effectively achieve appropriate ROSI. It is important to define strategic security measures in quantifiable user needs, develop a road map that incorporates a consensus-driven approach to define effective measures and provide periodic assessments to establish continuous improvement of ROSI.

1.3.3 IT audit and assurance professionals must have a clear understanding of the value proposition for ROSI. It is in this context that there is a need for a guideline to provide guidance to IT audit and assurance professionals to review return on security investments while carrying out audit assignments.

1.4 Guideline Application

1.4.1 This guideline provides guidance in applying Standard S10 IT Governance.

1.4.2 The IT audit and assurance professional should consider this guideline in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

1.4.3 When applying this guideline, the IT audit and assurance professional should consider its guidance in relation to other relevant ISACA standards and guidelines.

1.5 Risk Management

1.5.1 There should be collaborative periodic risk assessment developed amongst those responsible for securing information assets and the responsible senior management, with the business owner(s) managing the information assets of the enterprise. Specifically, the enterprisewide and business process owner risk assessments, denoting layers of controls, should be considered in the evaluation by the IT audit and assurance professional in gaining an understanding of the control environment. For example, the risk assessment performed by the business process owner, which includes an evaluation of the adequacy of the preventive control of periodically revalidating access to critical information assets, should be considered.

1.5.2 There is an inherent risk that the subject matter may be highly complicated coupled with security engineers/administrators who may not adequately understand all of the risks to the enterprise and the necessary mitigating control processes. For example, security over information assets may require technical controls at various entry and exit points within the network transmission in addition to the server controls. Thus, a security specialist for network security may be required, in addition to a security administrator with primary knowledge over server access controls, to fully understand all of the security risks. Thus, inherent within this risk assessment is the subject matter risk that all risks have been adequately identified, quantified and mitigated to the extent possible by the enterprise. Accordingly, an independent assessment may be required from various specialists knowledgeable on end-to-end security controls within the entire IT area to potentially identify all of the risks and necessary mitigating controls.

1.5.3 There is inherent audit risk resulting from the auditor responsible for performing an independent assessment not adequately understanding and/or reviewing the necessary control processes commensurate with the level of risk. In addition, there is a likelihood that the auditor will not properly conclude on the adequacy and efficiency of controls by leveraging sampling and other limited methodologies based upon economy of scale factors that will not always result in complete coverage of the risk area. Thus, management should be alerted that audit will not guarantee that the auditor will completely identify, test and conclude on the adequacy of all controls. Accordingly, additional oversight and independent assessment of the auditor's evaluation may be warranted given the size, complexity and significance of the enterprise's information assets.

2. ROSI

2.1 Introduction

2.1.1 ROSI for an enterprise is an important measure in today's cyberworld, in which hackers, computer viruses and cyberterrorists are making headlines. Security has become a priority for business enterprises that leads to answering many questions such as:

- How does a business become secure?
- How much security is enough?
- How does a business know when its security level is reasonable?
- How should security investment be accounted for?
- What is the right monetary and time investment to put in security?
- Which system components or other aspects should be targeted first?

Specifically, the primary basis of ROSI is the comparison of costs (e.g., creating firewalls, cost of the breach, cost of backing storage and various system elements that are redundant) and the preventive and corrective benefits that reduce the likelihood of cybersecurity breaches and resulting losses.

Measurement of risk is predicated, as with all IT-related impacts, in system availability, data integrity and information confidentiality.

Executive decision makers want to understand the impact of security on the bottom line. To arrive at how much to spend on security they need to know:

- How much is the lack of security costing the business?
- What impact is the lack of security having on productivity?
- What impact would a catastrophic security breach have?
- What are the cost-effective solutions?
- What impact will solutions have on productivity?
- Is the exposure being reduced?

2.1.4 ROSI is a key performance indicator that helps measure efficiency and effectiveness of spending on IT security. The metric is a top-down measure correlating IT security expense and its productivity into a concise, comparative metric for current performance assessment and planning.

2.1.5 By identifying ROSI, a business has a meaningful planning tool that allows it to determine both the appropriate level of IT security expense and the appropriate level of security required to protect the business.

2.1.6 By properly planning, managers should distinguish between operating costs benefiting the enterprise for a single time period or a capital investment extending beyond this single time period horizon in cybersecurity activities.

2.2 Determining ROSI

2.2.1 Identification and allocation of costs are essential to deploying the ROSI principle. Direct costs can be specifically linked to the particular cybersecurity breach, whereas indirect costs (e.g., an intrusion detection system that provides abundant controls for numerous types of breaches) cannot be linked with any certainty to a specific breach.

2.2.2 Another delineation is between explicit and implicit cost. Explicit cost can be measured, for example, in developing and maintaining firewalls, whereas implicit cost may be termed 'lost opportunities', such as loss in reputation, an ambiguous estimate. Regardless of ease of estimation, explicit and implicit costs should be included in the cost-benefit analysis in some quantifiable way.

2.2.3 To determine return on investment (ROI), a widely used equation is:

$$\text{ROI} = \frac{\text{Expected returns - Cost of investment}}{\text{Cost of investment}}$$

2.2.4 There are several quantifiable methods to employ for ROSI. For example, there is net present value (NPV), which compares anticipated benefits and costs over different time periods. In addition, there is a variant of the NPV called internal rate of return (IRR) , which sets the discount rate to make the NPV of the investment equal to zero. Both these methods provide a decision rule for accepting or rejecting incremental cybersecurity activities.

2.2.5 Calculation of ROSI in tabular form, without consideration of the time value of money, predicated upon the cost of prevention, is shown in **figure 1**.

2.2.6 Risk exposure is calculated by multiplying the projected cost of a single loss exposure (SLE) with its expected annual rate of occurrence (ARO). Risk exposure = SLE * ARO

The methods of estimating SLE and ARO are based upon metrics internally generated from past experience or drawn from external resources. Actuarial tables are created from insurance claim data, academic research and independent surveys.

2.2.7 Research from Idaho University (USA) defines ROSI based upon cost of recovery after the event as:

ROSI = R - annual loss expectancy (ALE), where ALE = (R - E) + T, i.e., ROSI = E - T

'R' is the annual cost to recover from any number of intrusions, 'E' is the monetary savings resulting from use of the security tool, and 'T' is the cost of the intrusion detection tool.

Figure 1—ROSI Calculation (without consideration of the time value of money, predicated upon the cost of prevention)					
#	**Numbers should be in the 000s**	**Options**			
		A	**B**	**C**	**D**
i	Financial investment level	0	650.00	1,300.00	1,950.00
ii	Total potential loss from cybersecurity breach without investment	10,000.00	10,000.00	10,000.00	10,000.00
iii	Probability of loss at each financial investment level denoted in i	.75	.50	.40	.33
iv	Expected loss at each investment level (iv) = (ii) X (iii)	7,500.00	5,000.00	4,000.00	3,300.00
v	Total expected cypersecurity costs equals investment costs plus expected loss from breaches (v) = (i) + (iv)	7,500.00	5,650.00	5,300.00	5,250.00
vi	Incremental benefits from increase in investment level, reduction in expected loss, i.e., reduction in (iv) values with additional investment	N/A	2,500.00	1,000.00	700.00
vii	Incremental level of investment increase in investment levels, i.e., increase in row i values	N/A	650.00	650.00	650.00
viii	Incremental net benefit of increase in investment level (viii) = (vi) – (vii)	N/A	1,850.00	350.00	50.00

A simplified equation for f**igure 1** is:

$$\text{ROSI} = \frac{\text{(Risk exposure * \% risk mitigated) - Cost of security investment}}{\text{Cost of security investment}}$$

2.2.8 In this approach ROSI must be greater than or equal to the difference between R and ALE. See appendix for example.

2.2.9 Two important components are insurance that analyses risks mitigated by proposed security investments and a component that assesses the productivity contribution of the investments. Insurance does not reduce the likelihood of a breach, but rather reduces the severity of losses if a breach occurs. The insurance component requires the comprehensive analysis of vulnerabilities, threats, and value of existing information assets and safeguards that are currently in place to quantify ALE. Security investments ideally aim to achieve either elimination of risk (improve security infrastructure), transfer of risk (purchase insurance), acceptance of risk (absorb potential losses) or a combination of the three.

Figure 2—ROSI Calculation Using NPV					
#	**Numbers should be in the 000s Rounded -**	**Options**			
		A	**B**	**C**	**D**
i	Financial investment levels at time t = 0	0	650.00	1,300.00	1,950.00
ii	Total potential loss from cybersecurity breach without investment at time, t = 1	10,000.00	10,000.00	10,000.00	10,000.00
iii	Probability of loss at each financial investment level denoted in i	.75	.50	.40	.33
iv	Expected loss at each investment level (iv) = (ii) X (iii)	7,500.00	5,000.00	4,000.00	3,300.00
v	Present value of expected loss at time, t =1 at each investment level (v) = (iv)/(1 + k) Note: k = interest rate	6,522.00	4,348.00	3,478.00	2,870.00
vi	Present value of total expected cybersecurity costs = investment costs + present value of expected loss from breaches (vi) = (i) + (v)	6,522.00	4,998.00	4,7778.00	4,820.00
vii	Present value (PV) of incremental benefits (B) of increase in investment level ($B_1/(1 + k)$ = reduction in PV of expected losses (i.e., reduction in column D values)	N/A	2,174.00	870.00	609.00
viii	Incremental level of investment (C_0), increase in investment levels, i.e., increase in ii values	N/A	650.00	650.00	650.00
ix	Incremental net benefits of increase in financial investment level resulting in NPV = $B_1/(1 + k) – C_o$ (ix) = (vii) – (viii)	N/A	1,524.00	220.00	41.00

2.2.10 Given the time value, money must be included in all cost-benefit analyses extending over several time periods. **Figure 2** shows the NPV method.

2.2.11 The incremental benefit of an investment is the present value of the reduction in expected losses. The present value of the expected loss for each investment level is given in **figure 2** in 'v' and reduction in the present value of the expected loss is given in 'vii'. In addition, the values derived in 'ix' represent the NPV for the additional financial investment level (e.g., see columns A through D). Accordingly, to find the optimal investment level, keep increasing the investment as long as the NPV of the incremental investment is positive.

2.2.12 Calculation of ROSI in tabular form, without consideration of the time value of money, is predicated upon the cost of prevention. It is evident from the approach that determining ROSI requires enterprises to have repeatable and consistent security metrics from which to identify and extract meaningful values.

2.3 Security Metrics

2.3.1 Security metrics are measures designed to facilitate decision making and improve performance and accountability through collection, analysis and reporting of relevant performance-related data. Security metrics focus on the actions (and results of those actions) that enterprises take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when security defences are breached. Primary considerations for development and implementation of a security metrics programme include the following:

- Metrics must yield quantifiable information such as percentages, averages and numbers.
- Data supporting metrics must be readily available.
- Only a repeatable process must be considered for measurement.
- Metrics must be useful for tracking performance and directing resources.
- Metrics should not be expensive or laborious to gather.

2.3.2 Security metrics may be of varied types such as:

- Implementation metrics—Measure the implementation of the security policy.
- Effectiveness/efficiency metrics—Measure results of security solutions.
- Impact metrics—Measure impact on business due to security events.

The types of metrics that can realistically be obtained and are useful depend upon the enterprise's security programme and control implementation. Over a period of time, the focus of gathering metrics shifts with maturing controls.

2.3.3 Data collection is a very important aspect of security metrics. Steps to be considered for data collection include:

- Metrics roles and responsibility, including responsibility for data collection, analysing and reporting
- Audience for the data collection
- Process for collection, analysing and reporting
- Co-ordination with all functions in the enterprise
- Creation or selection of data collection and tracking tools, and modification if required
- Collection of data, consolidation, storing, sorting in a format conducive to data analysis and reporting
- Metrics summary reporting formats
- Gap analysis, identification of cause and corrective action

2.3.4 Some common security metrics are:

- Baseline defence coverage (antivirus, antispyware, firewall, etc.)—Measures how well the enterprise is protected against basic information security threats
- Patch latency—The time between patch release and successful deployment in the enterprise. This is an indicator of the company's patching discipline and ability to react to incidents.
- Password strength—Reduces bad passwords. identifies potential weak spots and encourages the use of strong passwords that are hard to break
- Platform compliance scores—Benchmarks hardware against acceptable standards
- Legitimate e-mail traffic analysis—Analysis of incoming/outgoing traffic volume, traffic size and traffic flow pattern within the enterprise as well as external to the enterprise.
- Application risk index—Aids in categorising potential risk as high, medium or low

2.4 Optimum Investment in Information Security: Gordon-Loeb Model

2.4.1 Lawrence A. Gordon and Martin P. Loeb, University of Maryland (USA), presented an economic framework that characterises the optimal monetary investment to protect a given set of information assets. The model determines the optimal amount for an enterprise investment towards protecting a set of information in a single period model. It is shown that for a given potential loss, the optimum amount to spend to protect an information asset does not always increase with and increase in an information set's vulnerability. In addition, the model shows that the amount a firm should spend to protect information assets should generally be only a small fraction of the expected loss.

2.4.2 An information set is characterised by the following three parameters:

- λ—The monetary loss conditioned on a breach occurring
- t—The probability of a threat occurring
- v—The vulnerability, defined as the probability that a threat once realised (i.e., an attack) would be successful

Although the three parameters can change over time in the real world, the Gordon-Loeb model assumes them as pre-estimated constants.

The Gordon-Loeb model assumes the function S (z, v) denotes the probability that an information set with vulnerability 'v' will be breached—conditional on the realisation of a threat and given that the enterprise has made an information security investment of 'z' to protect that information set. The function S (z, v) is referred to as the security breach probability function. As is common with nearly all economic models, function S (z, v) is assumed to be sufficiently smooth and well behaved continuously, in particular the twice differentiable.

In addition to a general theory, Gordon-Loeb studied several classes of security breach probability functions. One of them is: S (z, v) = v^{AZ+1}

Where the parameter 'α' (>0) is a measure of productivity of information security, a closed-form solution to an optimisation problem is derived that maximises the expected net benefits from an investment in information security (ENBIS) defined as: ENBIS = {v-S (z, v)} tλ-z.

The optimum investment is given by: $z = z^*(v) = \frac{\ln \{-1/(avt\lambda \ln v)\}}{a \ln v}$

2.4.3 The model has two substantial restrictions—the loss 'ג' is considered a constant and investment 'z' is continuous, while the reality is the loss is not a constant and investments are discrete.

3. OBJECTIVES

3.1 Audit

3.1.1 The audit approach to ROSI should be directed towards:

- Ensuring availability of fully defined security requirements for the entire enterprise and/or programmes or projects identified for security coverage within the enterprise
- Establishing business goals that must be achieved by individual business units or the enterprise as a whole, focusing on critical impacts of security as a cost
- Awareness of management and business users towards system vulnerability, availability and reliability
- Analysis technology and operational efficiencies in terms of cost benefits and effectiveness in meeting security goals

3.1.2 Understanding employee/user perception of security is an important consideration for security investment and one of the means of achieving this is through an employee survey. The employee survey must be properly construed and should have a direct correlation between the survey score and financial performance. The survey should ask questions that have coarse quantitative answers or answers that imply a quantitative value. For example, how may spam messages do you receive every day (0-10, 10-30, 30-50, more than 50) or how often is the files server unavailable for more than 10 minutes (daily, weekly, monthly, rarely)? It is important to quantify risk and exposure in a repeatable and consistent manner. This is possible through an effective survey and scoring system for productivity and security, combined with external measurements of value propositions. IS auditors should review the internal survey where one is available.

3.1.3 Downtime assessment can provide an important postmortem analysis of lost productivity during a security incident. Productivity loss must also be considered in calculating the ROI of security solutions. **Figure 3** shows the average downtime and factors that affect productivity.

Figure 3—Factors That Affect Productivity and Average Downtime

Problem	Average Downtime (in Minutes)
Application and system crashes	10
E-mail filtering, sorting and spam	15
Bandwidth efficiency and throughput	10
Inefficient and ineffective security policies	10
Enforcement of security policies	10
System-related roll outs and upgrades for IT	10
Security patches for operating systems and applications	10
Insecure and inefficient network topology	15
Viruses, virus scanning	10
Worms	10
Trojan, key logging	10
Spyware, system trackers	10
Popup ads	10
Compatibility issues—hardware and software	15
Permissions-based security problems (user/pass)	15
File system disorganisation	10
Corrupt or inaccessible data	15
Hacked or stolen information and data	15
Backup/restoration	15
Application usage issues	15

Source: Sonnenreich, Wes; 'Return on Security Investment (ROSI): A Practical Quantitative Model', *Journal of Research and Practice in Information Technology,* vol., 38, no. 1, February 2006, a publication of the Australian Computer Society, Australia, 2006

3.1.4 IT audit and assurance professionals should be aware that there are number of ways in which lost productivity can provide a meaningful estimate of risk exposure, any of which could be used to calculate ROSI.

3.1.5 It is important for the enterprise to quantify risks mitigated to justify ROSI. Under normal circumstances, security solutions do not directly create any tangible value, rather they prevent loss. A loss prevented may be a loss that is unknown to the enterprise. For example, an enterprise's intrusion detection system (IDS) might show 20 successful break-ins last year to only 10 this year. Is it due to the new security solution implemented or were there less hackers attacking the network?

Figure 4—Productivity Loss Due to Security Solutions

Problem	Average Downtime (in Minutes)
Application and system crashes	10
Bandwidth efficiency and throughput	10
Over-restrictive security policies	10
Enforcement of security policies	10
System-related roll outs and upgrades from IT	10
Security patches for operating systems and applications	10
Trouble downloading files due to virus scanning	10
Compatibility issues—hardware and software	15
Security problems due to too many passwords/permissions	15

Source: Sonnenreich, Wes; 'Return on Security Investment (ROSI): A Practical Quantitative Model', *Journal of Research and Practice in Information Technology,* vol., 38, no. 1, February 2006, a publication of the Australian Computer Society, Australia, 2006

3.1.6 It is also important that enterprises capture the damage resulting from failures of security solutions to arrive at a correct ROSI. Security solutions do not work in isolation; the existence and effectiveness of other solutions have a major impact on the performance of the security solution. The most effective security solutions used are rarely implemented due to an unacceptable impact on productivity. **Figure 4** shows productivity loss resulting from implementing security solutions.

3.1.7 IT audit and assurance professionals should consider the fact that the cost of the security solution must include the impact of the solution on productivity, since more often than not this number is large enough to make or break the viability of the proposed solution.Security solutions become less effective over time as hackers find ways to work around them and create new risks. Therefore, it is important that the enterprise has a system for regular assessment of the security solution performance. IT audit and assurance professionals should review such assessment reports and action undertaken thereon.

3.1.8 Apart from the initial design and deployment of the security solution, it is equally essential that enterprises have a good process for managing the implemented solution and realise that security is a dynamic exercise. For example, the IDS needs to be updated at frequent intervals with new 'signatures', security policies must be regularly reviewed and evaluated, software patches must be regularly updated and installed, and firewalls must be adjusted to reflect growth and changes in the IT infrastructure. IT audit and assurance professionals should review the sustenance plan of the implemented security solution.

3.1.9 IT audit and assurance professionals should also recognise the challenges enterprises face in effectively implementing security solutions, such as:

- Availability of skilled manpower
- Retaining trained manpower
- Monitoring security performance 24x7
- Updating for the latest attacks, vulnerabilities, patches, technology advancements, upgrades and security solutions

4. CONSIDERATIONS

4.1 Audit

4.1.1 There are various ROSI models and there is no one model that fits all enterprises. Applicability of a model varies from enterprise to enterprise and depends upon various considerations, such as:

- Degree of exposure
- Nature of vulnerabilities
- Type of hazard
- Absence/weakness of compensating controls
- Geographical location—threat of external factors, such as war, vagaries of nature and such other uncontrollable events

4.1.2 Enterprises must have a well-defined process of data collection for security breaches and lapses. Data capture must not be restricted to events happening within the enterprise and should be extended beyond its regime giving due considerations to:

- Nature/type of business
- Business model (business to business, business to consumer, etc.)
- Critical business functions governed by IT
- Competitors and similar industry's strategy toward IT security

Such data are processed and appropriately analysed, and the result is reviewed by top management.

4.1.3 Security investments are made after proper analyses of security requirements, risk assessments, product performance, vendor service level agreement and, most importantly, alignment of the security plan to the overall business objectives.

4.1.4 No security is complete without adequate insurance. The enterprise should be adequately protected by appropriate insurance

4.1.5 Security must be considered as a business protector and enabler not as an inhibitor. Justifying the cost of security is a matter of ensuring that the technology will enable that business, security policies and procedures align directly with business goals, and that managing and maintaining security technology results in the maximum value of the investment in security.

4.1.6 Trust is the highest form of security. The enterprise should be evolving into a 'trusted enterprise' by partnering with key stakeholders to protect the enterprise's assets and proactively provide early warnings whenever breaches are anticipated.

4.1.7 Security policies and procedures should comply with applicable statutory and regulatory requirements.

5. EFFECTIVE DATE

5.1 This guideline is effective for all information systems audits beginning on or after 1 May 2010.

APPENDIX

Examples

A1. Example using ROSI = $\frac{\text{(Risk exposure * \% Risk mitigated) - Cost of security investment}}{\text{Cost of security investment}}$

Company A has had virus attacks previously. It estimates that its average cost of damage and loss of productivity due to virus attacks is US $25,000. Currently, Company A gets four attacks per year and expects to stop three of the four attacks by implementing a virus scanner solution costing US $25,000. ROSI is calculated in the following example:

Risk exposure: US $25,000 per exposure x 4 exposures in a year = US $100,000
Risk mitigated by the solution: 3 attacks out of 4 attacks, i.e., 75%
Cost of security investment = US $25,000

$$\text{ROSI} = \frac{\text{(US \$100,000 * 75\%) – US \$ 25,000}}{\text{US \$25,000}} = 200\%$$

In the example, it appears it is worth the investment on security. However, there are various assumptions and, therefore, the reality may be different. For example, what if, of the three attacks mitigated, each cost US $5,000 whereas the fourth attack cost US $85,000. The average would be US $25,000; however, the fourth attack would be a costly attack.

G41 Return on Security Investment (ROSI) cont.

A2. Example using ROSI = R - ALE, where ALE = (R - E) + T, i.e., ROSI = E - T.

Company A installs secure web servers to protect its business transactions over the Internet. The cost of the web server is US $100,000. The company estimates its annual cost to recover, based on three major intrusions it had in the past, as US $500,000, and the estimated savings gained by installing the web server as US $250,000. In this example:

- ALE = ($500,000 - $250,000) + $100,000 = $350,000
- ROSI = $500,000 - $350,000 = $150,000

References

Gordon, Lawrence A.; Martin P. Loeb; *The Economics of Information Security Investment*, ACM Transactions on Information and System Security, November 2002, p. 438-457

Matsuura, Kanta; *Information Security and Economics in Computer Networks: An interdisciplinary Survey and a proposal of Integrated Optimization of Investment*, Institute of Industrial Science, University of Tokyo, Japan, 2003

National Institute of Standards and Technology (NIST), *Security Metrics Guide for Information Technology Systems*, USA, 2003

Sonnenreich, Wes; 'Return on Security Investment (ROSI): A Practical Quantitative Model', *Journal of Research and Practice in Information Technology,* vol., 38, no. 1, February 2006, a publication of the Australian Computer Society, Australia, 2006

G42 Continuous Assurance

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S5 Planning states that the IT audit and assurance professional should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards.

1.1.2 Standard S6 Performance of Audit Work states that during the course of the audit, the IT audit and assurance professional should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by the appropriate analysis and interpretation of this evidence.

1.1.3 Standard S7 Reporting states that the IT audit and assurance professional should have sufficient and appropriate audit evidence to support the results reported.

1.1.4 Standard S14 Audit Evidence states that the IT audit and assurance professional should obtain sufficient and appropriate audit evidence to draw reasonable conclusions on which to base the audit results.

1.2 Linkage to Guidelines

1.2.1 Guideline G2 Audit Evidence Requirement provides guidance to the IT audit and assurance professional regarding the type and sufficiency of audit evidence used in information systems auditing.

1.2.2 Guideline G3 Use of Computer-assisted Audit Techniques (CAATs) provides guidance to the IT audit and assurance professional regarding the use of the many types of computer-assisted tools and techniques that can be used in performing various audit procedures.

1.2.3 Guideline G10 Audit Sampling provides guidance to the IT audit and assurance professional regarding the design and selection of an audit sample and evaluation of sample results.

1.3 Linkage to COBIT

1.3.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the IT governance requirement of IT audit and assurance professionals, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 The primary references are:

- DS5 *Ensure systems security*
- ME2 *Monitor and evaluate internal control*
- AI1 *Identify automated solution*

1.3.3 The information criteria most relevant are:

- Primary: Effectiveness, efficiency, confidentiality and integrity
- Secondary: Availability, compliance and reliability

1.4 Need for Guideline

1.4.1 Traditionally, the testing of controls has been performed on a retrospective and cyclical basis, often many months after business activities have occurred. The testing procedures have often been based on a sampling approach and included activities such as reviews of policies, procedures, approvals and reconciliations. Continuous assurance is a method used to perform control and risk assessments automatically on a more frequent basis. The main benefit of this approach is the intelligent and efficient continuous testing of controls and risks that result in timely notification of gaps and weaknesses to allow immediate follow-up and remediation.

1.4.2 While continuous assurance as a concept is not strictly limited to IT audit, IT audit and assurance professionals are often called upon to develop, implement and maintain continuous assurance processes and systems for their clients or within their enterprises. IT audit and assurance professionals can add value by leveraging the unique combination of business and technical skills and experience necessary to successfully implement continuous assurance processes and systems and engage the broad range of business and IT stakeholders involved.

1.4.3 This guideline provides guidance to IT audit and assurance professionals in applying the relevant IT audit and assurance standards during the planning, implementation and maintenance of continuous assurance processes and systems within an enterprise.

2. CONTINUOUS ASSURANCE, AUDITING AND MONITORING

2.1 CAATs and Continuous Assurance

2.1.1 Computer-assisted audit techniques (CAATs) are any automated audit technique that relate to generalised audit software, test data generators, integrated test facilities, computerized audit programs, and specialised audit and system software utilities.

2.1.2 Continuous assurance is an uninterrupted monitoring approach. It is a combination of an IT audit and assurance professional's oversight of management's continuous monitoring and an IT audit and assurance professional's continuous auditing approach using CAATs that allows management and IT audit and assurance professionals to monitor controls and risk on a continuous basis and to gather selective audit evidence using technology.

2.1.3 Continuous assurance is a process that can be used to provide timely reporting by IT audit and assurance professionals and lends itself to use in high-risk, high-volume paperless environments. It is an important tool for the IT audit and assurance professional to evaluate the control environment in an efficient and effective manner, and leads to increased audit coverage, more thorough and consistent analysis of data, and reduction in risk.

2.2 Continuous Auditing

2.2.1 Continuous auditing is a method used by the IT audit and assurance professional to perform control and risk assessments on a more frequent basis. It is a method using CAATs that allows IT audit and assurance professionals to monitor controls and risk on a continuous basis. This approach allows the IT audit and assurance professional to gather selective audit evidence through the computer.

2.3 Continuous Monitoring

2.3.1 Continuous monitoring is a management process to monitor whether policies, procedures and business processes are operating effectively on an ongoing basis. In addition to management-developed continuous monitoring processes, continuous auditing performed by IT audit and assurance professionals, when appropriate, may be transitioned to management, in which case it becomes a continuous monitoring procedure performed by management. Management's use of continuous monitoring procedures in conjunction with continuous auditing performed by the IT audit and assurance professional will satisfy the demands for assurance that control procedures are effective and that information produced for decision making is relevant and reliable.

3. PLANNING

3.1 Choosing Areas for Continuous Audit

3.1.1 The activity of choosing which areas to review using continuous auditing should be integrated as part of the development of the annual audit plan and should utilise the enterprise's risk management framework, if one has been developed. Rather than scheduling reviews according to a standard cycle, the frequency of reviews should be based on the risk factors in an area or business process. The IT audit and assurance professional should consider the following when deciding priority areas for continuous auditing:

- Identify the critical business processes that should be reviewed and prioritised based on risk.
- Review the enterprise's risk management framework, if one has been developed.
- Consider prior experience reviewing areas of the enterprise.
- Ascertain the availability and integrity of continuous auditing data for the risk areas identified.
- Prioritise the identified areas for review, considering where timely reporting of results might be of greater value to the enterprise.
- Determine the review frequency of the areas under review.
- Set the audit objectives of the areas to be reviewed that may be included in the terms of reference for the exercise.

4. RISK MANAGEMENT

4.1 Risk Identification and Assessment

4.1.1 Continuous auditing helps IT audit and assurance professionals to identify and assess risk and establish intelligent and dynamic thresholds that respond to changes in the enterprise. It also supports risk identification and assessment for the entire audit universe, contributing to the development of the annual audit plan as well as the objectives of a specific audit. The IT audit and assurance professional should review the enterprise's risk management framework, if one has been developed.

5. IMPLEMENTATION OF CONTINUOUS AUDITING

5.1 Engagement Planning

5.1.1 Successful implementation of continuous auditing requires the buy-in of stakeholders, including management, and a phased approach that initially addresses the most critical business systems. The following activities must be planned and managed when developing and supporting the use of continuous auditing:

- Prioritise areas for coverage and select an appropriate continuous auditing approach.
- Ensure the availability of key client personnel.
- Select the appropriate analysis tool—this could be in-house written routines or vendor-provided software.
- Develop continuous auditing routines to assess controls and identify deficiencies.
- Determine the frequency of applying continuous auditing routines.
- Define output requirements.
- Develop a reporting process.
- Establish relationships with relevant line and IT management.
- Assess data integrity and prepare data.
- Determine resource requirements, i.e., personnel, processing environment (the enterprise's IT facilities or IT audit facilities).
- Understand the extent to which management is performing its monitoring role (continuous monitoring).

5.2 Obtaining Management Support

5.2.1 Once the objectives of continuous auditing have been defined, senior management support should be obtained. Senior management must be informed of the preconditions, in particular the access requirements, as well as how and when the results will be reported. If this is done, when anomalies in transactions are identified and managers are contacted for explanations, the legitimacy of the continuous auditing activity will not be questioned.

5.2.2 Support from management can be obtained in conjunction with the approval of the terms of reference for the continuous auditing coverage. Support also should be obtained from the audit committee, if one has been formed. The period covered by the terms of reference for continuous auditing is usually longer than the period covered for a single assignment, and it is not unusual for the period covered to be up to one year.

5.3 Arrangements With the Auditee

5.3.1 Data files, such as detailed transaction files, are often only retained for a short period of time. Therefore, the IT audit and assurance professional should make arrangements for the retention of the data to cover the appropriate audit time frame.

5.3.2 Access to the enterprise's IT facilities, programs/system and data should be arranged well in advance of the needed time period to minimise the effect on the enterprise's production environment.

5.3.3 The IT audit and assurance professional should assess the effect that changes to the production programs/system may have on the use of continuous auditing routines. In doing so, the IT audit and assurance professional should consider the effect of these changes on the integrity and usefulness of the continuous auditing routines as well as the integrity of the programs/system and data used by the IT audit and assurance professional.

5.4 Developing Continuous Auditing Routines

5.4.1 The IT audit and assurance professional should obtain reasonable assurance of the integrity, reliability, usefulness and security of the continuous auditing routines, through appropriate planning, design, testing, processing and review of documentation. This should be done before reliance is placed on the continuous auditing routines. The IT audit and assurance professional should be able to demonstrate that the system development life cycle has been followed to ensure completeness and accuracy of the continuous auditing routines.

5.5 Scope of Continuous Assurance Testing

5.5.1 The extent to which detailed testing of controls and risks must be performed by the IT audit and assurance professional needs to be determined. A key factor in this determination will be the adequacy of the control environment and monitoring activities. The IT audit and assurance professional should examine the control framework and areas addressed by the enterprise risk management framework, if one has been developed. If management has well-established and functioning processes, including continuous monitoring, to assess controls and risk, the IT audit and assurance professional will be able to place more reliance on the control and risk levels being reported. However, if the processes are not adequate, the IT audit and assurance professional will, out of necessity, be required to perform detailed assessments of the controls and risks on a more continual basis.

5.6 Frequency of Testing

5.6.1 The IT audit and assurance professional should consider the objectives of continuous auditing, the risk appetite of the enterprise, the level and nature of management's continuous monitoring, and the enterprise risk activities, when setting the timing, scope and coverage of continuous auditing tests. IT audit and assurance professionals should prioritise the risks and select only a few high-risk areas or key control points for the first implementation of continuous auditing.

5.6.2 The next step is determining how often the continuous auditing tests will be run. The frequency of continuous auditing activities will range from a real-time or near real-time review of detailed transactions, to periodic analysis of detailed transactions, snapshots or summarised data. The frequency will depend not only on the level of risk associated with the system or process being examined, but also on the adequacy of the monitoring performed by management and resources available. Critical systems with key controls may be subject to real-time analysis of transactional data. Risk assessments to support the annual audit plan may be conducted quarterly, while those supporting individual auditing and the tracking of audit recommendations may occur on an *ad hoc* basis. The frequency of running continuous auditing routines should depend on risk. An important consideration when discussing frequency is that the automation of continuous auditing tests will lower the cost of performing risk assessments and control verification.

5.6.3 Finally, when determining how often and where continuous auditing will be performed, the IT audit and assurance professional should consider not only the regulatory requirements, but also the degree to which management is addressing the risk exposures and potential impacts. When management has implemented continuous monitoring systems for controls, internal and external audit and assurance professionals can take this into account and decide the extent to which they can rely on the continuous monitoring processes to reduce detailed controls testing.

5.7 Data Integrity and Security Concerns

5.7.1 Where continuous auditing routines are used to extract information for data analysis, the IT audit and assurance professional should verify the integrity of the information systems and IT environment from which the data have been extracted.

5.7.2 Sensitive program/system information and production data should be kept securely. The IT audit and assurance professional should safeguard the program/system information and production data with an appropriate level of security to ensure confidentiality. In doing so, the IT audit and assurance professional should consider the level of confidentiality and security required by the enterprise owning the data and any relevant legislation.

5.7.3 The IT audit and assurance professional should use and document the results of appropriate procedures to provide for the ongoing integrity, reliability, usefulness and security of the continuous auditing routines. For example, this should include a review of program maintenance and program change controls to determine that only authorised changes were made to the continuous auditing routines.

5.7.4 When the continuous auditing routines reside in an environment not under the control of the IT audit and assurance professional, an appropriate level of control should be in effect to identify changes to the continuous auditing routines. When the continuous auditing routines are changed, the IT audit and assurance professional should obtain assurances of their integrity, reliability, usefulness and security, through appropriate planning, design, testing, processing and review of documentation, before reliance is placed on the continuous auditing routines.

6. OVERSIGHT OF CONTINUOUS MONITORING

6.1 Continuous Monitoring

6.1.1 Continuous monitoring refers to the processes that management puts in place to ensure that the policies, procedures and business processes are operating effectively. It typically addresses management's responsibility to assess the adequacy and effectiveness of controls. Many of the techniques management uses to continuously monitor controls are similar to those that may be performed in continuous auditing by the IT audit and assurance professional. Continuous assurance also monitors the effectiveness of management monitoring.

6.1.2 The key to continuous monitoring is that the process should be owned and performed by management as part of its responsibility to implement and maintain an effective control environment. Since management is responsible for internal controls, it should have a means to determine, on an ongoing basis, whether the controls are operating as designed. By being able to identify and correct control problems on a timely basis, the overall control system can be improved. A typical additional benefit to the enterprise is that instances of error and fraud can be reduced. There is an inverse relationship between the adequacy of management's monitoring and risk management activities and the extent to which IT audit and assurance professionals must perform detailed testing of controls and assessments of risk. The IT audit and assurance professional's approach to, and amount of, continuous auditing depends on the extent to which management has implemented continuous monitoring.

6.2 Responsibilities of Management

6.2.1 Management is responsible for implementing processes and systems that continuously monitor the control environment to ensure that the operation of key controls, including policies, procedures and business processes, is meeting the intended business objectives in an efficient and effective manner.

6.2.2 Management may use various techniques to implement continuous monitoring of the control environment, including:

- Defining the risk and control points within a business process
- Identifying the control objectives and assertions for the business process
- Designing manual and automated controls to address the specific control objectives
- Testing the operation of these manual and automated controls
- Monitoring the operation of the manual and automated controls across normal business transactions
- Investigating control exceptions identified by management controls
- Taking any necessary action to remedy control weaknesses or transaction errors detected
- Updating and retest manual and automated controls to reflect changing business processes

6.3 Responsibilities of IT Audit and Assurance Professionals

6.3.1 IT audit and assurance professionals are required to provide oversight and assurance to the audit committee, if one has been formed, and other key stakeholders that continuous monitoring processes and systems are operating in an efficient and effective manner to address specific control objectives.

6.3.2 IT audit and assurance professionals may use several techniques to oversee the operation of management's continuous monitoring activities, including:

- Reviewing and testing the controls over the development of continuous monitoring mechanisms, including the documentation, systems development life cycle, training, logical access and change controls relating to key continuous monitoring activities
- Comparing the output of management's continuous monitoring activities to the results of similar continuous auditing procedures executed by the IT audit and assurance professional, for instance, comparing exception reports to ensure that the management reports are detecting potential errors completely and accurately
- Reviewing prior management reports and discussing with management what actions have been taken on the exceptions noted and the outcomes of such actions

7. PERFORMANCE OF CONTINUOUS AUDITING WORK

7.1 Gathering Audit Evidence

7.1.1 The use of continuous auditing routines should be controlled by the IT audit and assurance professional to provide reasonable assurance that the audit objectives and the detailed specifications of the routines have been met. The IT audit and assurance professional should:

- Perform a reconciliation of control totals where appropriate
- Review output for reasonableness
- Perform a review of the logic, parameters or other characteristics of the routines
- Review the enterprise's general IT controls that may contribute to the integrity of the continuous auditing routines (e.g., program change controls and access to system, program, and/or data files)

7.2 Interpretation of Continuous Auditing Results

7.2.1 Once the tests have been run, the IT audit and assurance professional should review the results to identify where problems exist. Control weaknesses are evidenced by transactions that fail the control tests. Increased levels of risk can be identified by comparative analysis (i.e., comparing one process to other processes, one entity to other entities, or running the same tests and comparing results over time). One of the practical challenges of implementing a continuous auditing or monitoring system is the efficient response to control exceptions and risks that are identified. When a continuous auditing or monitoring system is first implemented, it is not unusual for a large number of exceptions to be identified that, upon investigation, prove not to be a concern. The continuous auditing system needs to allow the test parameters to be adjusted so that, where appropriate, such exceptions do not result in alerts or notifications. Once the process of identifying such false-positives is performed, the system increasingly can be relied upon to only identify control deficiencies or risks of significant concern. In addition, the nature of the audit response to the identified transactions will vary, and not all will require an audit or immediate action. The results should be prioritised and acted upon accordingly. Details to be maintained should include:

- The results obtained
- Decisions regarding what action will be taken
- Who was notified and when
- The expected response date

7.3 Management Action

7.3.1 If a continuous auditing finding is referred to management, the IT audit and assurance professional should also request a management response outlining the action plan and date. Once the appropriate action has been taken, the IT audit and assurance professional should run the continuous auditing test again to see if the remediation has addressed the control weakness or reduced the level of risk. Subsequent tests should not identify the same problem.

7.4 Fine-tuning Continuous Assurance Routines

7.4.1 The use of a properly designed continuous auditing application will assist the audit activity in its role of providing assurance that management is maintaining an effective control framework and actively managing risk. However, continuous auditing must remain flexible and responsive to changes in the exposures and the control environment. It is not something that can be implemented and left alone for months. The IT audit and assurance professional should review the efficiency and effectiveness of the continuous auditing program periodically. Additional control points or risk exposures may need to be added, and others may be dropped. Thresholds and control tests and parameters for various analytics may need to be tightened or relaxed. During this review, the IT audit and assurance professional should also ensure that the results from continuous auditing are included in other management activities, such as enterprise resource management (ERM), balanced scorecard, and performance measurement and monitoring activities.

7.5 Documentation of Continuous Assurance Results

7.5.1 The continuous auditing process should be sufficiently documented to provide adequate audit evidence.

7.5.2 Specifically, the audit working papers should contain sufficient documentation to describe the continuous auditing routines, including the details set out in the following sections.

7.6 Planning Documentation

7.6.1 Documentation should include:

- Continuous auditing objectives
- Continuous auditing routines to be used
- An assessment of the continuous monitoring process owned by management
- Controls to be exercised
- Staffing and timing
- Who is getting the report

7.7 Execution Documentation

7.7.1 Documentation should include:

- Preparation and testing procedures and controls for the continuous auditing routines
- Details of the tests performed by the continuous auditing routines
- Details of inputs (e.g., data used, file layouts), processing (e.g., high-level flowcharts, logic) and outputs (e.g., log files, reports)
- Lists of relevant parameters or source code

7.8 Audit Evidence Documentation

7.8.1 The usual standard of documentation of audit evidence should apply to a continuous auditing assignment. Documentation should include:

- Output produced
- Description of the audit or an analysis of the audit work performed on the output
- Audit findings
- Audit conclusions
- Audit recommendations

7.8.2 Data and files used should be stored in a secure location.

8. REPORTING

8.1 Time Between Fieldwork Completion and Date of Report

8.1.1 In the traditional audit model (used by both internal and external auditors), a period of time passes between the completion of fieldwork and issuance of the related audit report. In many instances, the impact of this delay in issuance makes the information contained in the report less useful or beneficial to the user. This is a result of the aging of the information contained in the report that can be affected by such issues as auditee corrections to identified deficiencies or further deterioration to the control environment (or related auditee data) resulting from identified control weaknesses or deficiencies.

8.2 Continuous Assurance Reporting

8.2.1 Continuous auditing, therefore, is designed to enable IT audit and assurance professionals to report on subject matter within a much shorter time frame than under the current model. Theoretically, in some environments, it should be possible to shorten the reporting time frame to provide almost instantaneous or truly continuous assurance. The reporting process needs to be defined with stakeholders to ensure a more timely response and reporting of issues arising from continuous assurance exercises. Critical issues should be reported as soon as possible.

8.2.2 By definition, continuous auditing requires a higher degree of reliance on an auditee's information systems than traditional auditing requires. This is a result of the need to rely upon system-generated information vs. externally produced information as the basis for audit testing. Hence, IT audit and assurance professionals need to make judgements on both the quality of the auditee's systems as well as the information produced by the system itself. Systems that are of lower quality, or produce less-reliable information, (and require a higher degree of manual intervention) are less conducive to continuous auditing than those that are of high quality and produce reliable information.

8.2.3 Environments that are of a higher quality and produce reliable information are better suited to reporting periods of a short to continuous duration. Environments that are of a lower quality or produce less-reliable information should use longer reporting periods to compensate for the period of time that must pass for users to review and approve or correct information processed by the system.

8.3 Description of Continuous Assurance

8.3.1 The objectives, scope and methodology section of the report should contain a clear description of the continuous assurance process used. This description should be sufficiently detailed and should provide a good overview for the reader.

8.3.2 The description of the continuous auditing routine's objectives should also be included in the body of the report, where the specific finding related to the use of the routine is discussed.

8.3.3 If the description of the routine used is applicable to several findings, or is too detailed, it should be discussed briefly in the objectives, scope and methodology section of the report and the reader referred to an appendix with a more detailed description.

9. EFFECTIVE DATE

9.1 This guideline is effective for all IT audits beginning 1 May 2010.

10. REFERENCES

10.1 The Institute of Internal Auditors, 'Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment, Global Technology Audit Guide', USA, 2005

11. ACKNOWLEDGEMENTS

11.1 Kevin Mar Fan, CISA, CA, Brisbane City Council, Australia, assisted with the development of this guideline.

IT Audit and Assurance Tools and Techniques

IS Risk Assessment Measurement Procedure P1

1. BACKGROUND

1.1 Linkage to Standards/Guidelines

1.1.1 Standard S5 Planning states, "The IS auditor should plan the information systems audit coverage to address the audit objectives and comply with applicable laws and professional auditing standards."

1.1.2 Standard S6 Performanceof Audit Work states, "During the course of the audit, the IS auditorshould obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

1.1.3 Guideline G13 Use of Risk Assessment in Audit Planning provides guidance.

1.2 Need for Procedure

1.2.1 This procedure is designed to provide:

- A definition of IS audit risk assessment
- Guidance on the use of a IS audit risk assessment methodology for use by internal audit functions
- Guidance on the selection of risk ranking criteria and the use of weightings

2. IS RISK

2.1 Risk is the possibility of an act or event occurring that would have an adverse effect on the organisation and its information systems. Risk can also be the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of, or damage to, the assets. It is ordinarily measured by a combination of effect and likelihood of occurrence.

2.2 Inherent risk refers to the risk associated with an event in the absence of specific controls.

2.3 Residual risk refers to the risk associated with an event when the controls in place to reduce the effect or likelihood of that event are taken into account.

3. IS RISK ASSESSMENT MEASUREMENT

3.1 Risk assessment measurement is a process used to identify and evaluate risks and their potential effect.

4. IS AUDIT RISK ASSESSMENT MEASUREMENT METHODOLOGY

4.1. IS audit risk assessment measurement is a methodology to produce a risk model to optimise the assignment of IS audit resources through a comprehensive understanding of the organisation's IS environment and the risks associated with each auditable unit. See Section 9 for details of auditable units.

4.2. The objective of a risk model is to optimise the assignment of IS audit resources through a comprehensive understanding of the IS audit universe and risks associated with each universe item.

5. RISK-BASED IS AUDIT APPROACH

5.1. More and more organisations are moving to a risk-based audit approach that can be adapted to develop and improve the continuous audit process. This approach is used to assess risk and to assist an IS auditor's decision to do either compliance testing or substantive testing. In a risk based audit approach, IS auditors are not just relying on risk. They are also relying on internal and operational controls as well as knowledge of the organisation. This type of risk assessment decision can help relate the cost/benefit analysis of the control to the known risk, allowing practical choices.

5.2. By understanding the nature of the business, IS auditors can identify and categorise the types of risks that will better determine the risk model or approach used in conducting the review. The risk assessment model can be as simple as creating weights for the types of risks associated with the business and identifying the risk in an equation. On the other hand, risk assessment can be a scheme where risks have been given elaborate weights based on the nature of the business or the significance of the risk.

5.3 The IS auditor is interested in uncontrolled risks and in critical controls. Thus in a risk-based audit approach the IS auditor will be interested in technology-based systems which provide controls for business functions where there is a high inherent risk and in technology-based functions where there is a higher than acceptable residual risk.

5.4 Defining the IS audit universe is the first prerequisite to risk ranking. The determination of the audit universe will be based on knowledge of the organisation's IT strategic plan and organisation operations, a review of organisation charts and function and responsibility statements of all organisation affiliates, and discussions with responsible management personnel.

5.5 Audit planning cycles are ordinarily aligned with business planning cycles. Often, an annual audit planning cycle is selected—either a calendar year or another twelve-month period. Some organisations have planning cycles other than for twelve month periods such as six or eighteen months. Rather than have a fixed planning cycle, some organisations have rolling planning cycles that keep rolling forward a set period. For consistency, this procedure will assume an annual audit planning cycle.

5.6 Selection of audit projects to be included in the IS audit plan is one of the most important problems confronting IS audit management. The audit planning process presents the opportunity to quantify and justify the amount of IS audit resources needed to complete the annual IS audit plan. Failure to select appropriate projects results in unexploited opportunities to enhance control and operational efficiency.

5.7 The assumption underlying the IS audit plan is that an evaluation of prospective audit reviews/projects will be more effective if a formal process is followed for gathering the information necessary to make review/project selection decisions. The approaches described herein are basically a framework in which to apply common sense and professional judgment.

5.8 The methodology presented is relatively simple. However, in a great majority of cases, it should suffice to reach reasonable, prudent and defensible IS audit review/project selection decisions. A framework to use in performing a risk exposure analysis and establishing an audit review/project priority schedule is detailed in this procedure.

5.9 As used here, risk assessment is a technique used to examine auditable units and choose reviews/projects that have the greatest risk exposure. A risk assessment approach to audit review/project selection is important in that it affords a means of providing reasonable assurance that IS audit resources are deployed in an optimal manner, i.e., the IS audit plan allocates IS audit resources in a manner likely to achieve maximum benefits. To this end, the risk assessment approach provides explicit criteria for systematically selecting audit projects. The IS audit plan is often attached with the financial and operational audit plan to detail the complete planned IS audit coverage.

6. IS RISK ASSESSMENT MEASUREMENT TECHNIQUES

6.1 When determining which functional areas should be audited, the IS auditor could face a large variety of audit subjects. If possible all IS areas of the organisation should be included in the risk assessment exercise. Some organisations only rate IS projects. Others rate every IS auditable area/system. Each of these may represent different types of audit risks. The IS auditor should evaluate these various risk candidates to determine which are the high-risk areas and therefore should be audited. The purpose of this process is to:

- Identify areas where the residual risk is unacceptably high
- Identify critical control systems that address high inherent risks
- Assess the uncertainty that exists in relation to the critical control systems

6.2 Using risk assessment to determine IS areas to be audited:

- Enables management to effectively allocate limited IS audit resources
- Provides reasonable assurance that relevant information has been obtained from all levels of management, including the board of directors and functional area management. Generally, the information includes areas that will assist management in effectively discharging their responsibilities and provides reasonable assurance that the IS audit activities are directed to high business risk areas and will add value to management.
- Establishes a basis for effectively managing the IS audit function
- Provides a summary of how the individual review subject is related to the overall organisation as well as to the business plans

7. IS RISK ASSESSMENT MEASUREMENT METHODS

7.1 Several methods are currently employed to perform IS risk assessments. One such risk assessment approach is a scoring system that is useful in prioritising IS audits based on an evaluation of risk factors that consider variables such as technical complexity, extent of system and process change and materiality. These variables may or may not be weighted. These risk values are then compared to each other and ordinarily an annual IS audit plan is prepared. Often the IS audit plan is approved by the audit committee and or the chief executive officer. Reviews are then scheduled according to the IS audit plan. Another form of IS risk assessment is judgmental. This entails making an independent decision based upon executive management directives, historical perspectives and business climate.

8. COLLECTION OF DATA

8.1 Information describing all aspects of the organisation's operation will be used to define the various auditable units and to model the IS risks inherent in the unit's operations. Sources of this data include:

- Interviews conducted with senior management for the purpose of gathering data for the development of the IS risk model
- Returns of structured questionnaires sent to management to facilitate the gathering of IS risk model data
- Recent review reports
- The IT strategic plan
- The budgetary process may be a useful source of information
- Issues raised by the external auditors
- IS audit knowledge and awareness of significant issues gathered from any other sources
- The specific methods used to collect the data, whether they will be sufficient considering the time and resources available for the task

IS Risk Assessment Measurement Procedure P1 cont.

9. IS AUDITABLE UNITS

9.1 The model is meant to include and provide a risk rating for every IS auditable unit in the organisation (the IS audit universe). An auditable unit can be defined as the discrete segments of every organisation and its systems. There are no specific rules for determine or differentiate an individual auditable unit. However, the following are guidelines for use in this audit risk model for each unit/topic/function:

- Auditable in a reasonable timeframe
- A system, i.e., have recognisable inputs, processes, outputs, outcome
- Separable, i.e., able to be audited with minimal reference to other systems (This may be difficult if an application system under review has many interfaced systems.)

10. EXAMPLES

10.1 There are many different methods of performing IS risk assessment measurements. Sections 11 through 14 contain several types of IS risk assessments.

11. EXAMPLE I

11.1 Example I shows an IS risk assessment measurement evaluation with eight key variables. Each unit/area in the IS audit universe will be rated on these eight key variables using a numeric descriptive value ranking of 1 (low) to 5 (high). The results of these ranking judgments are then multiplied by significance weighting factors that range from 1 (low) to 10 (high) to give an extended value. Arbitrary examples of significance weighting factors are included in example I. These extended values are added together to give a total. Once the totals for each auditable unit/area have been obtained, the auditable units/areas are ranked by risk. The framework of the annual IS audit plan is then built from these rankings. The eight key variables are listed in sections 11.1.1 to 11.1.3 with a brief explanation of each.

11.1.1 Measures of Effect

- **Character of activity**—The criticality of the activity and the part of the organisation that utilises the activity. Infrequent or unusual activities or projects are more likely to result in error or inefficiency and are of greater audit interest.
- **Fall back arrangements**—This factor relates to the measures that have been put in place to continue operations if the new system has problems. Factors to consider include business continuity plans, disaster recovery plans, manual procedures, and the old system.

Generally speaking, if the above issues have been addressed, are achievable or are cost beneficial, then the risk is lowest.

- **Sensitivity of the function to executive management**—This factor relates to how important the unit, function or area is viewed by executive management.
- **Materiality**—A concept regarding the importance of an item of information with regard to the effect on the functioning of the organisation. An expression of the relative significance or importance of a particular matter in the context of the organisation as a whole.

11.1.2 Measures of Likelihood

- **Extent of system or process change**—A dynamic environment in terms of system or process change increases the probability of errors and consequently increases audit interest. A considerable amount of process re-engineering may have taken place. System or process change ordinarily occurs to effect improvement in the long term but often has short-term offsets that require increased audit coverage**.**
- **Complexity**—This risk factor reflects the potential for errors or misappropriation to go undetected because of a complicated environment. The rating for complexity will depend on many factors. Extent of automation, complex calculations, interrelated and interdependent activities, number of products or services, the time spans of estimates, dependency on third parties, customer demands, processing times, applicable laws and regulations and many other factors, some not recognised, affect judgments about the complexity of a particular audit.
- **Project management**—Consideration should be given to the following when ranking project management:
  - In-house or outside developers
  - Project structure
  - Personnel skills
  - Project timeframes

Generally speaking, the risk is shared if the project is outsourced.

11.1.3 Measures of Uncertainty about the Controls

- **Period since last review**—As the time since the last review coverage lengthens, the value of a new review is likely to increase. The beneficial effects of a review are greatest immediately before or after system implementation.

IS Risk Assessment Measurement Procedure P1 cont.

EXAMPLE I—IS RISK ASSESSMENT MEASUREMENT EVALUATION

KEY VARIABLES	DESCRIPTIVE VALUE 1 (low) to 5 (high)	SIGNIFICANCE WEIGHTING 1 (low) to 10 (high)	EXTENDED VALUE
1. **Character of activity**	**Consider:** Core activity = 4 to 5 Business unit = 2 to 3 Local system = 1	8*	
2. **Fall back**	**Consider:** Business continuity plans Disaster recovery plans Manual procedures Old system	5*	
3. **Sensitivity of the function to executive management**	Major interest = 4 to 5 Moderate interest = 2 to 3 Minor interest = 1	6*	
4. **Materiality**	**Significance of expenditures or revenues generated or resources consumed.** Project budget >$500,000 = 4 to 5 Project budget $100,000 to $500,000 = 2 to 3 Project budget <$100,000 = 1 Revenue/expenditure >$500,000 = 4 to 5 Revenue/expenditure $100,000 to $500,000 = 2 to 3 Revenue/expenditure <$100,000 = 1	5*	
5. Extent of system, procedure and process change	**Consider:** The extent of reengineering. Major reengineering = 4 to 5 Moderate reengineering = 2 to 3 Minor reengineering = 1 Or No procedures = 4 or 5 Local procedures = 3 or 2 Corporate procedures = 1	8*	
6. **Complexity**	**Consider:** Transactions volume Number of users Centralised or decentralised Number of interfaces Very complex = 4 to 5 Moderately complex = 2 to 3 Simple = 1	7*	
7. **Project management**	**Consider:** In-house or outside developers Project structure Personnel skills Project timeframes	7*	
8. **Period since last review**	Rating of 5 indicates 5 years or more since last audit or never	1*	
	Total		

* Uses arbitrary Significance Weighting Example

IS Risk Assessment Measurement Procedure P1 cont

12. EXAMPLE II

12.1 Example II extends the IS risk assessment measurement evaluation used in example I by incorporating business risks as well as the eight IS audit key variables used in example I. The IS audit risk ranking factor (from example I) is multiplied by business risk in this example. The business risk factors (financial, strategic, operational, and legal compliance) are considered regarding their relevance to each auditable unit/area.

12.2 Each unit/area in the IS audit universe will be rated on these eight key variables using a numeric rating of 1 (low) to 5 (high). The results of these rating judgments are then multiplied by a significance weighting factor, which ranges from 1 (low) to 10 (high) as in example I. These extended values are added together to give a total (using the arbitrary significance weightings used in example I). This total is the IS audit risk ranking factor.

12.3 The four business risk factors are defined below:

- **Financial risk**—As most systems potentially have some effect on the organisation's financial performance, the level and likelihood of such an effect needs to be considered. If the anticipated effect is indirect and relatively minor in comparison with other effects and purposes of the system and/or in comparison with other auditable areas/systems then we would probably score 0 rather then 1 for the financial risk factor.
- **Strategic risk**—Systems may have direct strategic effect on the organisation. Some that would be expected to score 1 on the risk factor are those identified by executive management.
- **Operational risk**—Operational risk will probably be rated 1 more commonly than any of the other business risk factors since most systems are designed to affect the manner in which, and the effectiveness with which, the organisation conducts its day-to-day business.
- **Legal compliance**—Systems can have a direct effect on how the organisation complies with statutory obligations.

12.4 Insert a score of 1 (relevant) or 0 (not relevant) for each *business risk factor*. Then multiply each score by the respective weighting and add, to give the total *business risk ranking factor* for each audit topic.

12.5 In assigning scores consider the following three issues:

- What are the anticipated purpose and objectives of the system being audited?
- What are the anticipated scope and objectives of the audit?
- Does the system directly effect the organisation's financial/strategic/operational/compliance performance? For example, if the system does not operate as intended, is it probable that the organisation will suffer financial loss, experience strategic disadvantage, have operational problems or contravene relevant legal requirements?

12.6 The final step in this example is to multiply the *audit risk* ranking factor by the *business risk ranking factor*, to give the *total risk ranking*. See the example in the table below. Once the *total risk rankings* for each auditable unit/area have been obtained the auditable units/areas are ranked by risk. The framework of the annual IS audit plan is then built from these rankings.

EXAMPLE II—IS RISK ASSESSMENT MEASUREMENT EVALUATION INCORPORATING BUSINESS RISK FACTORS

AUDITABLE UNIT	AUDIT RISK RANKING (from Example I)	BUSINESS RISK FACTORS (RATE 0 OR 1)				BUSINESS RISK RANKING FACTOR	TOTAL RISK RANKING
		FINANCIAL	STRATEGIC	OPERATIONAL	LEGAL COMPLIANCE		
Business	**Risk weighting**	**5***	**4***	**3***	**2***		
Treasury system	158	1	1	1	0	12	1896
Business continuity	162	0	0	1	1	5	810
Payroll	165	0	0	1	0	3	495
Local area networks	159	0	0	1	0	3	477
Computer operations	146	0	0	1	0	3	438
Software licencing	123	0	0	0	1	2	246
RACF	152	0	0	1	0	3	456

For Example-Treasury System: 158 *(5*1+4*1+3*1+2*0)=158*(5+4+3)=158*12=1896

IS Risk Assessment Measurement Procedure P1 cont.

13. EXAMPLE III

13.1 Some IS auditors prefer to just rank IS projects and not the whole IS auditable universe. Example III provides a methodology to rank IS projects. Each IS project in the IS audit universe will be rated on these eight key variables using a numeric risk value ranking of 1 (low) to 5 (high). The results of these ranking judgments are then multiplied by a Weighting factor that ranges from 1 (low) to 10 (high) to give an extended value. These extended values are added together to give a total. Once the totals for each project have been obtained, the projects are ranked by risk. The framework of the annual IS audit project coverage is then built from these rankings. The categories used in Example III are listed in 13.2 and 13.3.

13.2 Measures of Effect

- **Project budget**—The total budget of an IS project is an important factor to consider. As a guide, some organisations rank project budgets over US$500,000 as a risk level of 4 or 5. These organisations rank budgets between US $100,000 to US$ 500,000 as a risk ranking of 2 or 3 and budgets under US $100,000 as a risk level of 1.
- **Transaction volume**—The total volume of transactions that are estimated to be processed by the system in a given period.
- **Character of activity**—The criticality of the activity and the part of the organisation that utilises the activity. Infrequent or unusual activities or projects are more likely to result in error or inefficiency and are of greater audit interest.
- **Executive management interest**—This factor relates to how important the unit, function or area is viewed by executive management.
- **Fall back arrangements**—This factor relates to the measures that have been put in place to continue operations if the new system has problems. Factors to consider include:
  - Business continuity plans
  - Disaster recovery plans
  - Manual procedures
  - Old system

Generally speaking, if the above issues have been addressed, are achievable or are cost beneficial then the risk is lowest.

13.3 Measures of Likelihood

- **Changes in procedures**—The extent of procedural change or reengineering accompanying the system implementation.
- **Complexity of system**—Factors such as number of users, number of system modules, mainframe versus a client-server environment (centralised versus a decentralised environment), and the number of interfaces are considered.
- **Project management**—Consideration should be given to the following when ranking project management:
  - In-house or outside developers
  - Project structure
  - Personnel skills
  - Project timeframes

Generally, speaking the risk is shared if the project is outsourced.

EXAMPLE III—IT PROJECT RISK RANKING

Category	Risk level 1(Low) to 5(High)	Significance weighting 1(Low) to 10(High)	Total
1. Project budget >$500,000 = 4 to 5 $100,000 to $500,000 = 2 to 3 <$100,000 = 1		**5**	
2. Transaction volume		**2**	
3. Character of activity Core council 4 to 5 Business unit 2 to 3 Local system 1		**8**	
4. Executive management interest Major interest = 4 to 5 Moderate interest = 2 to 3 Minor interest = 1		**6**	
5. Fall-back arrangements Business continuity/ disaster recovery plans Manual procedures Old system		**7**	
6. Changes in procedures (Extent of reengineering) Major reengineering = 4 to 5 Moderate reengineering = 2 to 3 Minor reengineering = 1		**8**	
7. Complexity of system Number of users Number of modules Centralised or decentralised (mainframe v. client-server) Interfaces		**7**	
8. Project management In-house Outside developers Structure Skills Timeframe		**7**	
		Total	

14. EXAMPLE IV—IS RISK ASSESMENT OF AUDITABLE UNITS

14.1 Example IV ranks various categories of auditable units in the IS auditable universe after they have been identified. The categories are listed based on the nature of risk that these units are exposed to. Relevant information, such as, financial exposure, effect on business, and scope is collected. The categories are as follows:

i. Data centre operations
ii. Application systems (production)
iii. Application systems (development)
iv. IS procurement (manpower and material)
v. Software package acquisition
vi. Other IS functions

14.2 Under each category, major risk components are enumerated. Depending on the type of risk a weight is assigned to each risk element. Each risk element is then further subdivided and a score attached to it. This risk score of a particular risk element is the product of the *score* and its weight. The total risk score of the function is the sum of the scores of all its risk elements. For ease of comparison, the risk score is measured on a scale of 100. Separate risk assessment sheets can been prepared for each of the auditable unit. Finally the scores obtained for each of the auditable units are consolidated and audits prioritised.

IS Risk Assessment Measurement Procedure P1 cont.

EXAMPLE IV—RISK ASSESSMENT—IS AUDIT
i. DATA CENTRE OPERATIONS

	Rating factor	Weight	Score	Assigned score
1.	**Number of data centre staff**	**1**		5
	Very small under 2		1	
	Small 3—7		2	
	Moderate 7—15		3	
	Large 16—25		4	
	Very large Above 25		5	
2.	**Effect on the group's business**	**5**		25
	No effect		1	
	Small		2	
	Moderate		3	
	High		4	
	Put Group out of business		5	
3.	**Number of applications**	**5**		25
	Single		1	
	Under 5		2	
	5—15		3	
	16—25		4	
	Above 25		5	
4.	**Number of users**	**2**		10
	Below 25		1	
	26—50		2	
	51—100		3	
	100—250		4	
	Above 250		5	
5.	**Prior audit findings**	**1**		5
	No significant findings		1	
	A few insignificant findings		2	
	Many Insignificant findings		3	
	A few significant findings		4	
	Many significant findings		5	
6.	**Sophistication of processing**	**2**		10
	Batch		1	
	Batch/real-time		2	
	Batch/real-time/online		3	
	Client/server		4	
	Parallel/distributed		5	
7.	**Changes in equipment/platform/staff**	**1**		5
	No changes		1	
	Moderate changes/low turnover		2	
	Platform changes/low turnover		3	
	High turnover		4	
	Platform changes and high turnover		5	
8.	**Number of platforms**	**3**		15
	1		1	
	2		2	
	3		3	
	4		4	
	5+		5	
	Total risk score		100	100

IS Risk Assessment Measurement Procedure P1 cont.

EXAMPLE IV—RISK ASSESSMENT—IS AUDIT
ii. APPLICATION SYSTEMS (PRODUCTION)

	Rating factor	Weight	Score	Assigned score
1.	**Effect of system failure (criticality)**	**5**		25
	No immediate effect		1	
	Inconvenience to users		2	
	Loss of goodwill		3	
	Loss of revenue		4	
	Loss of business/revenue/goodwill		5	
2.	**Financial exposure (AED)**	**5**		25
	None		1	
	Small (<100,000)		2	
	Moderate (100,000—1 m)		3	
	High (1m—10 m)		4	
	Very high (>10 m)		5	
3.	**Scope of the system**	**2**		10
	Part of a department		1	
	Complete department		2	
	Multidepartment		3	
	Organisationwide		4	
	Organisation and external		5	
4.	**Age of the application**	**1**		5
	Over 10 years		1	
	7—10 years		2	
	4—6 years		3	
	1—3 years		4	
	Less than one year		5	
5.	**Prior audit findings**	**2**		10
	Recent Audit—no weaknesses		1	
	Recent Audit—minor weaknesses		2	
	Audit—Some weaknesses		3	
	Audit—Many weaknesses		4	
	No previous audit		5	
6.	**Size of the application (number of programs)**	**3**		15
	Below 25		1	
	25—50		2	
	50—100		3	
	100—250		4	
	Above 250		5	
7.	**Changes in environment/staff**	**1**		5
	No changes		1	
	Moderate changes/low turnover		2	
	Significant changes/low turnover		3	
	High turnover		4	
	Significant changes and high turnover		5	
8.	**Number of locations implemented**	**1**		5
	1		1	
	2		2	
	3		3	
	4		4	
	5+		5	
	Total risk score		**100**	100

IS Risk Assessment Measurement Procedure P1 cont.

EXAMPLE IV—RISK ASSESSMENT—IS AUDIT
iii. APPLICATION SYSTEMS (DEVELOPMENT)

	Rating factor	Weight	Score	Assigned score
1.	**Size, organisation and experience of team**	**3**		15
	Small, dedicated and experienced team		1	
	Average size, centralised and experienced team		2	
	Average, experienced and mixed priorities		3	
	Average, mostly centralised with other priorities		4	
	Large, decentralised, inexperienced and unclear reporting		5	
2.	**Size of the system**	**3**		15
	Small number of programs for 1 department		1	
	Moderate number of programs for 1 department		2	
	Large number of programs for many departments		3	
	Moderate number of programs for entire organisation		4	
	Large number of programs for entire organisation		5	
3.	**Duration of the development cycle**	**2**		10
	Less than 3 months		1	
	3—6 months		2	
	6—12 months		3	
	1—$1^1/_2$ years		4	
	2 or more years		5	
4.	**Development platform**	**3**		15
	Tried and widely used		1	
	Fairly new but accepted worldwide		2	
	Fairly new but not accepted worldwide		3	
	Tried and proprietary		4	
	New, untried proprietary		5	
5.	**Prior audit involvement**	**2**		10
	Controls building exercise		1	
	Requirement analysis phase		2	
	Project schedule monitoring		3	
	Project cost monitoring		4	
	None		5	
6.	**System development methodology**	**3**		15
	Standard methodology with documented standards and procedures		1	
	Standard methodology without documented standards and procedures		2	
	No standard methodology but experienced team		3	
	Experimental untried methodology		4	
	No development methodology used and no documented development standards and guidelines		5	
7.	**Project management experience**	**1**		5
	Very high		1	
	Above average		2	
	Average		3	
	Below average		4	
	No experience/multiproject		5	
8.	**Manpower outsourcing**	**1**		5
	Small quantity, single supplier		1	
	Small quantity, heterogeneous suppliers		2	
	Significant quantity, single suppliers		3	
	Significant quantity, heterogeneous suppliers		4	
	100%		5	
	Total risk score		**100**	**100**

IS Risk Assessment Measurement Procedure P1 cont.

EXAMPLE IV—RISK ASSESSMENT—IS AUDIT
iv. IS PROCUREMENT (MANPOWER AND MATERIAL)

	Rating factor	Weight	Score	Assigned score
1.	**Effect**	**5**		25
	No immediate effect			
	Inconvenience to users		1	
	Loss of goodwill		2	
	Loss of revenue		3	
	Loss of business/revenue/goodwill		4	
			5	
2.	**Financial exposure (AED)**	**5**		25
	None		1	
	Small (<100,000)		2	
	Moderate (100,000—1 m)		3	
	High (1m—10 m)		4	
	Very high (>10 m)		5	
3.	**Procedures and guidelines**	**5**		25
	Documented and tested procedures		1	
	Procedures not documented		2	
	Procedures but not implemented fully		3	
	No set procedures but controlled		4	
	No set procedures and uncontrolled		5	
4.	**Prior audit findings**	**2**		10
	Recent audit—No weaknesses		1	
	Recent audit—Minor weaknesses		2	
	Audit—Some weaknesses		3	
	Audit—Many weaknesses		4	
	No previous audit		5	
5.	**Complexity**	**3**		15
	Local sourcing for one department		1	
	Local sourcing for entire organisation		2	
	International sourcing for one technology		3	
	International sourcing for multitechnology		4	
	International and local sourcing for multitechnology		5	
	Total risk score		**100**	**100**

IS Risk Assessment Measurement Procedure P1 cont.

EXAMPLE IV—RISK ASSESSMENT—IS AUDIT
v. SOFTWARE PACKAGE ACQUISITION

	Rating factor	Weight	Score	Assigned score
1.	**Scope of the system**	**5**		25
	Part of a department			
	Complete department		1	
	Multidepartment		2	
	Organisationwide		3	
	Organisation and external		4	
			5	
2.	**Financial exposure (AED) associated with the system**	**5**		25
	None		1	
	Small (<100,000)		2	
	Moderate (100,000—1 m)		3	
	High (1m—10 m)		4	
	Very high (>10 m)		5	
3.	**Nature of package**	**2**		10
	Off the shelf product		1	
	Custom built by vendor, maintained by vendor		2	
	Vendor developed, in-house maintained		3	
	Jointly developed, vendor maintained		4	
	Jointly developed, in-house maintained		5	
4.	**Type of evaluation**	**1**		5
	By the user department/IS/consultant		1	
	By IS/user		2	
	By consultant		3	
	By IS		4	
	By the user department		5	
5.	**Cost and complexity of the package**	**2**		10
	Negligible		1	
	Small		2	
	Moderate		3	
	Significant		4	
	Very high		5	
6.	**Evaluation methodology**	**3**		15
	Vendor/product evaluated		1	
	Only product evaluated		2	
	Only supplier evaluated		3	
	Not evaluated both purchased conditionally		4	
	Not evaluated purchased unconditionally		5	
7.	**Selection**	**1**		5
	Selected from many candidates		1	
	Selected from few reputed vendors		2	
	Selected from few known systems		3	
	Selected a familiar system		4	
	Selected an unfamiliar system		5	
8.	**Business effect**	**1**		5
	No immediate effect		1	
	Inconvenience to users		2	
	Loss of goodwill		3	
	Loss of revenue		4	
	Loss of business/goodwill/revenue		5	
	Total risk score		**100**	**100**

EXAMPLE IV—RISK ASSESSMENT—IS AUDIT
vi. OTHER IS FUNCTIONS

	Rating factor	Weight	Score	Assigned score
1.	**Effect of the function failure (criticality)**	**5**		25
	No immediate effect			
	Inconvenience to users		1	
	Loss of goodwill		2	
	Loss of revenue		3	
	Loss of business/revenue/goodwill		4	
			5	
2.	**Financial exposure (AED)**	**5**		25
	None		1	
	Small (<100,000)		2	
	Moderate (100,000—1 m)		3	
	High (1m—10 m)		4	
	Very high (>10 m)		5	
3.	**Scope of the function**	**2**		10
	Part of a department		1	
	Complete department		2	
	Multidepartments		3	
	Organisationwide		4	
	Organisation and external		5	
4.	**Age of the function**	**1**		5
	Over 10 years		1	
	7—10 years		2	
	4—6 years		3	
	1—3 years		4	
	Less than one year		5	
5.	**Prior audit findings**	**2**		10
	Recent audit—No weaknesses		1	
	Recent audit—Minor weaknesses		2	
	No previous audit		3	
	Audit—Some weaknesses		4	
	Audit—Many weaknesses		5	
6.	**Complexity of the function**	**3**		15
	Very low		1	
	Low		2	
	Moderate		3	
	High		4	
	Very high		5	
7.	**Number of staff**	**1**		5
	One		1	
	Less than 5		2	
	6—10		3	
	11—25		4	
	Above 25		5	
8.	**Number of locations**	**1**		5
	1		1	
	2		2	
	3		3	
	4		4	
	5+		5	
	Total risk score		**100**	**100**

15. EFFECTIVE DATE

This procedure is effective for all information systems audits beginning on or after 1 July 2002.

Digital Signature and Key Management Procedure P2

1. INTRODUCTION

1.1 The purpose of this procedure is to provide a tool to help evaluate a certification authority (CA), both in terms of quality of services offered and reliability.

1.2 The techniques of authentication play an essential role in electronic commerce, whether they are used to provide access to a corporate intranet, or to identify the communicating or transacting parties (private or commercial). Authentication of the parties to a transaction or communication is a method of building trust in electronic commerce, when appropriately carried out by reliable and secure technology infrastructures.

1.3 Authentication may be performed at various levels of security and by different technologies based on the party's requirements and the transaction or communication characteristics. For years, people have used passwords or similar methods of authentication, but today there are many more technological approaches to help facilitate this critical part of a communication. Today there are a variety of biometric and cryptographic key-based solutions used for authentication. They can be used as stand-alone systems, in combination or as part of a larger technological environment. Many organisations believe that public key infrastructure (PKI) based tools provide the most scalable solutions for commercially robust authentication systems.

2. TERMINOLOGY AND TECHNOLOGY NEUTRALITY

2.1 The term authentication refers to a large class of electronic applications whose functions may range from pure identification and authorisation to legal recognition.

2.2 Referring to specific authentication techniques, the terms electronic signature and digital signature are often used interchangeably. This has led to significant international confusion as to the use of the two terms. Digital signature is a functional subset of the more inclusive term electronic signature. Terminology used in this document shall refer to definitions with a certain level of international acceptance achieved through recognised international forums.

2.2.1 The term electronic signature has been defined by many authors as a signature in electronic form in, or attached to or logically associated with, a data message, and used by or on behalf of a person with the intent to identify that person and to indicate that person's approval of the contents of the data message.

2.2.2 Consequently, digital signature has been defined as a transformation of a message using an asymmetric cryptosystem such that a person having the signer's message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the signed message has been altered since the transformation was made.

2.3 The distinction between electronic and digital signatures has been at the core of international discussions on whether policies should focus on electronic signatures or digital signatures. The question is still open, and this procedure applies both to electronic signature and digital signature authentication techniques.

3. DIGITAL SIGNATURE AND KEY MANAGEMENT PROCEDURE

3.1 Verifying the security requirements for public-key security technology, involves a trusted third-party known as the certification authority (CA). The CA distributes the electronic keys used to encrypt and decrypt user and server information and the electronic certificates are used to authenticate users and servers.

General Aspect of a CA	Procedures and Perspectives	√
Organisational management	**Suggested procedure(s):** Determine whether or not the CA has effective organisation structures able to facilitate the effective management of information and systems. **Perspective:** The organisational element must be carefully considered when reviewing a CA.	
Certification/ accreditation	**Suggested procedure(s):** Determine whether or not the CA has received accreditation by appropriate international standard organisations for secure communications. **Perspective:** The certifications and accreditations the CA has received from approved international standards organisations will provide valuable information related to the quality of their products and services.	
Technology architecture	**Suggested procedure(s):** Identify the appropriate and applicable standards (i.e., support for X.509 certificate and X.500 directory) and determine whether or not the technology architecture is based upon those. **Perspective:** The technology architecture should be based on standards to provide assurance, scalability and interoperability.	
Operations management	**Suggested procedure(s):** Identify what services the CA offers, such as registering users, issuing keys, updating keys, backing up and recovering keys, revoking and reissuing keys, disabling and reenabling keys. Determine whether or not the services administration and operation of CA, and external services and outsourcing are adequate. Provide reasonable assurance of the availability of a redundant/back-up site and professional support. **Perspective:** Adequate operations management will provide reasonable assurance the practices for supporting operations are effective.	

The purpose of the above controls is to understand how the CA operates and for data and document collection. Specific topics are covered by the following checklist:

Digital Signature and Key Management Procedure P2 cont.

Specific Technical Aspect of a CA	Procedures and Perspective	√
Organisational management	**Suggested procedure(s):** Determine whether or not the training programme is effective and a continuous process. **Perspective:** One of the greatest security threats is the lack of knowledge. A structured training programme for managers and CA operators must be in place.	
	Suggested procedure(s): Determine whether or not the CA specifically complies with BS 7799 (ISO 17799) or other applicable standard for security organisation structure. **Perspective:** British Standard BS 7799 (now ISO 17799), formerly called *Code of Practice* is the reference for security organisations. Although it is not mandatory to obtain this certification, adherence with this standard provides reasonable assurance that policies and procedures are appropriately designed and functioning.	
Certification/ accreditation	**Suggested procedure(s):** Determine whether or not a formal security evaluation has been performed and a certification obtained. **Perspective:** Many countries require CAs to obtain security certification in accordance with the applicable standards (i.e., TCSEC, ITSEC) before they can compete in the marketplace. Even when it is not specifically required, CAs should consider applying for such certification.	
	Suggested procedure(s): Determine whether or not ISO 9000 quality certification has been obtained**.** **Perspective:** Some countries require the quality certification (usually ISO 9002) assigned to the CA. Such certification guarantees that the internal processes and procedures are designed and carried out according to a well-designed methodology, with the purpose of reducing the risk of exposure.	
	Suggested procedure(s): Determine whether or not the CA has a public operation manual to meet the requirements of legislation for accreditation of CAs. **Perspective:** Legislation requires the accreditation of CAs. To apply for accreditation, the CA publishes the operation manual that details the responsibilities and operations of the CA and controls the provision and use of the CAs services.	
	Suggested procedure(s): Determine whether or not the CA's security measures are certified by an independent third party through a formal risk analysis. **Perspective:** Periodic risk assessments by an independent third party validate the security of the CA's environment and operations. Often, this is a legal requirement, which prescribes CAs to obtain a formal security certification.	
Technology architecture	**Suggested procedure(s):** Provide reasonable assurance the CA's software complies with applicable international standards for privacy and security, and local requirements. **Perspective:** International standards for security define requirements not only for the entire security infrastructure, but also for products used to protect sensitive information. In some countries, local regulations require the adoption of specific approved packages or encryption algorithms.	
	Suggested procedure(s): Determine whether or not the CA supports separate key pairs for encryption and digital signatures. **Perspective:** A communication between parties can differ according to their needs. A message can be signed, encrypted or both signed and encrypted. This implies adopting a separate pair of keys for encryption and for a digital signature. This is often the only approved procedure for CA operation by local regulations.	
	Suggested procedure(s): Determine whether or not a standards-based directory service is available for providing public keys, certificates, and timely certificate revocation information. **Perspective:** To facilitate access to the public keys, a standards-based access method should be supported, such as the Lightweight Directory Access Protocol (LDAP). Sometimes, the LDAP structure and operation are subjected by specific requirements, in order to provide reasonable assurance interoperability.	
	Suggested procedure(s): Determine whether or not additional information is provided as part of the directory service; does it affect interoperability among CAs. **Perspective:** The standard directory service provides the public keys and certificates for valid users. A typical directory service ordinarily provides other information that users might find helpful. This additional information is not subjected to any regulation and it is made available based on organisation policy. It's important to provide reasonable assurance that the interoperability is not affected (i.e., a certificate issued by a specific CA should be able to be accepted and verified by any other CA legally enabled to issue certificates).	
	Suggested procedure(s): Determine whether or not X.509 current profiles are supported. **Perspective:** Today, the only recognised standard for certificate structure is ITU-X.509 v3. Other formats could affect CA interoperability. By supporting X.509 v3, a CA can provide more flexible services and greater support	
Technology architecture continued	**Suggested procedure(s):** Determine whether one CA can recognize or validate the certificates issued by another CA. Also review how cross certification has been tested to determine the actual compatibility of the CA and systems used. Consider if this has been used elsewhere in a live environment. **Perspective:** *Cross-certification,* or interoperability, is the ability of one CA to validate certificates issued by another CA. Obviously, cross-certification is possible by CAs that use the same technology, but IETF (Internet Engineering Task Force) working-group is currently defining common interfaces which will make it possible for CAs with differing technologies to cross-certify. Additionally, some country's requirements are in effect for cross-certification (i.e., encryption algorithms, certificate formats, certificates distribution policies).	
	Suggested procedure(s): Determine whether or not alternative standard based validation protocols (e.g. OCSP) are supported. **Perspective:** Other validation protocols are becoming a must-have for current PKI, e.g., Identrus requires OCSP. Other protocols are being designed (e.g., DPV—Delegated Path Validation**).**	

Specific Technical Aspect of a CA	Procedures and Perspective	√
Operations management	**Suggested procedure(s):** Determine whether or not there is an online backup so that the CA is always available. **Perspective:** Even if the CA server goes down, the organisation still needs a way to validate certificates and obtain public keys. A CA should provide for the continuous availability of these services.	
	Suggested procedure(s): Determine whether or not secure key backup and recovery is supported. **Perspective:** In the event that a user's key information is accidentally deleted or the user forgets their password, it should be always possible to recover the keys, if security is not compromised. This requires that the keys are backed up securely.	
	Suggested procedure(s): Determine whether or not the CA has an adequate disaster recovery plan. **Perspective:** Disaster recovery, together with effective backup procedures, provides reasonable assurance of continuity of operations in the event that the CA experiences a disruption to its primary operations.	
	Suggested procedure(s): Provide reasonable assurance that privacy issues are appropriately considered and adhere with local and international regulations. **Perspective:** CAs maintain and manage lists of names and personal data, sometimes very sensitive, such as, certificates delivered to hospitals or intended to protect communications and transactions between patients and doctors. Many countries have approved specific laws to protect individuals' privacy with technical regulations, which must be appropriately taken into account.	
	Suggested procedure(s): Determine if the local registration authority (LRA) model has been employed. **Perspective:** The LRA model states that the CA handles certificate administration and the organisation retains control over who is allowed to receive certificates. This makes the enterprise free from the administrative overhead while it maintains local control over security. Sometimes it's a legal requirement.	
	Suggested procedure(s): Determine whether or not there is centralised support for encryption key management. **Perspective:** Management of keys requires many functions: update, back up, recover, revoke, reissue, disable, and re-enable. These functions should be handled centrally, in order keep security under control. Central key management helps maintain system integrity.	
	Suggested procedure(s): Determine whether or not the CA provides complete and detailed policies and procedures. **Perspective:** Technology alone is not sufficient to provide reasonable assurance of security. Organisational controls—documentation of policies, procedures, standards and guidelines; technical education; security awareness; and management approval—are also extremely important.	
	Suggested procedure(s): Determine whether or not the CA operation is role-based. **Perspective:** Role-based operation increases security, which implies an effective separation of duties, reduces the potential for internal compromise. For example, the task of setting security policies should be handled by a different person from the one who administers keys and certificates.	
	Suggested procedure(s): Determine whether or not keys and certificates are obtained online, securely, and transparently, both for initial registration and for updates and accordingly with applicable legal requirements **Perspective:** Online support for key management provides for fast and simple registration. All online key management—registration requests, revocation, and the distribution of keys and certificates—should be fully encrypted and authenticated. Security is the main issue, consequently the CA must adopt any means to validate an applicant's identity according to law. Often the law states (or provides guidelines) on how the key distribution should be handled.	
	Suggested procedure(s): Determine whether or not key updates are forced—according to organisation policy—securely and transparently. **Perspective:** Risk can be reduced by setting policies that govern how often keys and certificates must be updated. These updates should be performed automatically by the CA, based on organisation policy and be transparent to the user.	
	Suggested procedure(s): Determine whether or not keys and certificates are time-stamped and archived so that digital signatures can be verified over the long term. **Perspective:** Many countries have established specific requirements for signed document storage, such as, financial records must be kept a minimum of ten years, for fraud investigation purpose. The CA should maintain a time-stamped history of keys and certificates to verify documents that have been signed and encrypted in the past.	
Operations management (continued)	**Suggested procedure(s):** Determine whether or not revocation is supported and how (i.e. support online and centralised, CRL v2). Determine the elapsed time from a certificate declared as revoked and its publication in the CRL. **Perspective:** Revocation security privileges for a user occurs for many reasons, such as, when the user leaves the organisation or the user's private key or certificate is suspected of being compromised. Revocation needs to be easy to perform and absolute. Centralisation can reduce the time involved in revoking the certificate. CAs perform revocation through the use of a *certification revocation list* (CRL). Administrators place certificates that are revoked on the CRL. No user whose certificate is on the CRL should be able to access secure resources. This is prescribed by local requirement in many countries and the CA should also support the CRL v2 (second version of the standard governing CRLs). Usually the revoked certificate should appear in the CRL within 24 hours.	
	Suggested procedure(s): Determine whether or not disabling and re-enabling is supported and if that support is centralised. **Perspective:** In some cases, there's a need to immediately suspend the use of a user's security credentials, such as when a security breach is suspected. *Disabling*, as compared to revocation, immediately prevents use of the security credentials (revocation takes place the first time a user or service checks the CRL after the certificate has been placed on the list).	

Specific Technical Aspect of a CA	Procedures and Perspective	√
	Suggested procedure(s): Determine whether or not the CA maintains audit records of security relevant events. **Perspective:** A secure audit trail reduces the risk of compromise and also helps to contain any damage that should happen due to a security breach.	

4. EFFECTIVE DATE

This procedure is effective for all information systems audits beginning on or after 1 July 2002.

REFERENCES

Public Key Infrastructure

- AICPA/CICA WebTrust Principles and Criteria for CAs
- Department of Energy Records Schedule (DOERS), *http://ardor.nara.gov/doe/index.html*
- *Digital Signatures Security & Control*, ISACF, 2002, Rolling Meadows, IL, USA
- DOE IT standards repository and program-related information, *http://cio.doe.gov* Select Standards Records Management General Records Schedules (GRS), *http://gopher.nara.gov:70/1/managers/federal/schedule*
- National Institute of Standards and Technology Computer Security Division, PKI Specifications to support the DOE Travel Manager Program, August 15, 1996, *http://cio.doe.gov* and select Computer Security Standards
- Telecommunications Security Manual, DOE M 200.1-1, chapter 9

Legal Considerations

- ABA-PKI Assessment Guidelines (currently only draft)
- American Bar Association Digital Signature Guidelines, *www.abanet.org/scitech/ec/isc/dsg.html*
- ANSI X9.79 and the AICPA/CICA WebTrust for Certification Authorities, *www.cpawebtrust.org/CertAuth_fin.htm*
- ESSI – Final report of the ESSI Expert Team
- EU Directive on the matter can be found at *http://europa.eu.int/eur-lex/en/lif/dat/1999/en_399L0093.html*
- IETF PKIX
- ITU X.509
- McBride, Baker & Coles, Summary of Electronic Commerce and Digital Signature Legislation, *www.mbc.com/ds_sum.html*
- PKI assessment guidelines of the American Bar Association. Available at *www.abanet.org/scitech/ec/isc*
- Software Industry Issues: Digital Signatures, *www.SoftwareIndustry.org/issues/1digsig.html#s1*

Applications

- Entrust ISVs, *www.entrust.com/* click on search and type ISV.
- Netscape home page, *www.netscape.com*.
- NIST Special Publication 800-2, Public Key Cryptography.
- NIST: Public key infrastructure program (as of July 1998), http://csrc.nist.gov/pki/.
- OMG home page, *www.omg.org*.
- S/MIME Editor. S/MIME message specification PKCS security services for MIME.

Intrusion Detection Systems (IDS) Review Procedure P3

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, “During the course of the audit, the IS auditorshould obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.”

1.2 Linkage to COBIT

1.2.1 The COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."

1.2.2 The COBIT *Management Guidelines* provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 The *Management Guidelines* provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

1.2.4 The *Management Guidelines* can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT’s information criteria.

1.2.6 Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

1.3 Need for Procedure

1.3.1 The purpose of this procedure is to provide the steps to be followed by IS auditors when reviewing an intrusion detection system (IDS).

1.3.2 This procedure is designed to provide the following:

- A definition of an IDS and how it functions
- The purpose and benefits of using an IDS
- The principal types of IDSs and the advantages and disadvantages of each
- Guidance on the conditions necessary to appropriately implement and administer an IDS
- Planning considerations when reviewing an IDS
- An overview of the audit approach
- Reporting issues
- Types of audit procedures and audit evidence

1.3.3 This procedure also defines IDS controls within the existing COBIT 3rd Edition, *Framework,* published in 2000 by the IT Governance Institute.

2. WHAT IS AN IDS?

2.1 Definition

2.1.1 Intrusion detection is the process of detecting unauthorised use of systems and networks through the use of specialised software and/or hardware. The primary purpose of an IDS is to provide the ability to view network and system activity in real time and to identify unauthorised activity. In addition, it can provide a nearly real-time automated response. IDS products also provide the ability to analyse today's activity in relation to past activity to identify larger trends and problems.

2.2 Purpose and Benefits of an IDS

2.2.1 The primary purpose of performing intrusion detection is to help prevent the consequences caused by undetected intrusions. Implementing a programme of effective security controls is an effective starting point for establishing the supporting security infrastructure. Effective controls grow out of effective information security policies, standards and practices and the use of appropriate technology. Appropriate technology is defined as technology that supports and enforces an organisation’s policy effectively. Being able to detect an intrusion attempt in real time is an important aspect of intrusion detection. Knowing when an attack is in progress and being able to take immediate action significantly improves the odds of successfully terminating intrusions and tracing intrusion attempts to their source. Real-time detection depends upon having a watchdog system that sits in the background and monitors all activities involving the connected devices. The monitoring system must be able to interpret various incidents and diagnose actual attacks.

Intrusion Detection Procedure P3 cont.

2.2.2 Most traditional IDSs take either a network- or a host-based approach toward identifying and protecting against attacks. In either case, IDSs look for attack signatures, specific patterns that ordinarily indicate malicious intent or suspicious activity. A truly effective IDS will employ both methods.

2.3 Principal Types of IDSs

2.3.1 The principal types of IDSs are:

- Host-based
- Network-based
  - Statistical anomaly
  - Pattern matching

2.4 Host-based IDS

2.4.1 Host-based intrusion detection started in the early 1980s before networks were as prevalent, complex and interconnected as they are today. In this simpler environment, it was common practice to review audit logs for suspicious activity. because intrusions were rare, after-the-fact analysis proved adequate to prevent future attacks.

2.4.2 Host-based IDSs still use audit logs, but they are much more automated, having evolved to include more sophisticated and responsive detection techniques. Host-based IDSs typically monitor systems, events and security logs. When any of these files change, the IDS compares the new log with attack signatures to determine if there are any matches. If so, the system responds with administrator alerts and other calls to action. It monitors files on systems for changes. The primary host-based IDS purpose is to monitor systems for individual file changes.

2.4.3. Host-based IDSs have expanded to include other technologies. One popular method of detecting intrusions checks key system files and executables via checksums at regular intervals looking for unexpected changes. The timeliness of response is directly related to the frequency of the polling interval. Finally, some products monitor port activity and alert administrators when specific ports are accessed. This type of detection brings an elementary level of network-based intrusion detection into the host-based environment.

2.4.4 Host-based IDSs are not as fast as their network counterparts, however, they do offer advantages that network-based systems cannot match. These advantages include stronger forensics analysis, close focus on host-specific event data and lower entry-level costs.

2.4.5 The advantages of host-based IDSs include:

- They verify success or failure of an attack. While Network-based IDSs provide an early warning, host-based IDSs provide verification of whether an attack was successful or not.
- They monitor specific system activities. Host-based IDSs can monitor all user activity while connected to the network. It is very difficult for a network-based system to provide this level of event detail.
- They detect attacks that are not identified by network-based systems. for example, attacks from a keyboard inside a network may not be detected by a network-based system.
- They are well-suited for encrypted and switched environments. Since host-based systems reside on various hosts throughout an enterprise, they can overcome some of the problems of network-based systems in switched and encrypted environments. Identifying where to specifically place the IDS on internal networks can be difficult when trying to provide broad coverage for the enterprise. By the time a host-based system reviews the traffic, the data stream has already been decrypted.
- They have nearly real-time detection and response. Many current host-based systems can receive an interrupt from the operating system when there is a new log file entry. This new entry can be processed immediately, significantly reducing the time between attack recognition and response.
- They do not require additional hardware. Host-based IDSs reside on existing network infrastructure, including file servers, web servers and other shared resources.
- They have a lower cost of entry. Network-based IDSs can offer broad coverage with little effort and they are often expensive. Host-based intrusion detection systems are often priced in the hundreds of dollars for a single agent and can be deployed by with limited initial funding.

2.4.6 The disadvantages of host-based IDSs include:

- Their capabilities are compromised as soon as the host machine is compromised.
- They add additional overhead to an operating system and require a copy for every protected machine on a network.
- They are frequently compared to antivirus tools, so users tend to use just the antivirus, where the IDS provides security features not found in an antivirus software.
- They are very application-specific.
- They must be able to translate between Windows NT, UNIX, VMS and other mainframe operating system languages. There are very few IDSs today that provide that level of translation. Since portions of these systems reside on the host that is being attacked, host-based IDSs may be attacked and disabled by a clever attacker.
- They are not well-suited for detecting network scans of all hosts in a network since the IDS at each host only sees the network packets that it specifically receives.
- They often have difficulty detecting and operating during denial-of-service attacks.
- They use the computing resources of the hosts they are monitoring.

Intrusion Detection Systems (IDS) Review Procedure P3 cont.

2.5 Network based IDSs

2.5.1 Network-based IDSs use raw network packets as the data source. Network-based IDSs typically utilise network adapters running in promiscuous mode to monitor and analyse network traffic in real time. Promiscuous mode makes it extremely difficult for an attacker to detect and locate. Attack recognition functionality uses two common techniques to recognise an attack signature:

- Statistical anomaly detection
- Pattern, expression or byte code matching

2.5.2 The advantages of network-based IDSs include:

- Their greatest asset is stealth.
- They can be deployed with no effect on existing systems or infrastructure.
- Most are operating system independent. Deployed network-based intrusion-detection sensors will listen for all attacks, regardless of the destination operating system type.

2.5.3 The disadvantages of network-based IDSs include:

- They are not very scaleable; they have struggled to maintain capacities of 100 Mbps.
- They are based on predefined attack signatures—signatures that will always be a step behind the latest underground exploits.
- IDS vendors have not caught up with all known attacks, and signature updates are not released nearly as frequently as antivirus updates.

2.6 Statistical Anomaly IDSs

2.6.1 In the anomaly detection model, the IDS detects intrusions by looking for activity that is different from a user's or system's normal behaviour. Anomaly-based IDSs establish baselines of normal behaviour by profiling particular users or network connections and then monitoring for activities that deviate from the baseline.

2.6.2 The advantages of statistical anomaly based IDSs include:

- Many security experts feel they are capable of detecting never-before-seen attacks, unlike pattern matching-based IDSs that rely on attack signature analysis of past attacks.
- They can detect unusual behaviour and thus have the capability to detect attacks without having to be specifically programmed to detect them.

2.6.3 The disadvantages of statistical anomaly-based IDSs include:

- Often produce a large number of false positives due to the unpredictable nature of users and networks.
- Anomaly-based detection approaches often require extensive training sets of system event records to characterise normal behaviour patterns.
- Careful hackers can evade or disable them.

2.7 Pattern-matching IDSs

2.7.1 The majority of commercial products are based upon examining traffic, looking for documented patterns of attack. This means that the IDS is programmed to identify each known exploit technique. This can be as simple as a pattern match. The classic example is to examine every packet on the network segment for a defined pattern of activity that indicates an attempt to access a vulnerable script on a web server. Some IDSs are built from large databases that contain thousands of such patterns. The IDS monitors every packet, looking for packets that contain one of these defined patterns.

2.7.2 The advantages of pattern matching IDSs include:

- They have a shorter implementation timeline than anomaly IDSs. However, there must be a pattern-matching engine running on the network that looks for events that fit the specific pattern definitions.
- They are easy to implement, deploy, update and understand.
- They produce fewer false positives as compared to anomaly IDS because they produce higher numbers of false negatives. In other words, it is easier to slip something past a pattern matching detection system, but they are fast.

2.7.3 The disadvantages of pattern matching IDSs include:

- Normal network traffic causes many false positives, but less relative to anomaly-based IDS.
- Careful hackers can evade or disable the IDS.
- They cannot detect anything for which they do not have a pattern.
- They require constant updating with new rules.
- They are easier, as compared to anomaly-based IDSs, to fool by sending fragmented packets across the network.
- The majority of pattern updates are provided by the vendor of the IDS, giving a role in network security to the vendor. The ability of the vendor to provide patterns for newly discovered attacks is a key in maintaining an effective pattern-matching IDS.

Intrusion Detection Systems (IDS) Review Procedure P3 cont.

3. PROCEDURES TO REVIEW IDS IMPLEMENTATION

	Suggested Procedures	✓
Planning the review	An integral part of planning is understanding the organisation's information system environment to a sufficient extent for the IS auditor to determine the size and complexity of the systems and the extent of the organisation's dependence on information systems. The IS auditor should gain an understanding of the organisation's mission and business objectives, the level and manner in which information technology and information systems are used to support the organisation, and the risks and exposures associated with the organisation's objectives and its information systems. Also, an understanding of the organisational structure including roles and responsibilities of key IT staff responsible for maintaining the IDS should be obtained.	
	Develop objectives to address the seven COBIT information criteria and have the organisation agree to them. The seven COBIT information criteria are: • Effectiveness • Efficiency • Confidentiality • Integrity • Availability • Compliance • Reliability of information	
Positioning of an IDS within the network architecture	Determine where the critical assets are placed throughout the network and at what point an organisation wants the detection to begin. For example, if an organisation wants to review the traffic outside its perimeter router, a sensor should be placed in front of the perimeter router. If there are concerns with traffic entering the network beyond the perimeter router and firewall and before critical servers, then sensors should be deployed at that point. Factors that must be taken into account when determining where to place an IDS include: • Is it desirable to have network traffic monitoring beginning inside or outside the network architecture? • Placing sensors on certain high-volume segments of a network could result in network latency. There could be a trade off between protection and production. • Multiple sensors may be required to monitor for different vulnerabilities and to help support load balancing. This provides reasonable assurance that packets being passed will be thoroughly inspected, enhancing intrusion detection capabilities. This concept is referred to as "defence in depth." • What servers/applications are at risk and what effect a denial-of-service (DOS) attack would have on the organisation? Sensors should be placed in these areas.	
Installation parameters	Determine whether the: • System is configured either to push data to or pull data from the analysis engine. Pushing data is the preferred method. Push can be configured to report attacks to the analysis engine as they occur. A disadvantage of the push method is that the sensor sends responses to attackers, which can aid attackers with identifying the sensor and launching additional attacks against the sensor. To mitigate this weakness, sensors can be configured to send data to the analysis engine even if an attack does not occur. For the pull method, the analysis engine obtains data from the sensors and waits to be queried. It is still capable of sending alerts in this mode, but queries need to be made to get details. • IDS is configured to recognise patterns and user behaviour. An IDS should be configured to differentiate between normal and abnormal network traffic. This also includes configuring the system to recognise/identify well known malicious signatures (i.e., worms, Trojans). For example, if the IDS identifies someone from outside the network with the same address space as someone inside the network, this should raise a red flag that someone is spoofing the network. • IDS provides a feature for remote management.	
	Evaluate IDS configuration parameters to scan for attacks. Certain parameters can crash a system or application, rendering a system unusable.	
	Provide reasonable assurance that: • The IDS is configured to identify suspicious files and database modifications or even unexplained files that have been added. • User accounts, system files and log files are monitored for tampering. The IDS is configured to send alerts when high-level intrusions occur and to minimise alerting resulting from false positives and low level attacks • The IDS operates based on attack signatures (misuse detection). • Alerts either by page, e-mail or other means can be sent. • A reporting module exists to aggregate attacks over a given period (i.e., hourly, weekly, monthly). • Filters are positioned based upon security policy to minimise false positives.	
Relationship to	Determine that the IDS does not require software to be installed on the firewall.	

	Suggested Procedures	✓
firewalls	Provide reasonable assurance that appropriate actions are taken when intrusion incidents are identified. Incident response procedures should be developed in conjunction with IDS implementation. The basic approach to responding to network attacks should include preparation, detection, containment, eradication, recovery and follow-up.	
Other important control issues	Determine whether: • Any employees connect to the network through unauthorised modem lines (referred to as rogue modems) • Any employees run unauthorised software posing a security threat, such as any remote control software, e.g., Back Orifice • Certain e-mail attachments containing malicious code are restricted, without hampering productivity • Personnel is abreast of URLs that may pose a security threat, as some web sites are configured to exploit a network as it browses these sites • Correct action is taken on incidents noted from IDS. For example, determine that disciplinary action is taken if employees are found snooping around the network and running hacker tools.	
Performance of audit work	Document the system flow process by gathering information including both the computerised and manual aspects of the system. The focus should be on the processing related to data flows that are of significance to the audit objective. The IS auditor may find, depending upon the processes and the use of technology, that documenting the transaction flow may not be practical. In that event, the IS auditor should prepare a high level diagram or narrative and/or utilise quality system documentation if provided.	
	Identify and test the IDS controls. Identify specific controls to mitigate risks and obtain sufficient audit evidence to determine that the controls are operating as intended. This can be accomplished through procedures such as: • Inquiry and observation • Review of documentation • Testing of IDS controls	
	Determine whether: • A third party provides information and assists in incident response • The system communicates with firewalls/routers and that this communication is secured, or is a separate channel/network required for secure communications (a parallel control network) • The IDS includes a tool for generating written reports that summarise the daily event log • Automated response mechanisms are available	

	Suggested Procedures	✓
	Provide reasonable assurance that: • Signatures are updated often. • Updates are distributed via a secure method (such as encrypted or digitally sealed). • The IDS can detect many different types of attacks. • The false-positives are managed based on the level of risk. • The IDS requires updates to its rules. • A specialised figure is in place for providing/updating IDS rules. • Information about the latest attacks is used to keep the IDS updated. • The IDS is effectively scalable (such as many sensors can be monitored/managed at a time). • The product has a low effect on network/host performance. • Other performance issues the IDS raises can be controlled. • The maximum bandwidth the system has been measured to analyse without loss, so that it provides 100 percent analysis coverage, is compatible with organisation needs. • The IDS analyses all network protocols in place if the organisation is network-based. • The IDS has the capability to analyse the upper level application protocols with sufficient detail. • The IDS does not require software to be installed on the host. • The communications between the sensor and the central manager are robust enough. • Alarm capture is reliable. If a high volume of alarms is generated, all of them are to be captured and put into a database. • Data obtained from the IDS are appropriately and effectively managed (i.e., data visualisation is a key issue). • A detailed procedure is in place explaining the actions to be taken when the IDS detects a problem. • The operating mechanism of the IDS is known by personnel. • The IDS can be used to accomplish other adjunct network management activity such as network device management. • The IDS is appropriate for deployment on the perimeter of the network as well as inside the network. • Product detects internally-generated abuse by authorised users over a long period of time. • The IDS is customised or configured to meet specific site policies and requirements. • List of people having access to the IDS is small and controlled. • Expertise and training are conducted to set up and maintain the IDS and analyse the results on a regular basis. • The IDS takes advantage of logs produced by other systems. • The IDS integrates with other vulnerability assessment products. • The IDS can respond reactively (communicate with firewalls/routers to block packets from a presumed attacker's IP net address). • The IDS reporting tools are efficient and accurate (lists of events, GUIs with icons representing events). • The methods for alerting the IDS operator/security manager are efficient and effective.	
Reporting	Report weakness to management. Weaknesses identified in the IDS review either due to an absence of controls or to noncompliance should be brought to the attention of management. Where weaknesses identified during the intrusion detection system review are considered to be significant or material, the appropriate level of management should be advised to undertake immediate corrective action.	
	Consider including in the report recommendations to strengthen controls.	

4. EFFECTIVE DATE

4.1 This procedure is effective for all information systems audits beginning on or after 1 August 2003. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary*.

APPENDIX

COBIT Reference

Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.

- PO6—Communicate Management Aims and Direction
- PO9—Assess Risks
- AI3—Acquire and Maintain Technology Infrastructure
- DS5—Ensure Systems Security
- DS7—Educate and Train Users
- DS10—Manage Problems and Incidents

The information criteria most relevant to an IDS audit are:

- Primarily: confidentiality, integrity and availability
- Secondarily: efficiency and reliability

Virus and Other Malicious Code Procedure P4

1. BACKGROUND

1.1 Introduction

1.1.1 An antivirus and malicious logic policy should form part of the global security policy of the organisation. It also should provide the framework for procedures on prevention, detection and correction of viruses.

1.2 Linkage to COBIT

1.2.1 The COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."

1.2.2 The COBIT *Management Guidelines* provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 The *Management Guidelines* provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

1.2.4 The *Management Guidelines* can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.

1.2.6 Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

2. PREVENTION, DETECTION AND CORRECTION OF VIRUSES AND OTHER MALICIOUIS LOGIC

2.1 The IS auditor should provide reasonable assurance that the organisation has effective documented procedures on the prevention, detection and correction of viruses. The checklist below should be used as a guide by the IS auditor.

Suggested Procedures for Preventing and Managing Virus Infection	√
Review management's analysis and assessment of critical resources and the types of protection to implement. The organisation antivirus policy should be based on an assessment of risk and vulnerabilities to best protect the organisation's information systems.	
Through discussions with IT, identify all possible types of inputs into computer systems, such as: • Physical media—diskettes, CD-ROMs and, more generally, any removable media • Peripherals to PCs—modems, devices connected via serial, USB or infrared ports (including PDAs or cell phones) • Remote connections from laptops operating outside the organisation • Network connections with identified third-party organisations such as customers, suppliers and administrations • The Internet protocols allowed by the organisation (HTTP, FTP and SMTP) Special attention should be paid to modems since users can use dial-up connections without the organisation being aware of it. For example, laptops, which are often enabled to access LANs and the Internet through an internal or external modem, might be vehicles for virus infection. Additionally, these modems can be used to allow users to access organisation assets in an uncontrolled manner. External vendors pose a serious threat if the policies at the third-party organisations are weak or nonexistent.	
Identify risks considering potential weaknesses of all layers of software installed on each platform, such as, operating systems, services (such as TCP/IP stack, mail checker), mail, web browser and other application software. Many types of code can be executed and trigger viruses (such as, when a service is started or activated).	
Based on the organisation's assessment of risk of virus exposure—often made as part of the organisation's overall risk analysis—examine selected hardware components and their related systems to determine which types of files and resources are allowed to run on the system, such as: • Harmful code loaded at system start-up on a bootable device • Executable file launched by the operating system • Code interpreted or run together with an application (such as DLLs, Java, Vba) • Script or macro A risk assessment should have been performed to determine what files and resources should be available for each system. The IS auditor should compare existing files and resources to the related hardware/software standard. The IS auditor should also review the standard against current best practices to identify whether any potential weaknesses may exist.	
Review the antivirus policy for end users, because different types of users may have different behaviours and different resources and methods available to perpetuate the virus. Viruses may be introduced by different categories of users: • The organisation's employees	

Suggested Procedures for Preventing and Managing Virus Infection	√
• Other staff working in the organisation (such as, consultants, contractors, temps) • People from outside of the organisation, including customers, vendors and other third parties The results of this analysis will be helpful in reviewing the organisation's policy to determine if it is appropriate and addresses all risks associated with the users of the organisation's systems.	
Review the network architecture of the organisation to determine the paths viruses can use to spread: • LANs are the most common ways for virus to propagate within the organisation. • Servers may store and spread viruses, such as, through a mailing application. • E-mail, web mail, downloads, unpatched operating systems, employees or contractors bringing in infected diskettes • Use of e-mail/firewall technology to block specific file types or attachments known to contain malicious code This evaluation will help in reviewing the antivirus architecture to identify key points where viruses can be scanned. A program should be in place to communicate the policy to end users and to build end-user awareness.	
Review the antivirus policy measures aimed at avoiding virus infection. This consists mainly of organisational procedures and communication within the organisation.	
Review rewrite access and execution rights, as well as the operating system and key application configuration on users' workstations. The policy should mention how users may enter data into the system or run code on their machines. For example, depending on the user's needs: • Removable media may be disabled • Downloading some types of files from the Internet may be forbidden, either via e-mail or the web (for example, executables or Visual Basic files may be filtered) • Macros can be disabled or macros-free types of documents preferred (such as, RTF, CSV) • Viewers can be used instead of complete applications, if modification is not needed • Automatic e-mail virus detection and eradication In any case, write access and execution rights should be carefully set up and reviewed, as well as the operating system's configuration on users' workstations.	
Review organisation policies on unauthorised software to determine what restrictions exist on the use of unauthorised software and how those restrictions are enforced. While ideally users will not have the right to install software by themselves on their workstations, in most instances, this capability exists. As a result, the organisation should have methods to detect and assess the risk of unauthorised software being installed by employees.	
Assess the risk of staff members introducing malicious code for internally developed software. This may also be achieved by referring to existing procedures, including user acceptance testing on separate equipment before implementing in production.	
Review vendor information resources for security bug fixes. Procedures should ensure these patches are installed in a timely manner.	
Determine the backup strategy of the organisation. Since restoration of systems, application and/or data may be necessary due to a virus occurrence, the person in charge of the policy should ensure this strategy is sufficient to restart equipment without major losses of data after a virus outbreak. As most viruses cause a loss of data at the workstation level, it is important that users are made aware of policies and procedures surrounding the backup of data on workstations.	
Review policies to mitigate the risk of virus infection, i.e., preventive actions to avoid infection: • The types of documents or files that may prove harmful • The risks associated with e-mails • Reporting suspect behaviour of the systems in use Users take an important part of the prevention effort against viruses. One of their roles is to identify potential sources of infection.	
Review the organisation's assessment and mitigation of its risks if it propagates viruses to others. Clauses limiting an organisation's responsibility should be added at the end of outgoing e-mails and to the various contracts and agreements with entities with which the organisation shares data.	
Determine whether the antivirus software policy is clearly defined and applied. Although prevention is an important part of an antivirus policy, it is essential to be able to detect viruses efficiently as soon as they get into the systems.	
Evaluate antivirus software for the four levels where viruses may be checked: • User workstation resources, such as floppies, hard disk drives and removable media • File servers—incoming and outgoing files • Mail applications—attached files, which may include executable code • Internet gateways—incoming flow of data (SMTP, HTTP, FTP protocols) and active components (such as Java and ActiveX) The policy should describe which antivirus software is to be installed at each point identified during the threat analysis. For example, a computer accessing the Internet via an ISP should be protected locally to detect viruses before they spread.	
Perform standard technical analysis of the antivirus suppliers, and evaluate their malicious code procedures. Some issues to consider are: • How often definition updates are published • How fast special updates are delivered when a major outbreak occurs • By which means and how quickly the vendor communicates new threats • What administration tools are provided to help with deployment and updating • What assistance the vendor offers in case of an outbreak Depending on the threat analysis results and the complexity of the organisation, antivirus software from several vendors can be chosen. For example, installing one antivirus application on user workstations and another on mail servers may maximise the chances of detecting viruses, especially if these antiviruses use different technologies. Additionally, the	

Suggested Procedures for Preventing and Managing Virus Infection	√
organisation must manage the increased complexity of getting updates from multiple antivirus vendors.	
Determine whether the organisation has assessed the use of full scan technology versus the corresponding loss of performance. Verify if the organisation has performed such analysis and appropriately considered its result (if the loss of performance in doing a full scan is unacceptable, users tend to disable or circumvent the antivirus software in their systems, resulting in an increased exposure). The policy defines which type of scanning is to be applied depending on the resource considered and the threat evaluation. It should state how often or in which conditions on-demand checks should be triggered, as on-access scans are CPU-consuming. For example, the types of files to examine must be listed. Two types of scanning are ordinarily provided by antivirus software: • On-access, the antivirus monitors all data accessed in real time without any user intervention and should run permanently at least on file servers, mail servers and Internet resources • On-demand, the antivirus software must be launched to check a specific resource at a given time • Other scanning procedures should also be considered. For example, some organisations have one server that scans many others instead of loading virus protection software on multiple machines. This type of scan works in conjunction with "active" scanning.	
Review the organisation's procedures for the reporting of virus occurrences. This should include to whom in the organisation virus identification is reported (such as, help desk, antivirus taskforce), incident response procedures and event reporting. The occurrence of a virus within the organisation should be reported immediately and the organisation should have appropriate response procedures in place. These should include specifications as to what procedures should be followed, limits on who can disable or alter the configuration of antivirus software installed on user workstations, escalation and reporting procedures.	
Provide reasonable assurance that the frequency and scope of antivirus software updates are according to the recommendations of the antivirus software editor, organisation policy and the risk associated with each IT environment. Two types of updates are ordinarily available: • Engine updates, where the core of the antivirus software is changed • Virus definition updates, which are published when new viruses are discovered	
Provide reasonable assurance that virus definitions and antivirus engine updates, like any other software update, are tested on separate equipment before being implemented in a production environment. Some editors also publish emergency definition updates when a major outbreak occurs; a procedure must be set so management is immediately aware of these updates and can rapidly apply them (after appropriate testing is performed). Many antivirus software products come with automatic update features for both workstations and servers. This functionality should be taken into consideration, as manually performing updates can be a labour-intensive effort on large networked systems with multiple servers and workstations.	
Provide reasonable assurance that the status of the antivirus update is appropriately monitored by IT staff for completeness and accuracy: a single workstation not updated can constitute the starting point for a virus outbreak. In a LAN environment, the antivirus updates are always installed on servers by IT staff. Conversely, installation on clients/workstations is often delegated to users.	
Provide reasonable assurance that a policy exists to cover the use of tools, such as firewalls, in the antivirus strategy. Tools are not dedicated to dealing with viruses, but may help detect Trojan horses when they are activated. Other software products can detect suspect behaviour of mailing applications.	
Review existing procedures designed to halt the outbreak of a virus and to correct infected resources in case a virus is not detected and eradicated by the antivirus software (i.e., it may be necessary to shut down servers and/or disconnect physical connections to the network). These procedures should be triggered whenever a virus infection is suspected. The policy should detail the measures taken to stop the outbreak. Depending on the type of virus, some applications may have to be halted temporarily, such as, a mail application or a file server. Part of the organisation's network can also be isolated, if needed. The virus may either have entered the system because it bypassed detection paths or because its definition is not listed yet in the antivirus software databases. Therefore, the policy must specify the execution of on-demand checks after updating virus definitions. In case no virus can be located, the antivirus vendors can be sent suspected files for inspection.	
Provide reasonable assurance that a damage assessment is conducted to determine which parts of the systems were affected by an outbreak. Backups may be used to recover environments, programs and/or data. After checking that the antivirus software has been updated to deal with the new virus, the system can be restarted. Provide reasonable assurance that backup and restoration files are not infected with virus.	
Review the organisation's notification and alert process to assess whether other entities within the organisation are made aware of any outbreak, since they may have been infected as well. The policy should describe the way to deliver this information to the appropriate partners in a timely manner.	
Provide reasonable assurance that the antivirus policy is thoroughly documented, and procedures written to implement it at a more detailed level. Any procedure without proper documentation, is ineffective	
Provide reasonable assurance that policies and procedures are in effect for appropriate custody and retention of the documentation that support the formalised antivirus policy. Documentation should be retained to ensure proper follow-up.	
Provide reasonable assurance that users are trained in the procedures for an antivirus security policy, including testing of material learned. After successful testing has been completed, users should sign a document that describes their role within the policy. Users are to be informed about the antivirus security policy by such means as: • Employee meeting presentations • E-mail notifications • A security awareness web site	
Conduct an assessments on how the procedure is applied and its effectiveness on a recurring basis for each of the following areas: • Policy documentation	

Suggested Procedures for Preventing and Managing Virus Infection	√
• Threat analysis • Prevention of infections • Infection detection tools • Infection correction The results of policy assessments and the evolution of the organisation should be reviewed regularly and used to update the antivirus policy.	

3. TECHNIQUES TO ASSESS EFFECTIVENESS OF THE VIRUS AND OTHER MALICIOUS LOGIC POLICIES AND PROCEDURES

3.1 Suggested Techniques

Suggested Techniques to Assess the Effectiveness of the Virus and Other Malicious Logic Polices and Procedures	√
Evaluate use of proactive measures, including the maintenance of operating systems with all current patches and fixes; content filtering at gateways; enterprise-wide security awareness program, including reminders or follow-up programs; attachment stripping (such as .exe, .com, .vbs); use of "sandbox" methodology; restrict access to web-based e-mail sites at firewall or desktop level; and, block downloads from Internet, except for those that justify need.	
Obtain an understanding of the current network infrastructure (network architecture and design) by using network diagrams that document it.	
Determine if all types of desktops/PC, laptops, PDAs, file servers, e-mail gateways, Internet connection points, major types of software, remote locations, WAN, VAN and VPN connectivity platforms have been identified.	
Identify potential entry points where viruses could enter, including e-mail systems, downloads, infected diskettes, missing patches to operating systems and any lack of testing on standalone equipment of all software before it is installed on the network.	
Determine what virus scanning software is in place, how it determines if files are infected, and how it addresses these (such as, notification, fixes, quarantines) for each platform/environment (such as, firewall, UNIX, PC).	
Obtain and review all policies and procedures related to the malicious code, including, but not limited to the following: • Definition and dissemination • Awareness training for users, network and system administrators and help desk analysts on how to use software, avoid spreading of viruses, and procedures that must be taken when a virus is suspected. - Users are required to shut down PCs at least weekly, if antivirus software upgrade requires - Users cannot disable antivirus software on their desktop lementation of newly-acquired or new version of software lementation of software (system and application) patches and fixes ntenance of antivirus software is always current urity policies for system accounts (such as, administrator, guest) urity policies for all accounts/IDs (such as, length of passwords, periodic change of passwords, password history, iration period, lockout, password strength) and network configuration standards (possibly use of enterprise configuration management tool) lication standards ail standards ignment of responsibility to enforce these policies and procedures	
Evaluate vulnerabilities and security risks by performing specific tests, for example: • Select some network drives and run the antivirus detection software to see if any network servers have infected files. • Discuss with the NT administrator which services are running on the NT server, and the reason this is deemed appropriate. • Select sample of desktops/PCs (and laptops) and validate that the antivirus protection software is appropriately and adequately installed, and is the most current version (such as, check that the user cannot or has not disabled the virus protection software). • Determine if the virus signatures loaded are the most current version. • Select a sample of desktops/PCs (and laptops) and run the antivirus protection software to see if any PCs have infected files. • Query end users on knowledge of antivirus policy. • Obtain the third party antivirus policy and configuration, and evaluate for appropriateness.	
Determine accountability and timeliness to enforce any procedures that are in violation.	
Provide reasonable assurance that procedures to address an incident have been defined and are used.	
Review documentation of incidents reported during selected timeframe to verify that: • Appropriate managers were informed • Details were documented • Spread was minimised • Incident reports were communicated to other users • Viruses were eradicated • Incidents were investigated • Incidents were appropriately addressed • Preparations for reoccurrence were made • The network is monitored for unusual activity	
Review virus removal process, which should include the cutting off of Internet access, using scanners and detectors,	

Suggested Techniques to Assess the Effectiveness of the Virus and Other Malicious Logic Polices and Procedures	√
checking the start-up files, checking memory, looking for Trojan ports and deleting Trojan files and e-mail worms.	
Rights for all accounts/IDs should be reviewed for high-level privileges to provide reasonable assurance that these are limited to those whose job responsibilities require this level of access, if a data security audit has not been performed recently. Also, provide reasonable assurance that these require strong passwords, and other similar controls (i.e., access to powerful utilities is limited).	

4. REPORTING

4.1. Suspected infection

4.1.1. Each user is responsible for their own asset (computer and peripherals). When an infection due to malicious code is suspected the user should immediately stop computing and follow the emergency procedure provided by management and/or the security officer. In addition he/she should inform the appropriate parties (security department, help desk, etc.) about the problem in order to mitigate consequences and probability of malicious code propagation within the organization. If the user is not able to follow the procedure, he/she should immediately power off the computer and call the appropriate party (security department, help desk, etc.) for assistance.

5. EFFECTIVE DATE

5.1 This procedure is effective for all information systems audits beginning on or after 1 August 2003. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

APPENDIX

COBIT Reference

Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria:

- PO6—Communicate Management Aims and Direction
- PO9—Assess Risks
- AI3—Acquire and Maintain Technology Infrastructure
- AI6—Manage Changes
- DS4—Ensure Continuous Service
- DS5—Ensure Systems Security
- DS10—Manage Problems and Incidents

The information criteria most relevant to a viruses and other malicious logic audit are:

- Primarily: integrity and availability
- Secondarily: confidentiality and reliability

Control Risk Self-assessment Procedure P5

1. BACKGROUND

1.1 Linkage to ISACA Standards

1.1.1 Standard S5 Planning states, “The IS auditor should plan the information systems audit coverage to address the audit objectives and comply with applicable laws and professional auditing standards.”

1.1.2 Standard S6 Performance of Audit Work states, “During the course of the audit, the IS should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.”

1.1.3 Standard S7 Reporting states, “The IS auditor should provide a report, in an appropriate form, upon completion of the audit. The report should identify the organisation, the intended recipients and any restrictions on circulation. The audit report should state the scope, objectives, period of coverage and the nature, timing and extent of the audit work performed. The report should state the findings, conclusions and recommendations and any reservations, qualifications or limitations in scope that the IS auditor has with respect to the audit. The IS auditor should have sufficient and appropriate audit evidence to support the results reported. When issued, the IS auditor’s report should be signed, dated and distributed according to the terms of the audit charter or engagement letter.”

1.1.4 Standard S8 Follow-Up Activities states, “After the reporting of findings and recommendations, the IS auditor should request and evaluate relevant information to conclude whether appropriate action has been taken by management in a timely manner.”

1.1.5 Guideline G13 Use of Risk Assessment in Audit Planning provides guidance.

1.2 Linkage to COBIT

1.2.1 The COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."

1.2.2 The COBIT *Management Guidelines* provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 The *Management Guidelines* provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

1.2.4 The *Management Guidelines* can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT’s information criteria.

1.2.6 Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

1.3 Need for Procedure

1.3.1 This procedure is designed to provide the following:

- A definition of control risk self-assessment (CRSA)
- Guidance on the use of CRSA methodology
- Guidance on implementing CRSA

1. CRSA

1.1 Definition of CRSA

2.1.1 CRSA is an empowering method/process by which management and staff of all levels collectively identify and evaluate IS-related risks and controls under the guidance of a facilitator who could be an IS auditor. The IS auditor can utilise CRSA for gathering relevant information about risks and controls and to forge greater collaboration with management and staff. The terms control risk self-assessment and risk and control self-assessment can be used instead of CRSA. CRSA provides a framework and tools for management and employees to:

- Identify and prioritise their business objectives
- Assess and manage high risk areas of business processes
- Self-evaluate the adequacy of controls
- Develop risk treatment action plans
- Ensure that the identification, recognition and evaluation of business objectives and risks are consistent across all levels of the organisation

Control Risk Self-assessment Procedure P5 cont.

2.2 Objective

2.2.1 CRSA is a technique that adds value by increasing an operating unit's involvement in designing and maintaining control and risk systems as well as identifying risk exposures and determining corrective action. The CRSA process supports the following IS Auditing Standards: Planning, Performance of Audit Work and Reporting.

2.3 Involvement of the IS Auditor

2.3.1 The IS auditor's involvement in CRSA exercises can be significant and may involve sponsoring, designing, implementing and, in effect, managing the CRSA process, conducting CRSA training, supplying facilitators, orchestrating the participation of key management and staff, and scribing and reporting CRSA outcomes. In other CRSA exercises, the IS auditor's involvement may be minimal, serving as an interested party and consultant to the whole process and as an ultimate verifier of the evaluations produced by the teams. In most exercises, the IS auditor's involvement in CRSA exercises will be somewhere between these extremes.

2.3.2 Whatever the role of the IS auditor in the CRSA process, the IS auditor maintains professional independence and objectivity, in accordance with Standard S2 Independence and Guideline G12 Organisational Relationship and Independence. Ordinarily, the IS auditor acts as a facilitator, drawing on the functional expertise of line management and staff in identifying and assessing risks and developing action plans. The IS auditor contributes expertise in relation to the assessment, implementation and effectiveness of internal controls, just as he/she would in applying other auditing techniques. Line management remains responsible for the effective operation of internal controls and for considering and making decisions on the basis of advice received in the form of a CRSA report and proposed risk management action plan.

2.3.3 A CRSA exercise augments the traditional role of the IS auditor by assisting management in fulfilling its responsibilities to establish and maintain risk management and control processes and to evaluate the adequacy of that system. Through a CRSA exercise, the IS auditor and the business units and functions collaborate to produce better information about how well the control processes are working and how significant the residual risks are.

2.3.4 CRSA should not be seen as a substitute for more traditional auditing techniques, but rather should be considered as one tool within the overall IS assurance and audit framework, which includes CRSA, conventional IS audit techniques, reporting and follow-up activities.

2.3.5 Where a CRSA exercise has been conducted independently of the internal audit function, or the IS auditor has had minimal involvement, it is desirable for the IS auditor to review the CRSA outcomes, as a means of helping to validate the risk assessments and proposed action plans and also to help ensure the IS auditor remains up to date with the risk profile of the area or function concerned.

2.4 Benefits/Advantages of CRSA

2.4.1 CRSA aims to integrate risk management practices and culture into the way staff undertake their jobs, and business units achieve their objectives. The successful implementation of CRSA has a number of specific benefits:

- Directly involves the audit customer in risk assessment and control evaluation activities, and thereby assists in creating a partnership approach between the customer and the IS auditor
- Allows the IS auditor to better allocate scarce resources by involving the customer in the risk assessment and control evaluation process
- Educates management and employees in risk management and control evaluation
- Aligns business unit objectives with corporate goals
- Fosters a sense of ownership of risks and controls
- Builds teamwork in addressing risks
- Improves communication within business units and across the organisation
- Provides a mechanism for raising the awareness of management and staff with respect to the effect that soft controls such as organisational values, ethical standards competence and leadership styles can have on the overall health of the corporate control system

2.5 Limitations of CRSA

2.5.1 CRSA is not a technique to find fraud and may not be appropriate for regulatory audits that require testing of attributes and documentation of the attribute tested.

2.5.2 The particular style of management may mean that when issues are presented for discussion, participants may not be candid in terms of risk disclosure and may not trust each other and work effectively as a team.

2.5.2 CRSA works well in an organisational environment of devolved management and empowerment. It does not work well in an organisation that does not value innovation and collaboration.

2.5.3 Difficulties may be experienced in attempting to introduce new management practices, techniques or concepts to an organisation. The CRSA process involves initial and continuous investment and its cost/benefit ratio is not easy to determine.

2.5.4 Some of the major obstacles/restraints/pitfalls to the conducting of CRSA exercises are:

- Lack of top management support
- Selection of facilitators who lack skills and experience in facilitation, consensus oriented techniques, and knowledge of the theory and application of controls, or who do not adequately prepare for the CRSA workshop by familiarising themselves with the system under review
- Underestimation of the investment, learning or planning necessary to mount a successful workshop or series workshops
- Narrowing the focus and thereby limiting the potential of the CRSA exercise to be effective
-

- Starting off with a huge first project

2.6 Possible IS Areas Suitable for the CRSA Process

2.6.1 CRSA can be used in many areas that include system development projects, project development teams, data centre operations, system security for operating systems, networks, databases and application systems, help desk and call centres, telephone systems, business continuity and disaster preparedness, IS documentation, electronic data interchange, web server management, and IT governance.

2.6.2 CRSA can be used to identify and assess risks and controls in a target area or function and to develop a comprehensive risk management action plan.

2.6.3 Alternatively, or in addition to developing an action plan, CRSA can be used to highlight risk areas and issues that need additional testing. The additional testing can be carried out using traditional IS audit techniques, or it can be made the subject of follow up CRSA activity.

2.6.4 CRSA can be a valuable tool to assist in the planning of major projects, by providing early identification and evaluation of risks and development of risk management action plans.

2.7 Ownership of CRSA

2.7.1 The participants of CRSA are process owners, i.e., management and staff who are directly involved with or affected by the particular systems and issues under examination, who know them best and are critical to the implementation of appropriate process controls. CRSA highlights the fact that managers and staff at all levels of the organisation are responsible for effective and continuous risk management and internal control.

2.8 CRSA Approach

2.8.1 The primary forms of CRSA are facilitated workshops and structured questionnaires or surveys. Oganisations can combine more than one approach.

2.8.2 Frequently facilitated workshops are preferred and are a powerful means of obtaining excellent results in a short time.

2.8.3 The survey or questionnaire approach is often used if the desired respondents are too numerous or widely dispersed to be readily brought together for a workshop. They are also preferred if the culture of the organisation might hinder open, candid discussions in workshop settings or if management desires to minimise the initial time spent and cost incurred in gathering the information. Self-assessment questionnaires can be produced as an outcome of facilitated workshops, with the intention of using the questionnaires as a means of following up agreed workshop outcomes, or as a means for management to help maintain and monitor effective internal controls on a permanent basis.

2.9 Selecting Areas and Management Buy-in

2.9.1 CRSA can be implemented at different levels of an organisation. Strategically, senior management and the board can assess the risks and controls affecting the achievement of corporate objectives. Similarly, business units and functions within the organisation can identify risks and evaluate controls against their own objectives and outcomes. A guiding principle in selecting a business unit or function is that a set of objectives or results can be defined for the group concerned. This is important because there must be a common understanding and acceptance of what the group needs to achieve, against which risks and controls can be assessed and evaluated.

2.9.2 As with any major initiative, management buy-in and commitment is essential to CRSA's success. Senior management interest and involvement demonstrates the organisation's commitment to integrating risk management and control evaluation into the way the organisation does business at all levels. This commitment can be demonstrated through senior management issuing a policy or directive on the implementation of CRSA or briefing CRSA workshops in person.

2. CRSA WORKSHOP

3.1 Suggested Procedures

2.1.1 The purpose of CRSA is to give business units the knowledge, skills and support to assess and monitor their own risks. The process can assist the IS auditor in developing a strong control environment in organisation areas as well as encouraging a partnership approach to the management of risk. It enables the IS auditor to provide proactive and value-adding services in assisting business units to manage the achievement of their objectives and, consequently, meeting the organisation's goals.

Control Risk Self-assessment Procedure P5 cont.

	Suggested Procedures	√
Planning a CRSA workshop	Establish clear workshop objectives, and define the scope and the expected outcomes in conjunction with the organisation. Adequate planning is crucial in conducting a successful CRSA workshop. This enables the IS auditor to formulate an appropriate workshop strategy and plan. The approach taken by the workshop can use any of the following starting points, as the most suitable means of identifying system risks and controls. Each approach is intended to arrive at the same outcomes and none is inherently preferable. ■ Business objectives—Focuses on the best way to accomplish a business objective. The workshop ordinarily identifies business objectives and then identifies the controls presently in place to help achieve the objective and then assesses the residual risks that might mitigate against achievement of the objectives ■ Business risks—Focuses in the first instance on identifying all risks that impinge on the business or system, often with reference to a generic checklist of risks or risk categories. Having listed all possible obstacles, threats or exposures, the workshop examines the existing control procedures to determine if they are sufficient to manage the key risks. Risks that are not sufficiently mitigated are escalated upwards. ■ Internal controls—Focuses initially on identifying current controls and then assessing how well they are working to mitigate risk and promote the achievement of the business objectives. The workshop produces an analysis gap between how controls are working and how well management expects these controls to work. ■ Business processes—The workshop starts by examining key processes and assessing whether each process or subprocess is producing appropriate results. Where results are considered to be unacceptable or inadequate, then the controls are analysed to identify causes.	
	Estimate the completion date of the workshop and the reporting schedule.	
	Obtain and review information about the scope and the issues to be resolved in the workshop. The IS auditor should become familiar with the processes, activities, risks, controls and areas of emphasis in the workshop. This may involve obtaining relevant policies, plans, laws, regulations and contracts, organisational information, financial information, previous audit results, industry best practices, details of problems affecting the area and, where possible, details of challenges and opportunities expected to arise in the future.	
	Decide how, when and to whom workshop results will be communicated.	
Selecting participants	Select key process owners and staff involved in the process to participate in the workshop. Based on the workshop objectives and scope, and the preliminary information gathered, the IS auditor should identify the business units or functions that should participate in the workshop. Depending on the knowledge of the people within the organisation, the IS auditor can suggest specific participants in the workshop.	
	It is often desirable to include other key stakeholders in the workshop, such as key customers and suppliers to the business unit or process.	
Workshop preparation	Communicate to appropriate levels of management the information on participating business unit/function and participating personnel. The IS auditor should provide reasonable assurance that the participants and the appropriate management levels understand the CRSA process and recognise, and are committed to, the potential benefits and value of the process.	
	Determine any risk assessment or voting technology that will be used, and define the mechanism to resolve any conflict or disagreement and the approach that will be employed to follow-up CRSA outcomes.	
	Arrange accommodation for the workshop, and obtain tools and technology.	
Workshop tools	Determine how evaluations, decisions and planned actions developed during the workshop are to be recorded and monitored. The recording and monitoring tools can be as simple as paper-based documents and reports, or can involve the use of risk management software. Risk management software can provide for easy interrogation, can hold significant amounts of information and can be used to help consolidate relevant risk information from across the organisation. It also facilitates issues being tracked and monitored as action plans are implemented. As with any software it has costs, which include the license fees for its use and the potential for the functionality of off-the-shelf software to be an imperfect match to business requirements. Voting technology can be used with risk management software or separately. Anonymous voting techniques can be used to facilitate the free flow of information and viewpoints during workshops and to aid in negotiating differences between viewpoints and interest groups.	
	Decide on a common language, i.e., dictionary, glossary of risk terms, that gives business units a common understanding.	
	Provide risk checklists, i.e., assessment criteria, indicators, for the identification of new risks or the reassessment of existing risks. These checklists may provide examples of situations and events where business unit risk profiles may need to be revisited and updated.	

	Suggested Procedures	√
Facilitated workshop using the process-based approach—A facilitated workshop is an effective means to introduce business units to CRSA, conduct initial risk assessments and control evaluations, and transfer the tools and skills to be integrated into business practices. A suggested format for a workshop using the process-based approach is outlined.	Achieve a common understanding and agreement about what objectives and results need to be achieved. The business objectives or results for the business unit form the context against which risk is assessed and controls evaluated. Part of this process is also linking the business unit objectives to corporate objectives. This provides the strategic context for the business unit and raises staff awareness of how they contribute to the organisation's success.	
	Prioritise business unit objectives to help focus workshop discussion on the most significant risks and controls and provide the strategic context for the evaluation of risks. For example, refer to the Australian Standard on Risk Management (AS/NZS 4360).	
	Identify and assess risks against the key business objectives. This includes assessing the likelihood and consequence measures and an overall risk rating for each risk. The risk rating can be used to prioritise the risks of most significance. To facilitate this process, it is useful to use a generic checklist of sources of risk as a stimulus to identify what risks may effect specific business objectives. These sources range from economic circumstances to management activities and control. Examples of effects include the asset and resource base, revenue and entitlements, people, and timing and scheduling of activities. Risks associated with an IS project are listed in appendix 1. Definitions of likelihood, consequence and risk ratings need to be agreed by the group.	
	Examine the current control framework for each of the risks identified. A useful tool in completing this process is a control model. These models outline the different types of controls available to address risk, such as compliance controls, oversight controls or planning controls. The workshop group can review each of these types in turn and evaluate whether they exist and are effective in addressing risk	
	Assess the remaining levels of risk after existing controls are applied. They also must identify appropriate risk owners who have responsibility for managing specific risks. The risk owners are responsible and accountable for determining whether the level of residual risk is acceptable, or whether additional risk treatments are required.	
	Develop treatment strategies and timelines to address the risk where the level of risk is not acceptable. The risk owner has responsibility for the action plans developed.	
Validating workshop results	Examine and assess information from the CRSA workshop as to whether it is valid and legitimate. The extent to which the IS auditor needs to independently validate controls is based on the level of the residual risk, the importance of the issue, the consistency of the testimonies from one participant to the other and any other supporting information from the workshop, as well as the IS auditor's professional judgment. The IS auditor should give particular consideration to validating controls where the workshop has converted high-level inherent risks to low-level residual risks	
	Validation also may include using follow-up questionnaires/surveys and gathering audit evidence. The IS auditor should discuss, with the appropriate management level, his evaluation of the soft controls to get any valuable feedback to better accomplish business objectives.	
Workshop reporting	Each CRSA exercise should produce a report. In general, the substance of the report will be created during the deliberations, by way of a listing and description of relevant risks, control weaknesses and remedial actions proposed. A group consensus will be recorded for the various issues discussed and the group will review the proposed final report before the end of the session.	
	One of the outputs of the CRSA workshop will be a remedial action plan, the format of which will depend on users' requirements. The IS auditor should also issue a formal report on the CRSA process and outcomes, including relevant background, context, risk ratings and other material in accordance with ISACA IS Auditing Standard S7 Reporting.	
Ongoing monitoring	An important part of CRSA is that business units or process owners must revisit their risk assessments regularly and monitor the implementation of action plans. The tools provided for CRSA can act as support in achieving this. Follow-up workshops also can be considered, as should network meetings with business unit representatives to discuss risk management issues and concerns.	
	Monitor the implementation of the agreed actions, in accordance with normal audit and assurance practice and ISACA IS Auditing Standard S8 Follow-Up Activities.	

4. EFFECTIVE DATE

4.1 This procedure is effective for all information systems audits beginning on or after 1 August 2003. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

APPENDIX

CobiT Reference

Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT's information criteria.

Control Risk Self-assessment Procedure P5 cont.

COBIT provides a detailed set of controls and control techniques for the information systems management environment. Under the Monitoring domain, COBIT has a high-level control objective—"Assess Internal Control Adequacy (M2)" –that has a number of detailed control objectives, such as Internal Control Monitoring, Timely Operation of Internal Controls and Internal Control Reporting, underlying it. The achievement of each of these detailed control objectives could be assisted by the use of control risk self-assessment techniques. Control risk self-assessment techniques can be used both to assess the extent to which an area or function is meeting these detailed control objectives and also to help the area or function to improve its performance in meeting the objectives.

Under the Planning & Organisation domain, COBIT has a high-level control objective—"Assess Risks (PO9)"—that has a number of detailed control objectives, such as Risk Identification, Risk Measurement, and Risk Action Plan, underlying it. Also, the achievement of each of these detailed control objectives could be assisted by the use of control risk self-assessment techniques. Control risk self-assessment techniques can be used to identify and assess inherent and residual risks in an area or function and to help develop an action plan for the effective management of these risks.

Example of Risks Associated With an IT Project

- **Business**
  - Project/system requirements not adequately defined
  - Changes to Project/system requirements cannot be managed
  - Project outcomes do not satisfy business needs
  - Timing of project outcomes does not satisfy business needs
  - Required business changes are not managed

- **Contract**
  - Price changes
  - Contractor's resources not available as needed
  - Product or services do not meet expectations
  - Contractor fails
  - Contract conditions and terms not enforceable

- **External**
  - Emergence of new technologies
  - Failure of key technologies
  - Failure of essential services, such as telecommunications or power
  - Change or failure of supplier or other input provider
  - Organisation is taken over

- **Financial**
  - Funding becomes partially or totally unavailable
  - Project budget proves inaccurate
  - Significant input cost increases
  - Contract variations not managed
  - Project budget exceeded

- **Implementation**
  - Interdependent projects fail or are delayed
  - Poor project management methodology
  - Poor systems development methodology
  - Ineffective project reporting
  - Project not completed on time

- **Outcome**
  - Anticipated business benefits from the project are not realised
  - Poor systems documentation
  - Post-implementation problems and costs
  - Long term system maintenance problems and costs

- **Resource**
  - Skills inadequate to successfully complete implementation
  - Skilled resources unavailable
  - Skilled resources not retained
  - Hardware not available as required

- **Strategic**
  - Project outcomes prove to be inconsistent with corporate objectives and priorities
  - Change of corporate priorities or direction
  - Expansion of project scope

Control Risk Self-assessment Procedure P5 cont.

- **System Integration**
  - Platform not suitable
  - Associated existing systems, processes or hardware are not compatible with the project

- **Technology**
  - Project inputs do not perform as expected
  - Project outputs do not perform as expected

Firewalls Procedure P6

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, “IS audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met.”

1.1.2 Standard S6 Performance of Audit Work states, "During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

1.1.3 Guideline G25 Review of Virtual Private Networks Review provides guidance.

1.1.4 Procedure P3 Intrusion Detection Systems (IDS) Review provides guidance.

1.2 Linkage to COBIT

1.2.1 The COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."

1.2.2 The COBIT *Management Guidelines* provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 The *Management Guidelines* provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

1.2.4 The *Management Guidelines* can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT’s information criteria.

1.2.6 Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

1.3 Need for Procedure

1.3.1 Primarily intended for IS auditors—internal as well as external—this document can be used by other IS security professionals with responsibilities in firewall configuration.

1.3.2 Modern businesses are organised as a set of core processes operating within supply and demand networks. Almost every organisation in the world is faced with increasing pressure for effectiveness and efficiency (i.e., higher quality requirements for products and services, increased revenue, cost reduction, new product development), a pressure for better, faster and cheaper processes. These increasingly complex operating networks are supported by available communication technologies (mainly the Internet), allowing businesses to focus on their core competencies and partner with others to deliver enhanced value to customers.

1.3.3 The transformation of the old processes is enabled by new communication channels. These channels provide new linking possibilities among different systems and networks, making them available to more people and letting the entities and their processes interact, such as, e-procurement and e-sourcing.

1.3.4 These new processes have shown the necessity for new techniques to allow authorised access to an organisation’s data and programs and protect them from unauthorised (and mostly malicious) access through the new channels that interconnect the existing networks with external sources. In light of this, equipment has been developed with special kinds of functionality (firewalls) that help to minimise the previously mentioned risks.

1.3.5 There are various types of firewalls and they are used in several different configurations, each one suited for a specific protection need.

1.3.6 This document gives some guidance for IS auditors who are being increasingly faced with having to audit or review new processes that interconnect different entities through means such as the Internet, direct connections and leased networks, and thus evaluate the strength of the protection barriers to provide reasonable assurance of information integrity, availability and confidentiality.

2. FIREWALLS

2.1 Types of firewalls

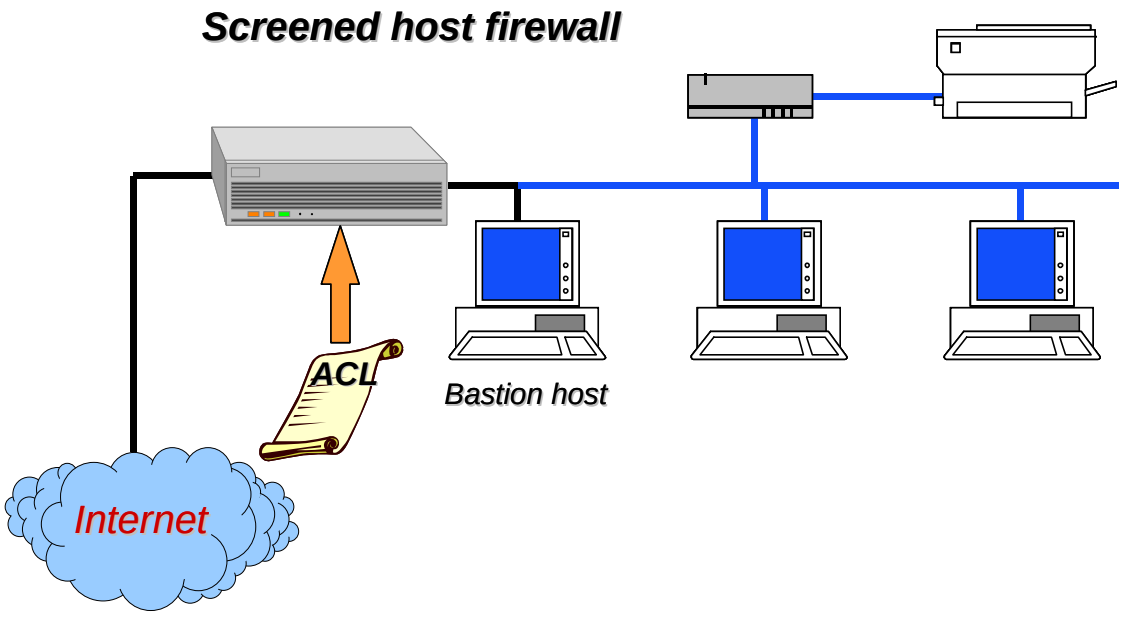
Note: OSI is an acronym for open standards interconnection.

OSI layer/ firewall type	7 Application	6 Presentation	5 Session	4 Transport	3 Network	2 Data Link	1 Physical
Routers used as a firewall							
Packet filter				(not always supported)			
Stateful inspection							
Hybrid firewall technologies							
Application-proxy gateway				(covered as a result of the functions on layer 7)			

2.1.1 Network layer firewalls generally make their decisions based on the source, on destination addresses and in individual IP packets. A simple router is the "traditional" network layer firewall, since it is not able to make particularly sophisticated decisions about what a packet is actually talking to or from where it actually came. Modern network layer firewalls have become increasingly sophisticated and now maintain internal information about the state of connections passing through them, the contents of some of the data streams, and so on. An important distinction about many network layer firewalls is that they route traffic directly through them, so to use one you either need to have a validly assigned IP address block or to use a "private Internet" address block. Network layer firewalls tend to be very fast and tend to be very transparent to users.

2.1.2 Screened host firewalls control access to and from a single host by means of a router operating at the network layer. The single host is typically a bastion host—a highly defended and secured strong-point that can resist attack.

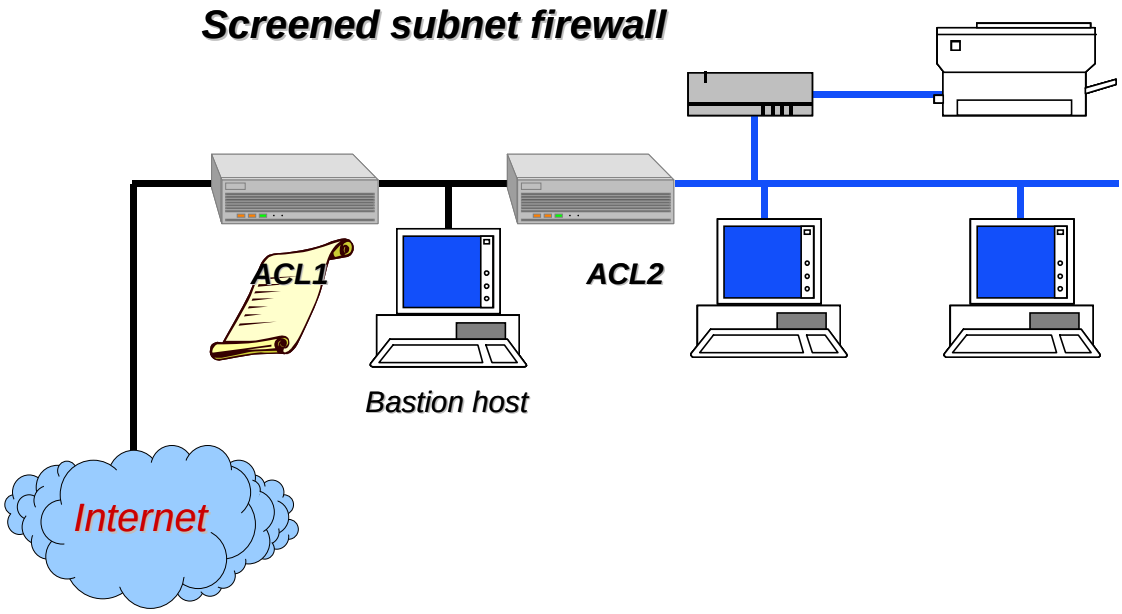
The Internet	Exterior Router	Bastion Host	Internal Network	Trusted Devices
traffic →	traffic → ←	traffic → ←	traffic → ←	traffic ←



Firewalls Procedure P6 cont.

2.1.3 Screened subnet firewalls control access to and from a whole network by means of a router operating at a network layer. It is similar to a screened host, except that it is, effectively, a network of screened hosts.

The Internet	Exterior Router	Bastion Host	Perimeter Network	Interior Router	Internal Network	Trusted Devices
traffic →	traffic → ←	traffic → ←		traffic → ←	traffic → ←	traffic ←



2.1.4 Packet filter firewalls (perimeter solutions) examine all the packets they see, then forward or drop them based on predefined rules. Packet filtering uses source/destination, protocol and port information from the packet header to restrict the flow of traffic. The packet filtering firewall is perhaps the most common and easiest to employ for small, uncomplicated sites. However, it suffers from a number of disadvantages and is less desirable than the other firewalls. Basically, a packet filtering router is installed at the Internet (or any subnet) gateway and then the packet filtering rules are configured in the router to block or filter protocols and addresses. The site systems ordinarily have direct access to the Internet while all or most access to site systems from the Internet is blocked. However, the router could allow selective access to systems and services, depending on the policy. Ordinarily, inherently dangerous services such as NIS, NFS, and X Windows are blocked. Packet filter firewalls can be found on TCP/IP based networks but also on other networks using layer 3 addressing (for example, IPX). Some routers also can provide some basic functions over layer 4, becoming a simple implementation of a stateful inspection firewall. As the filtering rules they use are very simple, they allow fast processing speeds, but at the same time, this feature makes them very susceptible to misconfiguration by defining a set of rules that does not comply with the organisation's security policy. As they do not examine higher layers of data, they are not suited to protect against attacks made using application function, nor can they protect effectively against spoofing attacks. They also have a limited logging capability. This type of firewall is used in environments that require high processing speeds, but no complex logging or authentication functions. This functionality can be included as the only firewalling feature (for example in a router) or may be one among others that operate at higher layers.

The Internet	Firewall	Internal Network	Trusted Devices
traffic →	traffic → ←	traffic → ←	traffic ←

2.1.5 Stateful inspection (or dynamic packet filtering) is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection examines not just the header information but also the contents of the packet to determine more about the packet than just information about its source and destination. It uses a combination of packet filtering, stateful inspection and proxy servers. SI/DPF uses state tables and programmed instructions to analyse information from the packet header and from the contents of the packet (application state), up through the application layer. The information is processed and stored to provide the firewall with a context for classifying traffic. The principal objective is to identify packets that are part of an established connection and to open and close specific ports for that traffic. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. These devices examine the packets, remember which connections use which port numbers, and shut down access to those ports after the connection closes. The expressions that define the filters have to be written under the vendor syntax. Stateful inspection/dynamic packet filtering is an extension of the firewall operating system that stores application state and packet header information in a table. That table is used to classify traffic and to apply different processing rules to established connections and to manage opening and closing specific ports.

2.1.6 Hybrid firewalls combine aspects of packet filtering and application-level filtering. Like packet filtering, these firewalls operate at the network layer of the OSI model, filtering all incoming packets based on source and destination IP addresses and port numbers, and determine whether the packets in a session are appropriate. They also can act like application-level firewalls in that they can review the contents of each packet up through the application layer. Ordinarily they employ some combination of security characteristics of both packet filtering and application filtering products. A hybrid firewall uses a combination of packet filtering, stateful inspection and proxy servers. The objective is to process different types of traffic according to the risk they present and to balance processing time against throughput. In a hybrid implementation, some hosts are behind a traditional firewall, while other hosts live on the outside. An IPSec gateway at the central site provides connectivity to the outside machines. This configuration is common at organisations with a major central site and some number of telecommuters. As in ordinary virtual private networks (VPNs), remote hosts have full access to the inside by virtue of the IPSec tunnel. Traffic from inside machines to the remote nodes is similarly protected. What is distinct is that traffic from remote nodes to the rest of the Internet is governed by the central site's security policy. That is, the firewall administrator distributes a security policy to the remote nodes. Ideally, of course, this same policy statement is used to control the traditional firewall, thus ensuring a consistent security policy.

2.1.7 Proxy server firewalls run special software written to allow specific programs to function and to enforce authentication, filtering and logging policies. For example, an HTTP proxy is written to specifically allow HTTP access, and only HTTP access, through it. It also requires special action to be taken at the user level. For example, in Netscape, the user must edit the properties dialog—specifically, go into "Advanced," then go into "Proxies," and make the appropriate entries there. As they have no firewall capabilities, they have to be placed behind a firewall. A user who needs to access external resources should use the proxy server that can enforce user authentication, log user activities and can scan, for example, web and e-mail contents. Additional supported functions are content scanning, service blocking, virus removal, etc. Proxy server firewalls typically act as an intermediary for user requests, they set up a second connection to the desired resource either at the application layer via application proxy or at the session or transport layer via circuit relay. They intercept all messages entering and leaving the network. The firewall only allows external systems to communicate with the proxy server. The proxy server effectively hides the true network addresses.

External Host	The Internet	Firewall	Dedicated Proxy Server	Internal Network	Trusted Devices
traffic →	traffic →	traffic → ←	traffic → ←	traffic → ←	traffic ←

Advantages of proxy server firewalls:

- The proxy ordinarily is highly aware of the data format it handles, and can look for many inconsistencies, and provide protection from them.
- Only specific protocols that are to be supported are allowed.

Disadvantages of proxy server firewalls:

- For any new protocol(s) that are allowed, a proxy that is specifically aware of that protocol is necessary.
- If an existing protocol is extended, proxy software will probably need to be updated.

Proxy server firewall provides a controlled network connection between internal and external systems. A virtual circuit exists between the internal client and the proxy server. Internet requests go through this circuit to the proxy server, and the proxy server delivers those requests to the Internet after changing the IP address. External users only see the IP address of the proxy server. Responses are then received by the proxy server and sent back through the circuit to the client. While traffic is allowed through, external systems never see the internal systems. This type of connection is often used to connect "trusted" internal users to the Internet. Used most often for outgoing connections that relay TCP connections and are transparent to the user. During a call, the gateway's relay programs copy bytes back and forth; the gateway acts as a wire.

Auto-connect capability, i.e., external hosts outside the gateway, need access to a printer on the inside. Restrictions on port designation and access control are implemented. Auto-connect assists with connection control, if a hole in the external host is created. Manual servicing is a protocol for the connection service that needs to be implemented to define the desired destination. Either a proxy (destination hostname) or SOCKS (IP address) is implemented. The logs store the bytes and TCP destination but do not examine them.

Firewalls Procedure P6 cont.

Advantages of auto-connect proxy firewall servers:

- More secure than a packet level gateway, although not as secure as an application gateway
- Replay TCP connections
- Permissions granted by port address
- Is capable of understanding the contents of the packet

Disadvantages of auto-connect proxy firewall servers:

- Inbound connections are inherently risky. They relay packets without inspection, have limited audit capabilities and no application specific controls
- No application-level checking

2.1.8 Transparent firewalls are amalgams of proxy server firewalls and network address translation (NAT) (see 4.1.1). An internal machine only has to know where to send packets to reach the outside, similar to a NAT firewall. However, the firewall may transparently invoke proxy-like mechanisms on certain traffic, for security purposes, rather than just blindly forwarding them through. The internal machines may or may not have a private IP address range.

Advantages of transparent firewalls:

- No special configuration on the client side, just like a NAT firewall
- Allows for finer control and protection for well-known services

Disadvantage of transparent firewalls:

- Shares most of the disadvantages of a NAT firewall. If a particular application protocol is being used on a non-standard port, all "special" protections are lost. Depending on the rules allowed, it may not even happen at all.

2.1.9 Application-level (gateway) firewalls have all the functionality of the dedicated proxy servers, plus the functionality of a firewall (i.e., each proxy application can access the firewall rule base to permit or deny packets). They are generally hosts running proxy servers, which permit no traffic directly between networks, and which perform elaborate logging and auditing of traffic passing through them, as they can inspect all the packets (destination address, ports and packet contents). They can implement enhanced authentication methods, as they can combine more information (they can consider additional information than packet filter and stateful inspection packet filter firewalls, that authenticate users based on the network layer address that it is easily spoofed). Since the proxy applications are software components running on the firewall, it is a good place to do lots of logging and access control. Application layer firewalls can be used as network address translators, since traffic goes in one side and out the other, after having passed through an application that effectively masks the origin of the initiating connection. Having an application in the way in some cases may effect performance and may make the firewall less transparent (in high-bandwidth applications a dedicated proxy server behind a firewall is often a preferred solution). An application-layer firewall, called a dual-homed gateway, is a highly secured host that runs the proxy software. It has two network interfaces, one on each network, and blocks all traffic passing through it.

The Internet	Firewall (Dual Homed Host)	Internal Network	Trusted Devices
traffic →	traffic → ←	traffic → ←	traffic ←

Advantages of application-level (gateway) firewalls:

- Easier to log and control all incoming and outgoing traffic
- Application layer firewalls can incorporate encryption to protect traffic transmissions

Disadvantages of application-level (gateway) firewalls:

- Administratively intensive—each networked service requires separate configuration (i.e., HTTP, telnet, mail, news)
- Inside users must use proxy-aware clients for most services
- Without further modifications to a service client, the user would have to connect to firewall. Modifications can be applied to make this connection transparent to the user

3. COMMON FUNCTIONS AND FEATURES RELATED TO FIREWALLS

3.1 Network Address Translation

3.1.1 NAT is a tool for "hiding" the network-addressing schema present behind a firewall environment. It allows a chosen addressing schema to be deployed behind a firewall, while still maintaining the ability to connect to external resources through the firewall. It also allows the mapping of nonroutable IP addresses to a smaller set of legal addresses. Network address translation can have three modes:

- Static NAT—Each internal system on the private network has a corresponding external, routable IP address associated with it. With this technique, it is possible to maintain the ability to provide selective access to external users (an external system could access an internal server and the firewall would perform mappings in either direction, outbound or inbound).
- Hiding NAT—All internal IP addresses are hidden behind a single IP address. The main weakness of this configuration is that it is not possible to make resources available to external users once they are placed behind a firewall, as mapping in reverse from outside systems to internal systems is not possible, so systems that must be accessible to external systems must not have their addresses mapped. In this type of implementation, the firewall must use its own external interface address as the substitute or translated address, impairing the flexibility of the configuration.
- Port address translation (PAT)—Similar to hiding network address translation, but with some differences. That is, it does not require use of the IP address of the external firewall interface, and the access to resources behind a firewall system can be granted selectively by forwarding inbound connections on certain port numbers to specific hosts.

3.1.2 Advantage of NAT:

- Requires no special configuration on the client side, except for normal routing configuration. Clients just have to know their default gateway.

3.1.3 Disadvantages of NAT:

- There is no additional security beyond selecting "allow this type of traffic." Once an internal client connects via an allowed protocol, anything can happen within the bounds of that protocol.
- There is no way to allow for special protocols that require a return connection to be made.

3.1.4 If certain types of protocols are to be restricted, access can be limited to certain ports. On the one hand, this is too restrictive, because internal users may not be able to access web servers on nonstandard ports. And at the same time, this is too permissive, because there may be a disallowed service running on a nonstandard port on the outside, and internal users will be able to access it in this case.

3.2 Intrusion Detection Systems (IDS)

4.2.1 These systems are designed to notify and prevent unauthorised access to a networked system or resource. Often they interact with firewalls to generate an automatic response against a perceived threat (e.g., blocking the source of the attack).

3.2.2 Attack recognition and response software works by continually monitoring network traffic and looking for known patterns of attack. When the software detects unauthorised activity, it responds automatically with some form of defined action configured by the administrator.

3.2.3 Requirements for a good intrusion detection system are:

- Installable throughout the overall network to ensure enterprisewide security
- Monitor incoming and outgoing traffic
- Provide protection for LANs, Internet, intranet and dial-up access
- Generate alarms in real time to appropriate personnel, such as administrators and security officers
- Configurable to automatically eliminate the intruder and block the intruder's reentry
- Selectively log session data
- Provide audit trails to help reconstruct the attack, for post-investigative analysis
- Can be administered remotely, and can encrypt the administration sessions for security purposes (if required by the client organisation)

3.2.4 Intrusion detection systems are not able to assist in:

- Compensating weaknesses in network protocols
- Analysing all the traffic on a busy network
- Dealing with some of the modern network hardware and related features
- Compensating for weak identification and authentication mechanism(s)
- Compensating for problems in the quality or integrity of information the system provides
- Conducting investigations of attacks without human intervention

3.2.5.1 The installation of an IDS should be made first by establishing the network perimeter and identifying all possible points of entry. Once identified, IDS sensors can be put in place, configured to report to a central management console. Possible placements are

suggested as follows:

- Between the network and extranet
- In the DMZ (demilitarised zone, see section 5.2) before the firewall to identify the attacks on servers in the DMZ
- Between the firewall and the network, to identify a threat in case of the firewall penetration
- In the remote access environment
- If possible between the servers and the user community, to identify the attacks from the inside
- On the intranet, FTP and database environments

3.2.6 Intrusion detection systems can be classified in two categories, host-based and network-based. The effectiveness of network-based intrusion detection is ordinarily greater than host-based intrusion detection, due to its ability to monitor multiple systems and resources. These types of systems ordinarily generate false attack identification, needing human intervention to determine the real attacks. Definitions of the two categories of IDS are as follows:

- Host-based intrusion detection—Highly integrated with the operating system, it should be installed on each individual computer system that is to be protected. There are some issues that arise from the use of this type of system:
  - They have a negative effect on system performance.
  - They do not provide effective detection over network-based (for example, denial of service).
  - They can affect system stability.

- Network-based intrusion detection—Analyses protocols, monitoring network traffic looking for specific strings that could indicate certain types of attacks. The issues that arise from the use of this type of systems are:
  - In most cases, they can not effectively detect signatures that are distributed among several packets.
  - They ordinarily require special equipment configurations (feature sometimes not supported) to establish promiscuous mode network interface.
  - They can be detected by identifying promiscuous mode network interface.
  - Sometimes it is difficult to predict the signature that identifies an attack.

3.3 Virtual Private Networks (VPN)

3.3.1 A virtual network is constructed in an encrypted or unencrypted form on top of existing network media, to establish secure network links across networks that are not trusted (for example the Internet). This technology can be used to provide secure remote access to corporate networks or link networks between different organisations. The most common protocols used are:

- IPSec
- PPTP (Microsoft Point-to-Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)

4. COMMON FIREWALL CONFIGURATIONS

4.1 Common Firewall Configurations Uses

4.1.1 Most common uses of firewalls are:

- Control access for internal and external networks (perimeter firewalls)
- Control access among public accessible and public inaccessible servers (DMZ firewalls)
- Control access among internal networks with different access and security requirements
- Control access thru pools of modems and private dial-up networks
- Control access to and from third party administered hosts and networks
- Encrypt internal and external networks that transmit sensitive data
- Hide internal network addresses from external networks (NAT)

4.2 Demilitarised Zone (DMZ)

4.2.1 A DMZ greatly increases the security of a network, protecting any computer that needs to be available from an external network behind one firewall and adding a layer of protection between the shared machine and the internal network. If appropriately configured, there are two protection layers for an attacker to compromise to get to anything valuable.

4.2.2 This type of configuration greatly increases the skills required by an external hacker to compromise the internal network and thus lowers the threat of the internal network being compromised. To further reduce risk, usage of different compatible technologies reduces the chances of exposure.

4.2.3 In a DMZ network, the untrusted host is brought “inside” the firewall, but placed on a network by itself (the firewall host then interconnects three networks). This increases the security, reliability, and availability of the untrusted host, but it does not increase the level of trust that other “inside” hosts can afford. Other untrustworthy hosts for other purposes, such as a public web site or FTP server, can easily be placed on the DMZ network, creating a public services network.

4.2.4 Sometimes a single firewall with three network interface cards is used to implement a DMZ. One of the cards is attached to the external network, the second to the internal network, and the third to the DMZ network. This configuration does not prevent against service degradation effectively during a denial-of-service attack.

The Internet	Firewall	DMZ (dual-homed) eth0/eth1 (SMTP/WWW/DNS, etc.)	Internal Network	Trusted Devices
traffic →	traffic → ←	traffic → ←	traffic → ←	traffic ←

4.2.5 Advantages and considerations of DMZs:

- Price of the hardware and software of the extra machines needed to implement a DMZ
- Slight decrease in performance
- Cost of the time to implement the DMZ
- Cost of down time the system suffers from adding on the DMZ
- Lowered level of accessibility to an attacker

4.3 DMZ with Dual Firewall Configuration

4.3.1 The organisation's internal network is further isolated from the untrustworthy network by adding a second firewall host. By connecting the untrustworthy network to one firewall host, the organisation's internal network to the other, and the DMZ between, traffic between the internal network and the Internet must traverse two firewalls and the DMZ.

4.3.2 In a more comprehensive definition, consider an Internet protocol (IP)-based infrastructure between an external network (the exterior) and an internal network (the interior). Such an infrastructure typically contains different types of machines: network devices (i.e., routers); systems (i.e., servers running applications, such as e-mail or a web service), and, of course, security appliances (i.e., firewalls). Each firewall interface is considered to represent a different segment of the infrastructure, which is called the DMZ network.

4.3.3 In each of these architectures, firewalls are used to control access at the border of the network mainly for the purpose of protecting the network from an untrusted network. Firewalls deployed entirely within the network can also be used to provide mutual protection among subnets of the network. Controlling access between internal subnets is no different than controlling access between a network and the Internet, so all of the above architectures can be used as internal firewall architectures as well.

4.3.4 In a multiple-layer architecture the firewall functions are distributed among a small number of hosts, typically connected in series, with DMZ networks between them. This approach is more difficult to design and operate, but can provide substantially greater security by diversifying the defences being implemented. Although more costly, it is prudent to use different technologies in each of these firewall hosts. This reduces the risk that the same implementation flaws or configuration errors may exist in every layer. This approach will reduce the chance of redundancy and greater possibility of compromise. The most common design approach for this type of architecture is an Internet firewall composed of two hosts interconnected with one DMZ network.

4.4 Proxy Server

4.4.1 Proxy servers are used in environments that require stronger authentication methods and good logging functions, as each proxy agent is able to require authentication of each individual network user. On the other side, these enhanced security capabilities require more processing power, and thus makes them unsuitable for environments with high-bandwidth requirements. A special agent for the traffic of each application is required on the firewall. They can analyse e-mail and web content by:

- Java applet, ActiveX control, JavaScript filtering
- Blocking some MIME types
- Virus, and macro virus scanning
- Application command blocking
- User-defined blocking functions

5. RISKS CONTROLLED BY FIREWALLS

5.1 Attacks Based on Software Weaknesses

5.1.1 The objective of this type of attack is to put the server on a virtual offline condition (denial of service attack, DoS), but unauthorised access could also occur.

5.1.2 Buffer overflow is probably one of the most effective types of attack. It is not associated with a particular application and it uses publicly known bugs or weaknesses of the software to generate an error condition in the program used to handle a service. The most common origin of the problem is when portions of memory used by the program are rewritten by an overflow condition. An example of an attack using this weakness is the one made by the virus Code Red.

5.1.3 Directory transversal attack is directed against web servers, trying to access the file systems outside the authorised pages. This can result in unauthorised access to data, or execution of unauthorised code. In some of the oldest versions of the software, using an URL in the form of http://server/../../ was enough. An example of an attack using this weakness is the one made by the virus NIMDA.

5.1.4 Source disclosure attack is directed against web servers that process dynamic pages. They try to access their source code that can include installation information, such as user IDs and passwords to access databases. This form of attack can be made issuing a special URL that the server processes incorrectly, or makes the server execute some software components that can contain errors or bugs.

5.1.5 MIME exploit attack is directed against mail clients and services and, in some cases, against browsers. The attack consists of the modification of headers to provoke certain situations, such as DOS, program executions. Some of the controls that can be in place are:

- Continuous follow-up of published bugs and weaknesses, and installation of patches and software updates
- Procedures to control system and application logs to detect attacks

5.2 Attacks Based on Processing Power

5.2.1 SYN floods are intended to generate an error in the program used to handle the service. In their simplest form, they overwrite memory used by data or program code and thus generate the error. In more dangerous forms, the attacks manage to execute program code provided by the attacker. As the services are ordinarily executed at a high level of privilege, these types of attacks are high risk. Ordinarily, packets include false origination addresses. SYN floods generate two basic problems—bandwidth shortage and growth of the connection table on the server. Controls that can be put in place against this type of attack (although they cannot have a total effectiveness) include:

- Configuring firewalls to detect and filter spoofed addresses
- Adjusting connection parameters, such as number of waiting connections and timeouts, to avoid excessive growth of connection table

UDP flooding is similar to the previous case. The main difference is that UDP does not use the concept of connections. The attack is based on the occupied bandwidth and, eventually, in the resources used by the server to answer the packets.

ICMP floods have been some of the most effective past attacks. They use the configuration problems to enhance the attacks. One of the most well-known applications, Smurf, is based on using other networks to attack the final target.

5.2.4 DdoS attacks intend to flood the target site with one or more attacks of DoS. It does not use software bugs or configuration errors. The attack ID is based on a massive use of bandwidth and requires that many previously affected nodes of the network (hundreds) participate in the attack. There are not so many options to prevent this type of attack. Some of the controls that can be in place are:

- Packet filtering
- Providing reasonable assurance that weaknesses of interconnected sites are as well controlled as they can be
- Adjusting parameters to control excessive connection table growth

6. PROCEDURES TO REVIEW FIREWALLS

	Suggested Procedures	√
Gather preliminary information—These are examples of information that can be obtained to plan the audit work.	Obtain security policies.	
	Obtain the firewall security policy.	
	Identify the services that the firewall is intended to protect and perform a high-level risk assessment of their sensitivity considering the seven information criteria defined by COBIT.	
	Identify the risk assessment process in place to identify the main sources of threats and the probability of their occurrence.	
	Develop an understanding of how the technology is being used, including the security measures in place, such as authentication methods, security administration and hardware maintenance.	
	Identify procedures used in the systems development life cycle, for the set of applications used from the outer network (those accessed directly and the ones they use thru interfaces) and for the system software of the firewall.	
	Determine the logging functionality in place.	
	Identify the procedures used for rule base maintenance.	
	Identify the procedures used to monitor new bugs or weaknesses of the software used.	
	Identify the procedures used to review systems and application logs to detect attacks.	
	Identify the procedures to share technical and security incident related information with neighbor sites.	
	Identify the configuration management procedures.	
Risk assessment	Adjust the scope of the review using the information on sensitivity of the services that the firewall is intended to protect, the identified risks, and the likelihood of their occurrence.	
Detailed planning— All the control objectives that can be identified as a result of selecting COBIT processes can be reviewed by usual installation reviews. This section includes some special procedures that can be included as a part of a firewall installation	For the IDS installation, review the analysis made to evaluate the existing network, the identification of entry points, the types of traffic allowed by firewalls, the analysis rules introduced, and the alarms and notification schema set.	
	Review each DMZ on an individual basis, while considering the others as a different network or computer as applicable. In this approach, the configuration and rules should be considered against all the types of traffic of the networks related to the DMZ.	
	Review the procedures used to monitor security-related sources of information (mainly web sites and specialised sources) and identify new types of attack, such as software bugs; consider verification of whether all available security patches have been applied.	
	Review the systems development life cycle controls in place over the code executed as part of the firewall software and the applications published to the outer side of the network, such as segregation of duties, initiation and testing.	
	Review the authentication controls used to control access from the outer network.	

	Suggested Procedures	√
review. These are examples of areas to include in the review.	Review the procedures used for device administration (including at least physical access and administrators passwords, for example, to reduce the risk of tampering the connections thru unauthorised access.	
	Review the procedures used to control remote access for administering network devices (by administrators or vendors).	
	Review the procedures to review the logs in an effective and timely manner and to deal with potential harmful traffic.	
	Review the procedures for dealing with potential or effective attacks.	
	Review the procedures for rule-base maintenance, such as reviewing access to maintenance functions, request procedures, new or modified rules testing, transfer to production and documentation. Determine if there is a formal and controlled process in place to request, review, approve and elevate firewall addition and changes into the production environment. Specifically: 1. Determine if the formal request includes the business purpose and sponsor, date it is requested and how long (in time duration) the rule will be needed. 2. Determine if the review is completed by technically competent individual who understands the risk associated with the rule. The reviewer should document the risk in relation to the protection of the entire information infrastructure. 3. Determine if the approval include both the head or supervisor of the firewall administrator and the appropriate business manager. The approval of the firewall rule request must be done formally. 4. Determine if the firewall rule is formally tested first in a test environment prior to elevation into the production processing environment. Where possible, test for outage of services (for example identifying unusual amounts of off-hours made by the unit where the change was requested).	
	Review risk management procedures.	
	Identify the existence of single points of failure.	
	Review virtual private network in place (see guidance on Virtual Private Networks from ISACA).	
	Review the plan for conducting penetration tests and the criteria for re-performing the tests when changes are made. Coverage of the risks identified by the tests.	
	Identify the filtering rules in place (to determine if they address all the issues included in the security policy and other applicable threats identified during the risk analysis). Verify that the overall firewall rule restrict access, unless specifically allowed by the rules.	
	Review the procedures to test revised rules prior to the transfer to production environment.	
	Review physical access controls to firewall and network equipment that connects it to the networks.	
	Review the procedures used to test new software and configure its security to accomplish defined security policies.	
	Review disaster recovery and contingency procedures. The existence of a fail-over device to back up the processing functions of the firewall should be considered (as its services ordinarily have high-availability requirements).	
	Review configuration management processes.	
Stateful inspection/ dynamic packet filtering (SI/DPF)	Document how SI/DPF will affect the controls provided by the other firewall when the SI/DPF is used as the border firewall and there is another firewall behind it.	
	Confirm that program change controls (specially testing controls) are applied to any API if APIs in SI/DPF are used (to execute code written by the organisation by the firewall operating system).	
	SI/DFP uses state tables and programmed instructions. It uses information from the packet header and from the contents of the packet, up through the application layer. The information is processed and stored to provide the firewall with a context for classifying traffic. The principal objective is to identify packets that are part of an established connection and to open and close specific ports for that traffic. Design and perform testing of traffic that will be affected by SI/DPF, to verify its proper functioning.	
	Examples of aspects to consider when reviewing filters—gateways, FTP sessions, X Windows, DNS, fixed addresses. Confirm that: • It only allows access to those addresses intended to be accessed from the outside • Does not allow use of unauthorised services, such as FTP and Telnet • Does not allow to access certain ports • Only allows packets that come from authorised sites from the outer network • Discard all source-routed traffic	
	Evaluate access control rules or other measures that are set up to drop packets representing undesirable communications such as denial of service attacks against the devices.	
	Confirm that there are rules in place to avoid IP spoofing.	
	Confirm that if NAT is used, only those packets that come from certain allowed IP addresses in the internal network are passed, and that incoming traffic is only allowed when a valid connection is established.	
0Packet filtering	When the router is used as the border firewall and there is another firewall behind it, document how it will affect the controls provided by the other firewall.	
	Obtain (or create) an understanding of how packet filtering is being used to filter the packets in terms of the use of source/destination, protocol, and port information from the packet header.	

	Suggested Procedures	√
	Assess the effect on controls and identify the key areas of risks created by the use of packet filtering. Confirm that: • It only allows access to those addresses intended to be accessed from the outside • Does not allow use of unauthorised services, such as ftp and telnet • Does not allow to access certain ports • Only allows packets that come from authorised sites from the outer network • Discard all source-routed traffic	
	Design and perform testing of traffic that will be affected by packet filtering.	
	Evaluate rules that are set up to drop packets representing undesirable communications such as denial of service attacks against the devices.	
	Confirm that there are rules in place to avoid IP spoofing.	
	Confirm that if NAT is used, routing to internal IP addresses cannot be made directly.	
Inherent risks of packet filtering	There is little or no logging capability, thus an administrator may not determine easily whether the router has been comprised or is under attack	
	Packet filtering rules are often difficult to test thoroughly, which may leave a site open to untested vulnerabilities.	
	If complex filtering rules are required, the filtering rules may become unmanageable.	
	Each host directly accessible from the Internet will require its own copy of advanced authentication measures.	
Hybrid firewalls	Document how the use of the hybrid firewall will affect the controls over network traffic.	
	Obtain (or create) an understanding of how the three firewall approaches are being used (packet filtering, stateful inspection and proxy servers). Determine the logic for passing traffic into each of the firewall's processes.	
	Assess the effect on controls and identify the key areas of risks created by the use of a hybrid approach. Assess the decision logic applied to determine which firewall approach will be applied to each type of traffic.	
	Design and perform testing of traffic that will be affected by SI/DPF, considering the following rules: • Confirm there is consistency in sending similar protocols to the same process within the hybrid. • Confirm that any API's used in stateful inspection are controlled. • Confirm the proxy process is maintaining the separation between the traffic and the application. • Confirm the balance between throughput and control processing is appropriate.	
	Evaluate access control rules or other measures that are set up to drop packets representing undesirable communications such as denial of service attacks against the devices.	
Proxy firewalls	The proxy firewall could be a separate device, or a service running on a multipurpose firewall device. Its purpose is to add special processing controls to one type of traffic.	
	Obtain (or create) an understanding of the use of the proxy—which traffic is being sent through the proxy and which devices are receiving the output.	
	Confirm that all traffic of the type being processed by the proxy must flow through the proxy firewall. For all devices on the inside of the proxy, confirm traffic of the type being proxied is only accepted from the proxy device address.	
	Design and perform testing of traffic that will be affected by the proxy, considering the following: • Confirm all traffic is directed to the proxy • Confirm that all traffic of the type being proxied is only processed from the address of the proxy.	
	Evaluate the procedures for the review of logs from the proxy and the effectiveness of procedures to address potential problems identified from the logs.	
DMZ—Consider a DMZ network with three segments: one embodies the connection to the exterior, one embodies the connection to the interior, and one, the DMZ segment**,** consists of the IP subnet on which reside systems that can be accessed from the exterior.	Verify the firewall is invisible to the exterior.	
	Verify systems on the DMZ segment are invisible to the exterior.	
	If external service providers can troubleshoot devices at the edge of the DMZ network where connectivity with the service providers (and with the exterior in general) is made, confirm that: • Tests have identified the precise extent to which what is in the DMZ network may be mapped and • The potential exploitation effect is understood.	
	Review the DMZ network to provide reasonable assurance that external entities cannot administer or configure: • The firewall • Network devices and systems in the DMZ Network (If network devices on the external facing segment, such as routers that connect with service providers, can be accessed for any reason, such as troubleshooting, verify controls exist over who can administer/configure these devices.)	
	Verify access control rules are set up in network devices on the external facing segment for the purpose of denying packets that represent undesirable communications, such as denial-of-service attacks.	
	Review firewall rules to verify every packet is by default denied unless a specific rule exists to permit the packet to proceed but only to a destination system in the DMZ segment.	

	Suggested Procedures	√
	Confirm systems on the DMZ segment are set up so they cannot communicate with any other system outside the DMZ segment except through the firewall. If exceptions exist, evaluate the specific risks, the justification, and the compensating controls.	
	Confirm systems on the DMZ segment are set up so that they cannot initiate communications with the interior. Again, if exceptions exist, evaluate the specific risks, justification and compensating controls.	
	Confirm network devices, firewalls and systems on the DMZ network are configured so that routing between any possible combination of devices, firewalls and systems is well defined: • All routes into, through and out of the DMZ network are easily identifiable. • The routing set up is the minimum needed to support authorised communications flows. (If nonroutable communications protocols are used, confirm they have a purpose consistent with security policy requirements for the DMZ network.)	
	If NAT is used, provide reasonable assurance it works in a manner consistent with security policy requirements and that the configuration is periodically recertified by accountable individuals.	
	Confirm the firewall is set up: • To deny all packets entering from the exterior with source IP addresses set up for internal networks. • To deny all packets coming from the interior with source IP addresses not set up for the interior.	
	Confirm firewall rules discover external attempts to scan for commonly scanned ports (regardless of whether systems actually exist to listen on such ports).	
	Confirm the firewall is set up so that no message is returned in reply to any incoming packet that is denied.	
	Confirm the firewall has been tested by scanning every segment, including the DMZ segment, from every other segment to identify what packets can and cannot get through. Provide reasonable assurance the results are consistent with the overall security policy.	
	Confirm every rule in the firewall is consistent with the security policy. That is, provide reasonable assurance of consistency with policy is verifiable by examining the following components of potentially acceptable packets: protocol, source system IP address, destination system IP address, source port and destination port. For example, the destination system and port combination in a rule should make sense when the function of the destination system on the DMZ segment is considered. A rule should protect the firewall itself; should align with the functions provided by the systems on the DMZ segment; and should permit systems on internal networks to initiate communications with systems on the DMZ segment or allow systems on the DMZ segment respond to communications initiated from the interior. If the rule base has too many rules to be reviewed during the test, it may be an indicator of a poor security architecture design, making it very difficult to administer and to ensure proper coverage.	
	Confirm the rules in the firewall deny all packets that include TCP or UDP ports above port 1023 to provide reasonable assurance the application ports are being used as intended. If not, evaluate the specific risks, justification and compensating controls.	
	If multiple physical firewalls exist in the DMZ network for high-availability, redundancy or failover purposes, confirm the running configurations of the firewalls are equivalent.	
Additional key points to consider		
Configuration	DNS, e-mail, server load balancing services, or any software or services not related to firewall-specific functions should not be installed in or processed by the firewall.	
	Firewalls should be configured to hide internal restricted DNS information from external networks.	
	External firewalls should restrict incoming SNMP queries.	
	Router access control lists do not provide the protection level required for a firewall solution. A router should be used as part of a firewall solution (for example: initial Internet facing filter). This provides connection and removes some of the workload from the firewall by only passing those ports that are required, rather than having the firewall filter every single port. (However, there should still be rules in place to block unused ports on the firewall, just in case.)	
	Configure firewalls as “fail closed.”	
	Hide internal network information from external sources.	
	Configure firewalls to “deny all services, unless explicitly allowed.”	
	Translate addresses of internal network nodes that are allowed to communicate with external networks.	
	Avoid UDP-based services when possible.	
	Scan, filter or block Java, JavaScript and Activex.	
	Limit NNTP to users that need it. This should be formally justified.	
	If possible, use static routing instead of routing protocols.	
	Apply strong security policies to the host where the firewall resides.	
	Restrict access to firewall generated logs to avoid its deletion or modification in an unauthorized manner.	
	Apply all security-related patches or similars to the components of the firewall system.	
	Determine procedures are in place to verify security policies (for example: penetration testing, manual reviews of rule base, OS security reviews, etc.).	
	Verify integrity monitoring tools for sensitive system files on the firewall system exist.	
Monitor, audit and	Monitor firewall alerts on a continuous basis.	

	Suggested Procedures	√
incident response	Log all the firewall activity.	
	Determine sensitive or high-risk connections have additional protection tools, such as intrusion detection systems.	
Backup and recovery	Verify continuity plans for firewalls are in accordance with those of other high-availability services, as firewalls ordinarily are components related to services with high-availability requirements.	

7. EFFECTIVE DATE

7.1 This procedure is effective for all information systems audits beginning on or after 1 August 2003. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

APPENDIX

CobiT Reference

Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT's information criteria.

This procedure links to the following primary CobiT processes:

- PO9 Assess risks
- DS4 Ensure continuous service
- DS5 Ensure systems security (5.20 is a specific control objective for firewalls)
- AI6 Manage changes

This procedure links to the following CobiT processes:

- AI2 Acquire and maintain application software
- AI3 Acquire and maintain technology infrastructure (3.4, 3.5, 3.6 and 3.7 control objectives)
- AI4 Develop and maintain IT procedures
- AI5 Install and Accredit Systems
- DS1 Define and manage service levels
- DS2 Manage third party services
- DS3 Manage performance and capacity
- DS10 Manage problems and incidents
- PO2 Define the information architecture
- M3 Obtain independent assurance

The information criteria most relevant to a firewall audit are:

- Primarily: integrity, availability and confidentiality
- Secondary: effectiveness and reliability

References

For reference purposes and only as an example some useful pages are listed:
CERT/CC (Computer Emergency Response Team/Coordination Center), *www.cert.org/tech_tips/packet_filtering.html*
Checkpoint FW1, *www.checkpoint.com/products/security/index.html*
Cisco Pix, *www.cisco.com/warp/public/cc/pd/fw/sqfw500/*
Digital Robotics (Internet Firewall 2000), *sysopt.earthweb.com/reviews/firewall/index3.html*
Federal Computer Incident Response Center (FedCIRC) *www.fedcirc.gov./*
Firewall Options Chart, *www.networkbuyersguide.com/search/105242.htm*
Guardian, *www.netguard.com/subpages/products.htm*National Infrastructure and Protection Center, *niap.nist.gov/*
NetScreen, *www.netscreen.com/products/*
Network Ice (Black Ice Defender), *www.networkice.com/products/soho_solutions.html*
NIST's Vulnerability Database, *icat.nist.gov*
Nokia, *www.nokia.com/securitysolutions/network/index.html*
SANS Institute, *www.sans.org/top20.htm*
Sonic FW, *www.rosser.com.au/products/Sonic/sonproducts.htm*
Symantec/Axent, *enterprisesecurity.symantec.com/content/productlink.cfm#2*
SYN Flooding and IP Spoofing Attacks *www.cert.org/advisories/CA-1996-21.html*
UDP Port Denial-of-Service Attacks *www.cert.org/advisories/CA-1996-01.html*

Firewalls Procedure P6 cont

Freeware Firewall Products
Sygate, *www.sygate.com/swat/products/default.htm*
Tiny Personal Firewall, *www.tinysoftware.com/home/tiny?s=6007837888603234397A0&la=EN&va=aa&pg=prod_home*
ZoneAlarm, *www.rosser.com.au/products/Sonic/sonproducts.htm*

Firewall Reporting Products
www.stonylakesolutions.com/sls/insideout.jsp

Hardware Platforms (commonly used configurations)
Dell
HP/Compaq
HP-UX
IBM
Macintosh
Sparc
Sun

Operating Systems (commonly used configurations)
Linux
Macintosh
Netware
UNIX
Windows

Irregularities and Illegal Acts Procedure P7

1. BACKGROUND

1.1 Linkage to ISACA Standards and Guidelines

1.1.1 Standard S3 Professional Ethics and Standards states, “The IS auditor should adhere to the ISACA Code of Professional Ethics in conducting audit assignments.”

1.1.2 Standard S3 Professional Ethics and Standards states, “The IS auditor should exercise due professional care, including observance of applicable professional auditing standards in conducting audit assignments.”

1.1.3 Guideline G19 Irregularities and Illegal Acts provides guidance.

1.1.4 Procedure P1IS Risk Assessment Measurement provides guidance.

1.1.5 Guideline G15 Planning provides guidance.

1.1.6 Guideline G6 Materiality Concepts for Auditing Information Systems provides guidance.

1.1.7 Guideline G2 Audit Evidence Requirement provides guidance. Linkage to ISACA Standards and Guidelines

1.2 Linkage to COBIT®

1.2.1 The COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."

1.2.2 COBIT's *Management Guidelines* provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
Performance measurement—How well is the IT function supporting business requirements?
IT control profiling—What IT processes are important? What are the critical success factors for control?
Awareness—What are the risks of not achieving the objectives?
Benchmarking—What do others do? How can results be measured and compared?

1.2.3 The *Management Guidelines* provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management measure control capability and identify control gaps and strategies for improvement.

1.2.4 The *Management Guidelines* can be used to support self-assessment workshops and they can also be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.

1.2.6 Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

1.3 Need for Procedures

1.3.1 Although the IS auditor has no explicit responsibility to detect or prevent irregularities, the IS auditor should assess the level of risk that irregularities could occur. The result of the risk assessment and other procedures performed during planning should be used to determine the nature, extent and timing of the procedures performed during the engagement. The IS auditor should use his/her professional judgment. This document is intended to assist the IS auditor in achieving this purpose.

1.3.2 An audit cannot guarantee that irregularities will be detected. Even when an audit is planned and performed appropriately, irregularities could go undetected.

1.3.3 The IS auditor may be given information about a suspected irregularity or illegal act and may use data analysis capabilities to gather further information.

2. DEFINITIONS

2.1 Commonly Used Terms

2.1.1 Error refers to unintentional misstatements or omissions.

2.1.2 Irregularities are intentional violations of established management policy or regulatory requirements, deliberate misstatements or omissions of information concerning the area under audit or the organisation as a whole, gross negligence or unintentional illegal acts.

2.1.3 Illegal acts are those contrary to the prescriptions of law.

2.1.4 Fraud involves the use of deception to obtain unjust or illegal financial advantage.

2.1.5 Although there may not be a definite line between the concepts, two elements define the difference from error to fraud, wilfulness and materiality. Wilfulness may be beyond the IS auditor to determine, so materiality will generally be the defining factor. Material errors ordinarily are corrected by an organisation when they are identified. If a material error that has been identified is not corrected, it becomes an irregularity, i.e., an unintentional act is converted into an intentional one.

2.1.6 For convenience in this document, use of the term irregularity will include all concepts of it.

2.2 Materiality

2.2.1 Where the IS audit objective relates to systems or operations that process financial transactions, the value of the assets controlled by the system(s) or the value of transactions processed per day/week/month/year should be considered in assessing materiality.

2.2.2 Where financial transactions are not processed, the following are examples of measures that could be considered to assess materiality:

- Criticality of the business processes supported by the system or operation
- Cost of the system or operation (hardware, software, staff, third-party services, overheads or a combination of these)
- Potential cost of errors (possibly in terms of lost sales, warranty claims, irrecoverable development costs, cost of publicity required for warnings, rectification costs, health and safety costs, unnecessarily high costs of production, high waste, etc.)
- Number of accesses/transactions/inquiries processed per period
- Nature, timing and extent of reports prepared and files maintained
- Nature and quantities of materials handled (such as where inventory movements are recorded without values)
- Service level agreement requirements and cost of potential penalties
- Penalties for failure to comply with legal and contractual requirements
- Penalties for failure to comply with public health and safety requirements
- Consequences to shareholders, organisation or management of irregularities going unresolved

3. RESPONSIBILITY

3.1 Management

3.1.1 Management is responsible for designing, implementing and maintaining a system of internal controls including the prevention and detection of irregularities. The IS auditor should understand that control mechanisms do not eliminate the possibility of irregularities, and they must be reasonably conversant with the subject of irregularities to identify real factors that may contribute to its occurrence.

3.1.2 Preconditions for detecting irregularities can be:

- Determining the organisation's risk of irregularities by studying its operational and control environments
- Thoroughly understanding the symptoms, which may include:
  - Unauthorised transactions
  - Cash overages or shortages
  - Unexplained variations in prices
  - Missing documentation
  - Excessive voids or refunds
  - Lack of segregation of duties
  - Lapping—withholding deposits, using subsequent days to cover shortages
  - Kiting—using float to create cash by using multiple sources of funds and taking advantage of check clearing times
  - Unreconciled accounts
  - Lack of attention to detail
  - Improper reconciliations
    - Plugging a number to balance reconciliation
    - Carrying old outstanding items long term
  - Failure to deliver adequate goods or services
  - Manipulation of management estimates
    - Depreciation
    - Allowances for losses
    - Allowances for future warranty/guarantee work
  - Unwillingness of employees to take vacation time or rotate job responsibilities
    - Being alert to the occurrence of these symptoms

3.2 Responsibility of the IS Auditor

3.2.1 The IS auditor is not professionally responsible for the prevention or detection of irregularities or illegal acts.

3.2.2 As a result, unless information exists that would indicate to the IS auditor that an irregularity or illegal act has occurred, the IS auditor has no obligation to perform procedures specifically designed to detect irregularities or illegal acts.

3.2.3 However, under the terms of reference for an engagement, the IS auditor may be given a specific requirement to perform procedures designed to detect irregularities or illegal acts.

3.2.4 An effective system of internal control is one of the main methods available to management for preventing and detecting irregularities and errors. The IS auditor does not have a specific responsibility to rely on it, and therefore to test it, except where required by specific legislation or by agreement. However, the IS auditor should be aware that weaknesses in the internal controls of an organisation may facilitate irregularities perpetrated by employees. The IS auditor also should be aware that management can override controls and this may facilitate fraud by senior management. If the IS auditor encounters an irregularity that could be fraud, he/she should seek legal advice on how to proceed.

3.2.5 Risk is the possibility that the established system of internal control may not prevent or detect the occurrence of an act or event that would have an adverse effect on the organisation and its information systems. Risk also can be the potential that a given risk will exploit vulnerabilities of an asset or group of assets to cause loss of, or damage to, the assets. It is ordinarily measured by a combination of effect and likelihood of occurrence. Inherent risk refers to the risk associated with an event in the absence of specific controls. Residual risk refers to the risk associated with an event when the controls in place to reduce the effect or likelihood of that event are taken into account. Risk assessment measurement is a process used to identify and evaluate risks and their potential effect.

3.2.6 The IS auditor, when evaluating the internal controls in a financial auditing engagement should assess the risk of irregularities. This control objective ordinarily is driven by the following main information criteria:

- Confidentiality
- Integrity
- Completeness
- Availability
- Compliance
- Reliability
- Illegal transactions
- Operating or investing in illegal tax shelters
- Speculative investing
- Unreliable systems

4. AUDIT CONSIDERATIONS

4.1 The IS auditor may be required to provide reasonable assurance the organisation has adequate controls to prevent or detect significant irregularities. The following checklist is provided for example purposes only and is not exhaustive.

Irregularities and Illegal Acts: Investigation		
PO9, Assess Risk and DS5, Ensure Systems Security, DS11 Manage Data	Consider whether to consult a forensic specialist or investigator.	
	Determine the nature of the business, such as assets held in a fiduciary capacity and assets readily susceptible to misappropriation.	
	Identify circumstances that may unduly influence management, such as the holding of shares or options by management and performance-related bonuses.	
	Determine pressure to meet a profit forecast.	
	Determine management integrity.	
	Identify transactions with third parties that are unusual and/or not on arms length basis.	
	Identify transactions with related parties.	
	Identify unusual transactions with companies registered in tax havens.	
	Determine if liquidity is under pressure and borrowing limits are almost reached.	
	Identify management overrides.	
	Identify incompetent control personnel.	
	Determine whether there is a lack of segregation of duties.	
	Identify excessive authority vested in a senior officer.	
	Identify poor systems.	
Risk assessment results	Use the results of the risk assessment to determine the nature, timing and extent of the testing required to obtain sufficient audit evidence to provide reasonable assurance that: Irregularities that could have material effect on the area under audit or on the organisation as a whole are identified Control weaknesses that would fail to prevent or detect material irregularities are identified	
	Procedures to assist the auditor in the detection and/or confirmation of irregularities would focus on identified areas of higher risk and may be based upon conditions within the audit environment including the auditee's: Corporate and management attitudes/standards toward security and internal controls Physical and logical security methodologies Financial pressures Operating and industry environments Regulatory environment and privacy responsibilities Internal monitoring controls Management procedures in place to prevent and/or detect irregularities and illegal acts Unexplained activities, out of balance conditions and statistical deviations • Human resources policies including hiring/screening processes and incentive programs	

Irregularities and Illegal Acts: Investigation		
Analytical procedures	A very useful irregularities detections technique is the calculation of ratios for key numeric fields. Among many others, according to the area under consideration, some commonly employed ones are ratios of the: Highest value to the lowest value (review unusually big differences) Highest value to the next highest (review significant deviations from norm) Previous year to the current year (help to focus attention on areas of highest risk) Plan/budget to actual variance analysis Multi year trend analysis	
Duties	If irregularities have been detected, the IS auditor should assess the effect of these activities on the audit objectives and on the reliability of audit evidence collected.	
	If the audit evidence indicates that irregularities could have occurred, the IS auditor should recommend to management that the matter be investigated in detail or the appropriate actions taken.	
	If audit evidence indicates that an irregularity could involve an illegal act, the IS auditor should consider seeking legal advice directly or recommending that management seek legal advice.	
Application of CAATs by area to identify areas for further investigation	Identify high-value credit notes, balances and invoices.	
	Report on gaps in the sequencing of invoices generated.	
	Identify duplicate invoices, credits or receipts.	
	Determine credits, receipts and invoices not in proper sequence or range.	
	Report gaps in the sequence of generated invoices.	
	Identify adjustments to discounts.	
	Summarise large invoices without purchase orders, by vendor.	
	Compare voucher or invoice amounts to purchase orders or contact amounts.	
	Determine duplicate item or serial numbers.	
	Determine percentage change in sales, price and/or cost levels by product/vendor.	
	Match inventory receipts with vendor ledger and report variances.	
	Show items depreciated to cost in order to highlight assets greater than cost.	
	Calculate turnover by inventory class and/or item.	
	Match inventory receipts with vendor ledger amounts and report variances.	
	Identify unusual delivery addresses.	
	Identify items with high return or allowance rates.	
	Extract all payroll checks where amount exceeds set amount (by category of employee).	
	Identify persons on payroll with no time off for vacations or sick leave.	
	Identify stale purchase orders, or purchase orders with only partial orders received.	
	Identify purchases by ordering clerk for each vendor.	
	Compare inventory levels and turnover rates.	
	Check for split contract (same vendor, same day).	
	Identify duplicate vendor numbers on master vendor file.	
	Match vendor and employee names, addresses and phone numbers.	
	Test credit card balances against credit limits.	
	Determine duplicate return transactions.	
	Identify voided transactions followed by no sale.	
	Identify items sold for less than the selling price.	
	Calculate the number and amount of voids by sales clerk.	
	Determine inventory day sales by store.	
	Compare selling prices across stores.	
	Compare products on work orders and sales orders for net demand analysis.	
	Compare master planning orders to capacity to improve schedules.	
	Identify items (labor, materials) charged to project that are already completed.	
	Compute ratios such as cost of goods/revenue.	
	Generate vendor cash activity summary to support rebate negotiations.	
	Calculate market value of collateral for outstanding loans.	
	Duplicate claims for the same time period.	
	Identify duplicate invoices.	
	Identify duplicate invoice addresses.	
	Identify outstanding checks.	
	Identify uncleared pending/clearing items in accounts.	
	Determine cash over/short by sales clerk.	
	Determine cash balances (overdrafts).	
	Verify computer access controls are appropriate.	
	Verify computer processing exceptions are followed-up and missing transactions are processed.	
	Verify computer rerun analysis.	
	Verify computer fault analysis.	
	Verify computer usage-analysis capacity planning, analysis and management.	

4.2 Examples of Irregularities

4.2.1 The IS auditor draws some assurance from the absence of cause for suspicion, but should neither assume that management is dishonest nor assume unquestioned honesty. In carrying out these procedures, the IS auditor may discover circumstances that could be indicative of irregularities. Examples of such circumstances follow.

4.2.2 Unsatisfactory records/control breakdowns include:

- Poor accounting records in general
- Audit evidence of falsified documents
- Key controls not being operated
- Shredding of organisation documents prior to required corporate retention guidelines

4.2.3 Unsatisfactory explanations include:

- For figures, trends or results which do not accord with expectations
- For unusual items or reconciliations or suspense accounts
- For the unusual investment of funds held in a fiduciary capacity
- For large or "unusual" transactions, particularly when close to a period end and especially with related companies or banks
- Proper period recording and reporting
- Proper classification of transactions
- A/R—unexplained accumulation of sales on account at end of reporting period (overbooked sales)
- A/R—unexplained write off of A/R balances
- A/P—deferred payments of expenses at end of reporting period (to improve cash position)
- Receipts—unexplained shortage or receipts/deposits

4.2.4 Questionable payments include:

- Substantial payments of fees to consultants or advisers for unspecified services
- Commissions or fees which appear either excessive or unusually low in relation to the normal payments for similar work
- Large payments in cash or by banker's draft to or via overseas "shell" companies or numbered bank accounts
- Payments made to officials of domestic or overseas governments
- General lack of supporting audit evidence

4.2.5 Other questionable circumstances include:

- Correspondence between the organisation and its regulatory authority concerning problems with authorisation
- Correspondence between the organisation and its legal adviser, the substance of which is to advise against a particular course of action and which the organisation has ignored
- Investigation by government department or the police
- Audit evidence of unduly lavish life styles by officers and employees

5. REPORTING

5.1 Significant Weaknesses

5.1.1 Significant weaknesses in internal control identified during the audit should be reported promptly to management (see IS Auditing Guideline G20 Reporting, or to an outside body if required by law.

5.1.2 A significant weakness means a situation where, according to the IS auditor's judgment, the established procedures for internal control or its level of accomplishment do not provide a reasonable assurance that significant irregularities will be prevented or detected.

5.1.3 When the IS auditor suspects that an irregularity could have been occurring, where a higher level of risk could occur, or where illegal acts could occur (even if none are detected) the IS auditor should initially advise management.

5.2 Audit Evidence

5.2.1 The IS auditor's duty to investigate irregularities arises in circumstances where the occurrence of an irregularity or illegal act is suspected or where evidence exists of an irregularity or illegal act having occurred.

5.2.2 In this case, the IS auditor should consider submitting a report in writing to the appropriate parties in a separate document (not a part of the audit report) and the report should state at least that:

- The scope of the assessment carried out according with the terms of the engagement so other irregularities may have not been identified
- The report does not imply an opinion about the internal control as a whole
- Identified weaknesses were taken into account for the audit report
- Establishment and monitoring of an adequate internal control are the responsibility of the management

- The report has been prepared with the purpose of informing only and should not be used with any other purpose

6. EFFECTIVE DATE

6.1 This procedure is effective for all information system audits beginning on or after 1 November 2003. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

APPENDIX

CobiT Reference
Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT's information criteria. CobiT's Control Objective M2 covers control monitoring and the timely operation of internal controls, which are essential to prevent and detect Irregularities and Illegal Acts.

Security Assessment–Penetration Testing and Vulnerability Analysis Procedure P8

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, “IS audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met.”

1.1.2 Standard S6 Performance of Audit Work states, "During the course of the audit, the IS auditorshould obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

1.1.3 Procedure P3 Intrusion Detection System Review.

1.1.4 Guideline G25 Review of Virtual Private Networks.

1.2 Linkage to CobiT

1.2.1 CobiT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility as well as to achieve its expectations, management should establish an adequate system of internal control."

1.2.2 CobiT *Management Guidelines* provides a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 CobiT *Management Guidelines* provides example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

1.2.4 CobiT *Management Guidelines* can be used to support self-assessment workshops and can also be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 CobiT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT information criteria.

1.2.6 The CobiT references located in the appendix of this document outline the specific objectives or processes of CobiT that should be considered when reviewing the area addressed by this guidance.

1.3 Need for Procedure

1.3.1 Primarily intended for IS auditors—internal as well as external auditors—this document can be used by other IS security professionals with responsibilities in capacity of information security.

1.3.2 Modern businesses are organised as a set of core processes operating within supply and demand networks. Almost every organisation in the world is faced with increasing pressure for effectiveness and efficiency (i.e., higher quality requirements for products and services, increased revenue, cost reduction, new product development), a pressure for better, faster and cheaper processes. These increasingly complex operating networks are supported by available communication technologies (mainly the Internet), allowing businesses to focus on their core competencies and partner with others to deliver enhanced value to customers; thereby, complexity introduces multiple avenues of threats and vulnerabilities.

1.3.3 The transformation of the old processes is enabled by new communication channels. These channels provide new linking possibilities among different systems and networks, making them available to more people and letting the organisations and their processes interact (e.g., e-procurement and e-sourcing).

1.3.4 This document provides guidance for IS auditors who are required increasingly to audit or review perimeter and internal controls to provide reasonable assurance that all external and internal threats, including potential system compromises, are minimised by identification and correction of vulnerabilities detected in performing a penetration test and vulnerability assessment.

1.3.5 **This procedure is not a substitute for an internal audit including an organisationwide risk assessment and internal general controls and application audits of all critical infrastructures and applications, including those with financial statement implications. Weaknesses in a noncritical infrastructure and applications component could have a consequential impact on a critical infrastructure and application components; therefore, a system wide audit should be completed in its totality and not in a piece-meal fashion.**

2. PENETRATION TESTING

2.1 Introduction and Planning

2.1.1 The penetration testing scope determines whether the individual tasks should occur in phases or in single sequence. The IS auditor’s review should begin with a formal threat assessment to ascertain the likelihood of any threats to the organisation resulting from, among other reasons, hardware and/or software failures, internal employee compromise or data theft, or outside attacks.

2.1.2 The risks associated with unauthorised access vary from financial loss; inappropriate release of personal, commercial or politically sensitive information; and reputation lost; to total loss of system control. The specific information system risk of unauthorised access to information resources includes loss of system availability, data and processing integrity, and information confidentiality.

2.1.3 The purpose of this procedure is to test controls that should be employed to protect against unauthorised access. Since methods used for unauthorised access vary greatly and are becoming more sophisticated, the procedures defined are general in nature and should be supplemented, wherever possible, with techniques and tools specific to the environment(s) under examination.

2.1.4 The significant difference in the actions taken by an IS auditor performing penetration testing (beyond having management authority) and a hacker is that the former is searching for (via testing) as many potential vulnerabilities as the testing script/program mandates, while hackers ordinarily will search for a specific vulnerability(ies) to exploit to fulfil their goal of (typically) obtaining control, or disrupting the operation or availability of the system. The hacker is likely to continue to attempt to find additional vulnerabilities once one is found to obtain increased system privileges and to protect against the increased risk of detection. Therefore, while an IS auditor performing penetration testing has a greater overall scope for finding general vulnerabilities, the hacker is likely to attempt to exploit any identified vulnerabilities more extensively.

2.2 Record Keeping

2.2.1 Records should be in sufficient detail to support the findings and conclusions reached as a result of the testing to:

- Defend against accusations of unethical or unauthorised practices against the IS auditor performing the test
- Provide the organisation with a detailed description of the weaknesses and how they were identified and exploited
- Provide an audit log for future testing to provide reasonable assurance that vulnerabilities identified have been addressed
- Demonstrate the possibility and risk of unauthorised access from any determined/willing attacker possessing the skills

3. TYPES OF PENETRATION TESTING AND VULNERABILITY ASSESSMENT

3.1 Scope of Evaluation

3.1.1 There are several types of penetration tests that will, depending upon the circumstances, affect the scope of the evaluation, methodology adopted and assurance levels of the audit.

3.1.2 The individual (appropriate IT management) responsible for safeguarding the organisation should evaluate various alternatives, selecting that which provides the maximum level of assurance with the least disruption acceptable to the organisation (cost/risk analysis).

3.1.3 There should be agreement on the type of penetration testing to be carried out–intrusive or nonintrusive.

4. EXTERNAL PENETRATION TESTING AND VULNERABILITY ASSESSMENT

4.1 Internet

4.1.1 The purpose of Internet testing is to compromise the target network. The methodology needed to perform this test allows for a systematic checking for known vulnerabilities and pursuit of potential security risks. The methodology ordinarily employed includes the processes of:

- Information gathering (reconnaissance)
- Network enumeration
- Vulnerability analysis
- Exploitation
- Results analysis and reporting

4.1.2 There are several variations to the processes listed in section 4.1.1. However, a common, standardised and objective script is ordinarily followed and should provide a detailed and exact method of execution. In addition, the intricacies of new vulnerabilities and methods of exploitation require detailed study with a history of information to draw upon.

4.2 Dial-in

4.2.1 War dialling is the systematic calling of each number in the target range in search of listening modems. Once all listening modems are identified, brute force default password attempts or strategic guessing attempts are made on the username/password challenge (sometimes only passwords are necessary) to gain unauthorised access.

4.2.2 Access to the login screen banner is crucial to accessing any system. Some systems require only a password, which can be a vendor-provided default password or just hitting “enter.”

4.2.3 At times of poor configuration, even a login banner does not appear and access is granted directly devoid of any authentication mechanism.

5. INTERNAL PENETRATION TESTING AND VULNERABILITY ASSESSMENT

5.1 Goal

5.1.1 The goal of internal penetration testing is to ascertain vulnerabilities inside the network perimeter. The testing performed closely parallels that which an internal IS auditor will be assigned to audit, given the size, complexity and financial resources devoted to risk associated with lack of security concerns. The overall objective is to identify potential vulnerabilities within the internal network and weaknesses in controls in place to prevent and/or detect their exploitation by a hacker/malicious employee/contractor who may obtain unauthorised access to information resources, orcause system disruption or a system outage.

5.1.2 The first phase relates to information gathering, which is comprised of public information search, googling, obtaining maximum information about business, employees, etc., thereby profiling the target. For instance, this phase may result in obtaining resumes/CVs of employees which may be useful in understanding technologies employed at the attack site.

5.1.2 The first testing goal is to ascertain the internal network topology or footprint that provides a map of the critical access paths/points and devices including their Internet protocol (IP) address ranges. This is the network discovery stage.

5.1.3 Once critical points/devices are identified within the network, the next step is to attack those devices given the various types of known vulnerabilities within the system and operating software running on the devices (e.g., UNIX, NT, Apache, Netscape and IIS). This comprises the vulnerability analysis phase.

5.1.4 Exploitation and notification is the third and final phase.

6. PHYSICAL ACCESS CONTROLS TO DATA CENTRE AND OTHER WORK SITES

6.1 Rogue Access Jacks

6.1.1 Identification of telecommunication access paths into and out of the organisation's premises, including communications rooms, and the data centre areas are critical to identifying potential methods to intercept, prevent or modify data communications. These access paths should be physically secured from unauthorised access and rendered inaccessible without the knowledge and specific permission of the organisation as well as specialised equipment.

7. SOCIAL ENGINEERING TESTING

7.1 Tests of Controls

7.1.1 Social engineering techniques are employed in an attempt to obtain information regarding perimeter network devices and their defenses (i.e., IP address ranges, firewalls and default gateways) as well as potential internal targets. The information gathered during the reconnaissance phase outlines the basis of this test. The purpose of this testing is to assess the ease of extraction of critical information from internal organisation resources and employees/contractors, or others with detailed knowledge of the organisation, without their becoming aware of the significance of the information obtained. Of particular interest is testing whether the organisation's help desk will assist an unauthorised or unidentified user.

7.2 Telephone Access

7.2.1 First, and most importantly, the more information that the individual performing the test has about the organisation, employee and network, the greater the likelihood of success of extracting information. The individual performing the test should have a script. For example, the individual performing the test may pose as on of the technical support personnel, whose name was obtained in an earlier help desk call seeking information pertaining to connectivity and, therefore, requesting network information. Typically, these social engineering efforts succeed when information obtained from one source is used in combination with information from a second, progressive source.

7.2.2 Using information obtained from the help desk in the example in 7.2.1, the test continues by having an auditor pose as an organisation employee over the telephone asking for a password reset/change. These tests are best performed using a telephone inside the organisation, as help desk/security personnel employees may be more willing to accept the masquerade and provide the information requested without detailed authentication/personal confirmation. Acting as an impatient, disgruntled or aggravated customer over the phone as well as other personal behaviours (i.e., telling the help desk employee that they need access to get information to their superior without specifying their name) may add to the likelihood of success.

7.2.3 Background information, such as the mother's maiden name, zip code or social security number, of the employee being impersonated by the individual performing the test is helpful. In addition, obtaining resumes/CVs of employees through an Internet search or a stranger headhunter approach could be of more help.

7.2.4 Impersonating a consultant/auditor and reaching IT staff directly without any introduction is another approach. Management should be aware and agree to this approach to prevent unnecessary troubles.

7.2.5 Nevertheless, it is recommended that if caught because confidential propriety information is unknown, the tester should excuse themselves using some plausible justification (e.g., not feeling well, their boss needs them right away, do not have time right now). Each piece of information obtained adds to increase the likelihood of a successful penetration to a critical information asset.

7.2.6 Each organisation differs in its structure (i.e., centralised in the same geographical area vs. segmented over a large physical area under different management), size (i.e., medium size bank with 500-800 employees to large financial management organisation with over 10,000 employees), network complexity and security awareness (i.e., well-known organisation or federal agency that is continuously probed by port scanning). All types of testing are valuable in obtaining valuable and sensitive information by social engineering.

7.3 Garbage Viewing

7.3.1 Review of garbage disposal areas and bins for information can be a valuable source of sensitive security and overall organisational information that could be useful in a social engineering examination. Access to recycled paper bins should also be considered a source of critical information.

7.3.2 Physical harm is possible in going through an organisation's garbage, as there could be everything from sharp objects to hypodermic needles to hazardous chemicals. The penetration testing contract, if performed by external consultants, should explicitly allow for this type of testing.

7.4 Desktop Review

7.4.1 As noted previously, none of the information obtained using social engineering may be particularly relevant except when taken together with other information obtained via other tests defined in this procedure. The most important aspect when attempting to exploit individuals' naivete or lack of training for the security of organisation proprietary information is that there will always be someone who will divulge information and it is ordinarily only a matter of time before such an individual is contacted.

8. WIRELESS TECHNOLOGY BACKGROUND

8.1 Background and Risks Associated With Wireless Technologies

8.1.1 With the advent of wireless technology for transmitting data and voice, the well-known and relied upon controls instituted using perimeter devices are disappearing. Gone are the physical security controls, such as security guards, cameras and locks, that were effective in protecting wired networks and data transmissions. The major vulnerabilities result from the users of wireless technologies not addressing the following:

- Reliance on WEP for encryption
- Wireless networks not being segregated from other networks
- Descriptive SSID or AP names being used
- Hard-coded MAC addresses
- Weak or nonexistent key management
- Beacon packets that have not been disabled or are "enabled"
- Distributed APs
- Default passwords/IP addresses
- WEP weak key avoidance
- DHCP being used on WLANs
- Unprotected rogue access points

8.1.2 The risks and threats associated with attacks against wireless networks are widespread including:

- Attacks where message traffic is captured and analysed and encryption keys cracked, i.e., initialisation vector—IV
- Resource theft, where Internet access is obtained that in return is used as a launch pad for other attacks, i.e., cyclical redundancy check (CRC-32)
- Denial-of-service due to signal interference and propagation of threat from viruses and worms

8.1.3 In addition, as with other types of technologies, the greatest weakness with wireless security is not the technical shortcomings but out-of-the-box insecure installations. The human factor is typically the weakest link.

9. WEB APPLICATION

9.1 Manual and Automated

9.1.1 Web application testing includes manual and automated testing of the portal site as an outsider with no login information. This testing compliments the external penetration testing. The goal of this testing is to gain an understanding of how individuals interact with the system in accessing sensitive data.

9.1.2 Additional testing may include testing of the portal site by an insider through a standard login account. The goal of this testing is to determine the ease of access to sensitive information that is not authorised by the login account (i.e., privilege escalation).

9.1.3 Identification and exploitation of vulnerabilities can be accomplished through the use of various commercial and open source vulnerability assessment tools.

10. SUGGESTED PROCEDURES

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Planning	Define the scope based on the nature, timing and extent of the evaluation.	
	Verify that no test will violate any specific law of local or national statute. Also, the auditor should consider obtaining a signed "authorisation form" from the organisation agreeing to the deployment of penetration testing tools and methods.	
	Investigate and use available automated tools to perform penetration testing and vulnerability assessments. These tools improve the efficiency and effectiveness of penetration testing.	
	Define the scope of the review by asking the following questions: ■ Will the chief information officer, computer security and IT personnel be told of the penetration test? ■ Will the audit testing focus on detecting control weaknesses from those accessing the information infrastructure from the Internet and dial-in access (external) or from inside the organisation (internal)?	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Planning continued	■ How far into the network and information asset will the penetration testing be performed? For example, will the testing be performed to the extent of actually accessing the information assets or will it occur to an access check point (where access to the information assets is not accomplished but there is sufficient information that it could occur based on testing)? Will the test be intrusive or nonintrusive? ■ What level of overall system degradation, and for what duration, will be acceptable in performing the tests? ■ Can the test be performed off hours to avoid potential conflicts with causing critical system outage (e.g., executing nmaps against firewall off hours, such as Sunday morning, while web application services are not used)?	
	Obtain access to a (public) vulnerability database, such as bugtraQ, packetstorm, etc. The tester should determine that any tools used are up to date with the latest vulnerability database.	
Skills Required	Possess sufficient technical knowledge of, and ability to recognise and/or detect different types and variations of, security flaws/bugs/weaknesses/vulnerabilities. For example, the individual should have an understanding of the controls required over dial-in penetration, denial-of-service, password cracking, buffer overflows and wireless, as well as have access to up-to-date vulnerabilities database services.	
	Possess strong knowledge of how various technologies work, such as firewalls and routers, intrusion detection systems, and various types of authentication mechanisms.	
	Possess working knowledge of application programming, such as JAVA, Visual Basic and C++.	
	Possess knowledge of various operating systems, such as UNIX, Linux, NT/2000, Windows and OS/390 (or its current mainframe version).	
	Possess working knowledge of TCP/IP and networking protocols.	
	Possess working knowledge of web server software, including Microsoft IIS and Apache.	
	Possess knowledge in utilising the penetration tools selected to detect bugs and vulnerabilities.	
	Possess knowledge the effect on internal system of executing penetration and vulnerability tools, including the NMAP, ISS, Whisker, Nikto, WebInspect, AppScan, ESM and Root, Nessus.	
Agreements	Keep all records, including specific and detailed logging of all keystrokes and verbal discussions, of all activities during the penetration and vulnerability testing. These records should be in sufficient detail to recreate the test, if necessary.	
	Keep all records of the penetration testing, including the results, confidential as they are the property of the organisation. All records of the penetration and vulnerability testing should be maintained within the organisation's control. The individual performing the test should sign nondisclosure and code of ethical conduct statements with the organisation regarding the confidentiality of the scope of the test and results.	
	If the test is to be performed by external consultants, include a contract to protect the organisation. The contract should state the boundaries and scope of the work to be performed, the ownership of the results and test procedures, as well as require confidentiality and ethical conduct of the consultants. In addition, the external consultant should provide insurance and a "hold harmless" clause to mitigate risks as a result of an inadvertent release of information.	
Scope Questions	Does the testing consist of evaluating the control environment based on penetrating the information infrastructure from inside vs. outside the network perimeter? For example, if the test consists of evaluating the firewall rule set based on attempted access to penetrate the network from the Internet, the evaluation is focused on determining the access control from outside the network perimeter. Testing of perimeter controls is limited in scope to the physical and logical controls that safeguard the information assets from those threats external to the organisation. However, once the perimeter security controls are compromised, a decision should be made, whether to continue testing to determine the adequacy of the controls over the target information systems. Conversely, the vulnerability testing may be focused on evaluating the internal control environment to prohibit access to information assets from inside the organisation.	
	Is the appropriate level of management, including IT security, notified of the penetration or vulnerability testing? If a formal announcement is made of the testing, strong cooperation and more thorough evaluation may be achieved. Conversely, unannounced testing may better represent the actual risks and management's response based on real-world threats from unauthorised access attempts. It is essential to assess the best-case scenario and level of assurance needed.	
	Are the individuals performing the test provided information about the organisation in advance? This question goes with whether management is notified of the nature and scope of the test. However, there are times when just the executive or high-ranking IT management is notified of the test and it is not announced to the staff. Nevertheless, if information is provided (i.e., network topology) and used by the tester, a more exact review of the target systems and processes can be examined, possibly resulting in better identification of risks and vulnerabilities. However, providing insider information may result in difficulty in understanding the depth of the vulnerabilities and their likelihood of exploitation. In addition, the IP ranges, if provided by management should also be tested.	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Internet Penetration Testing	• Network enumeration is the information obtained: network resources and shares, user logins including generic installation (out of the box) hardware and software vendor user IDs, IDs and their groups, and applications and banners. The steps to consider are: • Identify the domain name, IP address range and other critical information. Ordinarily, the "who is" query is used, which typically provides the address of the target network (i.e., domain name servers and IP address mapping), administrative contact and billing contact. The individual executing the "who is" query should provide reasonable assurance that all listings are obtained, and not just the first 50 items, which may require grouping the names into plurals or modified organisation names. • Identify IP address ranges that may be owned by the organisation. This is typically done by querying Internet number registries such as ARIN, RIP, APNIC and LACNIC. • Identify external e-mail servers by gathering MX record information from DNS servers. • Attempt a zone transfer between all systems identified as a DNS server (including back-up servers) to obtain the network IP listing and the machine host names. A zone transfer requests the complete list of matched IP addresses and host names stored within a DNS for a specified domain. In addition, the "nslookup," which is supported by both the UNIX and Windows platforms, may also be used to perform a zone transfer using a DNS server that is authoritative for the domain of interest. In addition, the machine's host names may indicate its purpose (i.e., mail server and firewall), which is one more critical piece of information. Recent technologies prevent the ability to perform a zone transfer without the initiating device. • Determine whether the organisation has outsourced its domain name function to an Internet service provider (ISP). In cases where this function is outsourced, it is recommended that the terms of the penetration test clearly state whether the hosted system is within the scope of the engagement. • Notify network staff that a penetration test may be underway because zone transfer can be detected. • Use ICMP (ping) or TCP ping (with a full or half TCP handshake) sweeps to determine which machines for IP addresses are "up" or "live." Though this step may provide critical information regarding which devices are active, there is a likelihood that perimeter security devices or firewalls may drop the ICMP traffic to the host. It may be filtered and dropped with a response indicating the device is down, when it is not. It is recommended that randomising the order of the IP addresses being pinged helps avoid detection, as does varying the NMAP. NMAP is a popular tool used for UNIX-based systems and Pinger, and Ws PingPro Pack are used in Windows-based environments for performing Ping sweeps. • Use the traceroute method to identify the paths from the Ping packets to the destination target. The routes can then be traced to the destination live hosts, detected using the Ping sweeps to derive an estimated map of the organisation's architecture topology. The two commonly used tools are tracer route and tracert, available for both UNIX- and Windows-based operating systems. The purpose of this method is to identify the common and uncommon "hops" prior to reaching the destination targets, which could represent such things as firewalls, filtering routers or other gateways, load-balancing devices ,or web redirectors. It is not uncommon for network segments to have multiple connections to the Internet—unknown to the network group. However, these uncommon paths can lead to network compromises, if uncontrolled. • Send "bogus" e-mail messages to domains owned by the organisation in an attempt to receive a returned e-mail. Review the header of returned e-mails to determine possible network paths.	
	To perform a vulnerability analysis: • Assess possible methods of attacks based on identification of vulnerabilities. To do this, identified machines within the target network are examined to identify all open ports, the operating systems (OS), the applications and their hosts (including version number, patch level and/or service pack). In addition, this information is compared with Internet vulnerability databases to ascertain what current vulnerabilities and exploits may be applicable to the target network. • Identify the type of OS employed by target hosts. For those target hosts identified in the network enumeration phase, the NMAP tool can be used to identify the type of OS employed. The type of OS employed is critical in predicting the types of service available and then to tailor the targeted analysis of service rendered through that port, which, when executed, will determine if specific vulnerabilities exist. In conjunction with this step is the need to obtain a current list of vulnerabilities for the OS employed by searching the OS vendor's web site and vulnerability databases to obtain details of these vulnerabilities. • Obtain permission to execute a port scan for those destination target hosts that are "live." A port scan may be needed on all possible ports (1-65535), if the security group is aware of the penetration testing. The list of ports should include applications that have known vulnerabilities. Ports examined should relate to weaknesses, vulnerabilities or information gathering. For example, the ports for file transfer protocol (FTP), Telnet, and RealSecure (ports 21, 23 and 2998) are often selected to attempt to exploit vulnerabilities. NMAP is the standard tool and can be programmed to execute a port scan for those destination target hosts that are "live" (from a port scan). Port scanning is clearly unethical without the express	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Internet Penetration Testing continued	permission of the port owner. Port scanning, as with many other vulnerability tests, is a technique that may be employed by hackers, and should alarm the security group of a potential attempted penetration. • Perform an application enumeration to identify assigned services (applications) of ports. In addition to the port scan, the specific identification of assigned services (applications) to a port is known as application enumeration. Knowing which applications the target hosts are running goes a long way toward performing a vulnerability analysis. Ordinarily, the applications are run through the Internet. Find a list of known vulnerabilities and exploits for these applications, which often comes from the vendors themselves and vulnerability databases. Application enumeration also involves banner grabbing, which may be helpful in identifying running applications. This can be done with many applications, including Netcat, which runs from either the UNIX or Windows command line; Telnet; and What's Running, a Windows GUI tool. Examples of common sources of information about system and application software vulnerabilities and exploits are Bugtraq lists, Packetstorm and SecurityFocus. • Run commercial or open source network vulnerability assessment tools to verify results. Popular tools include Nessus, ISS Internet Scanner, Foundstone's FoundScan, eEye's Retina Scanner and GFI's LANguard.	
	Exploit vulnerabilities identified in the vulnerability analysis to attempt to gain root or administrator-level access to the target systems or other trusted user account access as follows: • Document all relevant information upon access to the command line of a targeted system, via the access points identified in the vulnerability analysis, including the host and directory or share name to which access was gained; the host from which access was gained; date, time and the level of access; and finally the security hole(s) that were exploited to gain access. • Launch attacks against other systems on the network from the host that was compromised. If possible, a tool kit is installed on the exploited hosts that are tailored to the operating system of the other targeted machines to ascertain their vulnerabilities. The tool kit may include Netcat, password crackers, remote control software, sniffers and discovery tools, which can be executed from the command line. At this point, the method of Internet (external) penetration merges with internal testing methods described in section 5. • Notify the organisation if the access level is achieved, allowing installation of critical viruses that could result in consequential system outage.	
Dial-in Penetration Testing	Gain penetration by dialing in over the telephone line that is listening for incoming connections, and log into the host machine. Example of vulnerabilities searched for may include: • Modems attached to machines, such as routers, that are used by the hardware and software vendors to maintain it (i.e., installation of patches) • Rogue modems that are connected to actively listening users' desktops • Modems where remote management tools are installed, such as PCAnywhere • Modems that are authorised but insecurely configured	
	Gather the groupings of phone numbers used to make calls. Sources include phone books, online directories, company brochures and literature. Internal telephone directories may be particularly valuable, if accessible. These may be based on block(s) of phone numbers within a specified range that may be geographically assigned: • Find where the target organisation physically resides, which will define its area code and, to a lesser extent, its prefix. • Attempt to obtain these numbers independently of the organisation to ascertain the difficulty. It may require a level of social engineering.	
	Identify listening modems by calling each number in the target range randomly. War dialing software can be employed to dial and record the responses to determine if there is a modem listening.	
	After detecting a modem that is listening, gain unauthorised access by making brute force default passwords or strategic guessing attempts on the username/password challenge. War dialing software can be set to attempt to gain login access by using the largest list possible and/or selective list of default user IDs and passwords. The selective default list may also include strategic guesses of the user ID/password pair. For example, for a Cisco router, the username/password pair may be Cisco/Cisco or enable/Cisco or, when only a password is asked c, cc, cisco, and Cisco router, may be attempted. Vendor provided default user ID/password pairs should be attempted, as these are very often not changed or disabled.	
	Determine whether sniffers and keyboard loggers are installed on web devices within the demilitarised zone (DMZ) to pick up user IDs and passwords.	
	Consider whether PCAnywhere is being used, configured to allow connection without authentication as long as the calling client is using the PCAnywhere.	
Internal Penetration Testing	Perform a network discovery test using the following steps: • Perform a Ping sweep to identify live hosts. Popular tools include NMAP Pinger, NetScan tools and WS_Ping ProPack tools. • Also, if possible, install sniffers on the hosts that have been compromised in the external penetration test that identifies ARP tables, SNMP data and routing information. • Attempt to perform a zone transfer to learn internal IP addresses and computer names, which may indicate the purpose of the host. • Attempt to perform a tracer route to fine tune the target list of hosts deemed critical.	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Internal Penetration Testing continued	• Guess the community strings or whether it was set to public or private to obtain SNMP information, which includes routing tables, protocols, error logs, and other system and network data, to build an attack. Also attempt to guess commonly used community strings (e.g., Cisco, {company name}, router, switch, network) • After completing the above, obtain authorisation from the security group to install host-based automated discovery tools that provide a full listing of vulnerabilities. Popular tools include Enterprise Security Manager (ESM), ISS, etc.	
	Perform a vulnerability analysis using the following steps: • Execute a port scan and banner grabbing programs on the target hosts to identify active services. This is comparable to external penetration testing. This step can be performed in conjunction with the Ping sweeps using NMAP. • Test the individual known vulnerabilities for each type of system software, in conjunction with the open ports for exploitation. For example, known anonymous FTP vulnerabilities should be tested to determine if these weaknesses could be exploited by utilising an exploit script and subsequently installing a root kit containing Netcat to open up a command prompt on a particular point. There are numerous known vulnerabilities that constantly expand. • Obtain authorisation from the security group to install automated discovery tools that provide a full listing of vulnerabilities. These tools include CyperCop, Enterprise Security Manager (ESM) and Internet Security Scanner (ISS) and Nessus. • Generate a schedule of IP addresses host names, types of system software (i.e., UNIX and NT), open ports and application (Netscape and IIS and Apache).	
	Perform the exploitation and notification using the following steps: • Determine the level of attack that the organisation would desire and approve. • Determine the level of attack based on the level of access obtained on the open ports and the target hosts identified by the discovery and analysis stages, or on the basis of information provided by the organisation. For example, if the target host is UNIX-based, the next step after gaining access to this device could be to attempt to crack the password file. In addition, if the attacker can obtain access to other devices and valuable organisation data without detection, the penetration was a full success. • Notify the organisation if access level is achieved, allowing installation of critical viruses or root kits or other tools or software that could result in consequential system outage or to demonstrate the ability of an attacker to retain unauthorised access devoid of detection. • Record all vulnerabilities noted and provide to the organisation for immediate follow-up at the conclusion of the penetration test/vulnerability analysis.	
Physical Access Controls	Search for rogue access jacks that can be exploited. Identify telecommunication access paths into and out of the business and data centre area. Access paths should be buried or cancelled and not accessible by the general public. Attempt to identify cabling in ceilings or closets where an unauthorised tap can occur, though this may not be always possible especially given the use of fiber optic cable.	
	Perform brute and selective access to default userIDs once access to the network is physically obtained.	
	Obtain physical access and initiate social engineering as defined in section 7 of this procedure: • Without authentication as an employee, one should attempt to obtain unimpeded access. For those organisation sites with physical security via mechanical, electronic or physical guard, this testing can be accomplished in multiple ways including piggybacking into the site with a legitimate employee or signing in without an escort and walking directly into the data centre or business work sites. • Standard business practice should restrict direct unimpeded access to all work areas. • The consulting agreement or internal auditor performing the test should explicitly require this evaluation. • A data centre audit should be performed to evaluate all the physical controls to the data centre and other work sites.	
	Create burs around the data centre complex to avoid intruders or interlopers from obtaining transmission signals.	
Social Engineering Testing	Test controls to prevent social engineering or circumvention of logical security measure in place by masquerading as an individual calling over an internal phone with a business need requesting critically sensitive information or access to basic computing services.	
	Explicitly allow the penetration testing contract, if performed by external consultants, to test garbage disposal areas.	
	Review confidentially polices and practices to ascertain whose responsibility it is for the disposing and shredding of organisation-related information in hard copy form. Safeguards for the disposal of data are critical.	
	Review measures for the disposal of magnetic media holding sensitive data.	
	Review individual employee work areas as well as printer baskets for propriety information, such as user ID, other employee's information and computer names, if physical access to the work area is obtained. Sticky notes and to-do lists can be sources of important information.	
	Obtain a building and floor schematic of critical areas. Work areas, such as the treasury and disbursement departments as well as executive offices, are primary targets.	
	Determine whether individual desktop computers have a screen saver and work desks are locked.	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
	Provide reasonable assurance the scope of the work does not break any laws.	
Wireless **Wireless continued**	Find and map the wireless networks into a street or physical geographic area map. The tools needed to perform a penetration test of a wireless network may include a laptop/PDA, a wireless NIC (ORiNOCO or Lucent PC, Card Dell TrueMobile 1150, Avaya Wireless PC Card, Compaq WL110, Enterasys Roamabout Elsa Airlancer MC-11), freeware software, and an antenna and GPS. One technique used for finding a wireless network is War Driving. This is done by detecting the beacon and broadcast. War Driving is used to capture and map wireless band signal.	
	Crack the WEP (Wired Equivalent Privacy) keys by using automated tools such as WEPCrack and AirSnort. The techniques used include IV Collisions and Weak key packet capture.	
	Sniff and analyse the network traffic to ascertain the number of packet passes, SSID, etc. There are a variety of automated tools, such as PrismDump, Iris, AiroPeek and Sniffer Wireless.	
	After the key is known, reassemble the packet to complete the penetration test. Document all issues noted for management review. Before this test, it is best to consult legal representatives practicing within the individual countries and, where necessary, local and state municipalities to provide reasonable assurance that performing this test will not violate any laws or regulations due to picking up information packets from other unintended targets.	
Web Application	Analyse the web application and environment by first crawling through the web pages to gather the information including mapping of all pages and general understanding of all functionality to ascertain risk. Specifically, manually surf the application with a recording proxy (e.g., webproxy, ebsleuth) to find hidden data and locate form weaknesses. In conjunction with this survey, complete the following: • Review inventory SSL/TLS ciphers to determine accordance with policies or standard industry practices. • Analyse session tracking including mechanism and session ID. • Identify authentication methods employed, including client certificates, auditing and revoking certificates, use of encryption or HTTP basic authentication and deployment of SSL. • Identify sign-on and sign-off (use of anticaching techniques and session inactivity cause automatic sign-off) mechanisms. • Identify all points of user input by recording every form element, specifically: ▪ Test SQL injection ▪ Attempt buffer overflow to gain control ▪ Cross-site scripting (XSS) ▪ Special characters (pipes, returns, etc.) ▪ For numeric input try 0, a negative value, a really large value ▪ Record any verbose error messages. In addition, test any HTTP headers being used as input such as: ▪ Cookie, Referrer, Host, User-agent ▪ Record permutation list used ▪ Record any verbose error messages ▪ Test user input embedded into URL for POST • Review for hidden content or information leakage in Web Application Output • Search for client-side code for unnecessary information (meta tags, comments). • Ascertain if HTTP from server for unneeded information (Server:, X-). • Determine if Java applets and similar are decompiled. • Retrieve robots.txt file for each known directory and review. ▪ Review security over session IDs including the following tests: ▪ Determine if they are random, not related to user information, large enough to avoid brute force, perishable, transmitted over secured path, controls to prevent tempering, and have a detection mechanism. ▪ Determine that cookies with session IDs are marked “secure” (encrypted), nonpersistent (not stored on hard-drive), reasonably limited to path and domain and, if appropriate, digitally signed. ▪ Verify URLs with session ID are sent with encryption, such as SSL. ▪ Review controls over sign-on including the: • Warning banner and error messages to warn against an unauthorised hacking attempt • Generic message does not providing specific knowledge of which is incorrect when a login is made with an invalid password or login account • Encryption of initial login involving credentials • Timeout after a period of inactivity to prevent half open sessions • Lockout mechanism for invalid login attempts to minimise exposure to brute-force attacks • Lock mechanism does not result in denial of service of a substantial number of suspended login accounts, rather it provides notification of attack resulting in an escalation process • Determine if all information transmitted is encrypted, such as verifying lock is shown on web browser. Ascertain if all pages sent and received are encrypted. Collectively review results of the survey evaluation and results of the portal testing steps to ascertain the vulnerabilities that could be exploited to gain access to sensitive information by an	

	Suggested Penetration Test and Vulnerability Analysis Procedures	√
Web Application continued	outsider with no information of the system and no login account and an insider with knowledge of the system with a login account. **Note:** Since there are significant numbers of exploits detected via port 80, as time goes by, it is recommended that those performing this test possess current knowledge that would exceed that which is defined in various research documents, white pages and web sites. In addition, there is a series of audit testing of the web servers, including standard access control list evaluation and TCP/IP weakness, that should be performed and are included in other sections of this procedure.	
	Run commercial or open source application vulnerability assessment tools to verify results. Popular tools include Nikto, WebInspect, ScanDo and Appscan. There are numerous potential vulnerabilities that could be detected by performing the above testing. Accordingly, the second step is to exploit potential vulnerabilities, which would include, but are not limited to, the following: • Alter contents of cookies (e.g., altering the parameters passed to the application through a URL) resulting in access to sensitive information or impersonating another user. • Change JavaScript within the application or hidden form files on application forms, parameter tampering, SQL injection (passing SQL code into an application that was not intended), cross-site scripting (entering executable commands into web site buffers). • Insert code into text fields to take control of an application. • Directly access a web page that can ordinarily only be reached through authentication by a brute force attack. Collect user IDs where wrong passwords are entered and execute the dictionary against them. • Directly exploit backdoors and debug options including executing debug syntax on URLs (e.g., there is a listing of vulnerabilities on various web sites including CERT and vendor sites, such as *www.nstalker.com*). • Exploit any configuration errors in third-party applications, such as web or database servers. Specific attempts should be made to exploit web server default configuration vulnerabilities that are known. • Insert scripting languages in a text field that other users will see. • Pass excessive data in an application request (e.g., sending large numbers of characters to a web site form/field).	
Report	Prepare report in accordance with ISACA IS Auditing Standards including: • Defining the scope • Objectives • Period of work performed • Nature, timing and extent of the penetration testing and vulnerability analysis performed • Conclusion as to the effectiveness of controls and the significance of vulnerabilities identified	
	Follow-up to provide reasonable assurance that controls were implemented and security holes were plugged on all known vulnerabilities.	
	Perform a specific process and attribute review of perimeter firewalls and routers, and discuss risks identified with management.	

11. EFFECTIVE DATE

11.1 This guideline is effective for all information systems audits effective 1 September 2004. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

APPENDIX

COBIT References

Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT information criteria:

- PO6—Communicate Management Aims and Direction
- PO9—Assess Risks
- A13—Acquire and Maintain Technology Infrastructure
- DS5—Ensure Systems Security
- DS7—Educate and Train Users
- DS10—Manage Problems and Incidents

The information criteria most relevant to a penetration testing and vulnerability assessment are:

- Primary: confidentiality, integrity and availability
- Secondary: efficiency and reliability

References

Bosworth, Seymour; Michel E. Kabay, Editor; *Computer Security Handbook*, 4th edition, John Wiley & Sons, Indianapolis, Indiana, USA, April 2002

The CERT Guide to System and Network Security Practices, 1st Edition, Addison-Wesley Publishing Co., June 2001

e-Commerce Security: Security the Network Perimeter, IT Governance Institute, Rolling Meadows, Illinois, USA, 2002

Klevinsky, T.J.; Scott Laliberte; Ajay Gupta; *Hack I.T.—Security Through Penetration Testing,* Addison-Wesley, Boston, Massachusetts, USA, June 2002

Kreutz, Vines,;"The CISSP Prep Guide;" John Wiley & Sons, Inc.; 2001

Rhoades, David; "Hacking and Securing Web-based Applications," Maven Security Consulting Inc., 12th USENIX Security Symposium, Washington, DC, USA, 4-8 August 2003

Scambray, Joel; Stuart McClure; George Kurtz; *Hacking Exposed—Network Security Secrets & Solutions,* 2nd Edition, Osborne/McGraw-Hill, Berkeley, California, USA, 2001

Yeager, Nancy J.; Robert E. McGrath; *Web Server Technology*, Morgan Kaufmann Publishers Inc.

Evaluation of Management Control Over Encryption Methodologies Procedure P9

1. INTRODUCTION

1.1 CobiT Reference

1.1.1 Refer to the CobiT reference for the specific objectives or processes of CobiT that should be considered when reviewing the area addressed by this guidance. Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT information criteria.

1.1.2 CobiT guidance for the following processes should be considered relevant when performing the audit:

- PO8—Ensure Compliance with External Requirements
- DS5—Ensure Systems Security
- DS11—Manage Data

1.1.3 The information criteria most relevant to an encryption technology audit are:

- Primary—Effectiveness, confidentiality, integrity, availability and compliance
- Secondary—Efficiency and reliability

1.2 Fundamentals of Encryption

1.2.1 Encryption is a means of transforming data from a readable form (known as plaintext or cleartext) to one that is unintelligible (referred to as ciphertext). This definition differs from encoding, which is a substitution of a symbol or set of symbols for a plaintext message (such as, “one if by land, two if by sea”).

1.2.2 A mathematical algorithm that encrypts data is referred to as a **cipher**. Most modern ciphers encrypt cleartext data with a **key**, or a piece of secret information known only to authorised parties. By the 17th century, cryptographers understood that maintaining the secrecy of encrypted data relied upon keeping the key secret, rather than the inner workings of the algorithm or cipher.

1.2.3 Encryption technology provides a safeguard against accessing legible information but does not restrict access to unintelligible data packets. One could use cryptographic tools to provide data integrity, but the process of encrypting a plaintext message into ciphertext does not, in and of itself, provide anything other than data confidentiality.

1.2.4 This procedure includes an evaluation requirement for organisations and agencies where top secret security is not required. There are alternative methods to encrypt data via keys burned into hardware devices, which elevates the use of entrusting individual workstations with control of encryption keys. However, this procedure does not cover the specification relating to this.

1.2.5 There are restrictions by various governments, including the US, from exporting products employing encryption. This is intended to restrict the use of products that could facilitate making enemy nations’ communication undecipherable to intelligence agencies.

1.3 Risk Assessment in use of Encryption

1.3.1 The most critical aspect of encryption is the determination of what data should be encrypted and where and when it should be encrypted. The IS auditor should provide reasonable assurance, via a documented risk assessment or policy in written form, that the following managerial considerations are evaluated when employing encryption:

- The most critical aspect of a cryptography system is the evaluation and determination of what data are sensitive and should be encrypted. Certain data do not contain any recognisable or distinguishable data/information and may not be a candidate for encryption unless there is a unique business need. There should be a risk assessment performed to understand what data (or group of data) are sensitive and whether they should be encrypted. In addition, there are other vehicles to safeguard the confidentiality of information when the data are considered a critical asset. For example, a large hospital that constantly supplies medical information to an insurance company regarding individual patients represents a significant enough risk to warrant a virtual private network that allows point-to-point encryption. In summary, all data should be evaluated from a risk perspective for unauthorised viewing and the justifiable business need given the cost vs. benefit or risk reduction.
- The IS auditor should evaluate the potential paths used to transport data and who will eventually have access to the data. The IS auditor should understand that, with commonly accessible tools available today, data can be easily transported outside the organisation and sold to a competitor or violate privacy laws (HIPAA). These methods include, at a minimum, electronically through a firewall or by copying it to a CD and physically carrying it from the organisation’s premises. In addition, there is a likelihood that other software tools can be used to obtain data packets transported over the network that may contain sensitive information, such as passwords. Accordingly, the IS auditor should assume worst-case scenario when evaluating the encryption methods employed.
- Data can be encrypted in a central location or allowed to be in cleartext form within the central location and encrypted when transported to the end user. Determination of when and where it should be encrypted is critically important. The security over data is only as good as the weakest or nonexistent control to protect the data from unauthorised viewing.
- For example, the security over the keys and other sensitive information about type and employment of encryption should be limited to only those with a business need. Depending upon a current and strict business need, passwords and keys in themselves should be encrypted by security administration personnel with sole access to the key. All information pertaining to encryption should not be maintained in a development or test environment, but rather in the production environment where access is strictly limited. Another example is that the same encryption key used in the test environment should not be used in production.
- The IS auditor should ensure there is a policy regarding encryption that would include when the encryption should be applied, to what type and form of data, strength of encryption keys, method used to encrypt and changing of keys.

- Data encrypted in a central location, extracted and sent to the end user's workstation in encrypted form, where it is unencrypted, may be very secure at its source and then is transported. Conversely, the data maintained in an unencrypted form in the database and only encrypted when it is transported is another method. The second method appears to be less secure, given that inappropriate access can be achieved if there is a lack of compensating controls, but there could be the need for a trade-off between production processing needs with security. Specifically, if the data within the database or file is constantly updated (highly transactional) versus static (not changed), encryption at the central repository may not be suitable. While the IS auditor should not make a judgment on where and when data is encrypted, the IS auditor should investigate whether management has completely evaluated all the conditions to make the best decision possible.

1.3.2 There are multiple considerations that need to be made when evaluating the deployment of an encryption process. For example, when encrypting data, the use of a one-way or two-way hash is a common decision that needs to be made. The following are considerations that should be documented as part of management decisions.

- The one-way hash encrypts data and does not allow the data to be unencrypted. The encrypted data in the system is compared with data entered by the customer and then encrypted. If the two values equal, the data entered by the user is authenticated. One-way hash is typically used to encrypt passwords where the system administrator only has the authority to reset the password and not view it. One-way hash is ordinarily used for encrypting passwords for applications that are web enabled, which may be a more secured method than a two-way hash. One risk associated with this method is the inability to recover a large number of passwords for customers if the customer database is lost. Therefore, an organisation may have to notify all users to revalidate their personal credentials and receive a new password, which may result in negative public relations.
- Two-way hash allows encrypting and unencrypting data. The major risk associated with this method is that the encryption key may be inappropriately taken, and all sensitive data, including passwords, could be unencrypted. Conversely, encrypted data can be recovered quickly to avoid a public relation issue if the database is corrupted. Additional compensating controls are needed to ensure that the encryption key should be stronger, fully secured from internal access and changed more frequently.

1.3.3 The IS auditor should provide reasonable assurance that as much consideration as possible is given to the numerous managerial types of risks to the confidentiality of data prior to deployment. Simply put, not all encryption weaknesses are technical in nature, and the IS auditor should clearly evaluate the management decision-making process to verify that the most effective decision is made.

1.3.4 There are numerous third-party products used to transport data in an encrypted form. The selection process should be cognisant of need for use over multiple computing platforms (UNIX vs. Windows) to ensure consistency in its use. In addition, there are tools that automatically promote encryption, such as secured shell (ssh) in UNIX.

1.3.5 The IS auditor should understand the significance of compensating controls around data, including the evaluation of access points into the data. Finally, legal review of the responsibility and encryption methods should be completed and approved to ensure compliance with all legal requirements.

1.4 Three Primary Forms of Modern Ciphers

1.4.1 Symmetric key cryptography (sometimes referred to as secret key cryptography) uses the same key to encrypt and decrypt a message. Symmetric key ciphers are faster than asymmetric key ciphers, but the challenge of distributing the key as necessary, while keeping it secret from unauthorised parties has plagued cryptographers for centuries. Examples of modern symmetric key ciphers are DES, Blowfish, Twofish, CAST, IDEA, 3DES and AES.

1.4.2 Public key cryptography (asymmetric key cryptography) uses a pair of keys; a message encrypted with one key can only be decrypted with the other key in the pair. Users of a public key system make one of these keys publicly available and keep secret the other. When a sender wishes to send an encrypted message to a recipient, the sender looks up the recipient's public key and encrypts the plain text with that key. When the recipient receives the message encrypted with his public key, only he has the key to decrypt the message. Examples are Diffie-Hellman (DH) and Rivest-Shamir-Adelman (RSA). In addition, a message encrypted using the author's private key is considered "signed" by the owner of the private key. Everyone can decipher the message and read it using the author's public key, but only the owner of the private key can create or modify the message, thus ensuring its integrity and authenticity.

1.4.3 One-way hashes (one-way cryptography, message authentication codes (MAC) or message digests) encrypt data in a non-reversiible form. One-way hashes use the plaintext data as the key, rather than a separate piece of information, and produce a fixed-length digest or hash of this plaintext. Hash functions are known as one-way functions, as it is not possible to derive the plaintext from the hash. One-way hashes are often used to provide data integrity and to store passwords in an encrypted form on a computer. Examples are MD5 and SHA-1.

1.5 Common Applications of Encryption

1.5.1 Cryptography can be used to achieve the following assurance:

- Confidentiality—Ensuring that data can be viewed only by intended parties. The chief means for ensuring confidentiality of communicated data is through the use of symmetric algorithms, although asymmetric cryptography (also known as public key cryptography") is also used for lower volumes of data.
- Data integrity—Assurance that data has not been changed, that the data received was the same data sent. Data integrity can be provided by digital signatures and hash algorithms.
- User authentication—The means by which a user, server or entity is proven to be who they claim to be. Asymmetric cryptography can be used for authentication through testing knowledge of the secret key.

- Nonrepudiation—Assurance that a transaction or message has come from the person from which it purports and has not been changed. Nonrepudiation is a key requirement for electronic payments and commercial documentation. The sender will not be able to later refute that the message was sent by them. This proof must be sufficiently strong to stand up in law. Nonrepudiation may be achieved through a digital signature for short messages or more ordinarily through the use of a combination of MAC and digital signature.

1.5.2 Secure Sockets Layer/Transport Layer Security (SSL/TLS) is a means of encrypting network traffic, primarily HTTP (web) traffic over the Internet. SSL was developed by Netscape Communications Inc. and became a *de facto* standard in the industry. The Internet Engineering Task Force (IETF) has revised the standard, renaming it Transport Layer Security (TLS). The two terms are currently used interchangeably. SSL uses a combination of public key cryptography, symmetric key cryptography and one-way hashes to provide confidentiality, data integrity and authentication of the web server. Mutual authentication of the user and web server is also possible. For Internet communications, SSL is commonly used in conjunction with public key infrastructure.

1.5.3 Public key infrastructure (PKI) is a system for distributing public keys through digital certificates. A PKI is made of up of policies, procedures, hardware, software and personnel required to create, manage, store, distribute and revoke public key certificates. A PKI system validates that the public key distributed through the certificate belongs to the individual or organisation. Essentially, one obtains a digital certificate through a certificate authority (CA), such as Verisign or Thawte, containing one's public key. The CA digitally signs the certificate, thus validating the certificate, and thus the public key belongs to the alleged owner. Certificate authorities sell digital certificates for varying prices, depending on the type of certificate. An individual or organisation may have to present a form of authentication (such as an address or credit report), depending on the type of certificate.

1.5.4 Digital certificates are the primary delivery mechanism for certificate authorities to distribute public keys. Digital certificates include data about the owner of the key, the validity of the key and a copy of the public key. Digital certificates are signed by the certification authority.

1.5.5 Digital signatures are a means of authenticating the sender of a message. They also ensure message integrity and nonrepudiation. The sender takes an agreed-upon piece of data and encrypts it with his/her private key. If the recipient can decrypt this data with the sender's public key, then it could only have been encrypted with the sender's private key.

1.5.6 "Encryption technologies are solutions for access control. PKI-based solutions are popular to ensure authentication of users and to provide protection of business transactions. PKI stands for public key infrastructure and refers to the use of digital signatures, certificate authorities, and the related hardware and software to administer and manage the exchange of authorised, validated business information across an organisation or multiple organisations."[1]

1.5.7 This procedure does not aim to investigate the different approaches to the use of encryption technologies in various countries or to give opinion about systems or vendors. The checklists aim to provide the IS auditor with a framework to utilise when performing an audit, which involves checking the correct use of encryption techniques. It is not focused on a specific environment, such as e-commerce.

1.5.8 In some cases, it is possible to circumvent the need for encryption by using different techniques, such as a call-back procedure for originator authentication, but alternatives are often expensive and cumbersome. Encryption technologies are often cost effective. Audit/reviews must also focus on the processes management follows to identify data that are to be encrypted and the persons who will be granted access to this data. Assessments of encryption systems should include known vulnerabilities to provide reasonable assurance that the data are protected to the level required by management.

1.5.9 Encryption is built into many security products today. It is commonly seen in many different applications; for example, on the market, there is a popular DES-like algorithm with a 128-bit key length used for encrypting e-mail. When a secure web page is visited, the security offered is generally SSL (secure sockets layer), which offers a variety of encryption strengths depending upon the version of the browser.[2]

2. ENCRYPTION LEGISLATION/REGULATION

2.1 E-commerce

2.1.1 The development of electronic commerce is strictly connected to the use of cryptography as a reliable method for bringing order and security in the otherwise natural anarchy of the Internet.

2.2 Government Approaches to Encryption

2.2.1 The eagerness of most governments to guide the development of encryption technologies restricts the publishing and exportation of really strong encryption products, in the interest of their national security. Governments are typically adopting one of two approaches on encryption.

2.2.2 The European Union (EU) aims to reach a greater level of liberalisation of telecommunication and information services, including the use and trade of encoding devices and encryption methods. The EU is pressing members to harmonise national law with the directives of the community. European countries seem to be very sensitive about the needs of the free market and those of privacy, for example:

- France increased from 40 to 128 bits free use of cryptology from 40 to 128 bits, while looking to grant complete freedom of the use of cryptology.

[1] TechWeb Encyclopaedia

[2] Ouellette, Tim; "Encryption Quick Study," *Computerworld*, 25 January 1999

- Finland released a series of guidelines expressing their position on national cryptography policy. According to the guidelines, free trade of encryption products is supported, and the use of strong encryption should be not restricted by law or by international agreements.
- Ireland announced the key principles of its future legislative policy on cryptography. Users will have the right to access and choose strong and secure encryption products to safeguard their privacy in electronic commerce. The production, import and use of encryption technologies in Ireland will not be subject to any regulatory controls, other than obligations relating to lawful access. The export of cryptographic products will be regulated in accordance with the relevant EU Regulations on Export Controls for Dual-use Goods and Technologies and Conventional Arms.
- Spain issued a telecommunications law providing freedom of use of encryption software for telecommunications purposes.

2.2.3 Other governments, such as those in the US, Canada and the Russian Federation, are more concerned about national security, both in the field of foreign and domestic policy.

- The E-privacy Act (Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace) was introduced in the US but never adopted. The Act tried to ensure freedom to use encryption to protect the security, confidentiality and privacy of lawful communications and promote privacy and constitutional rights in a digital environment. In 2000, the US government published new encryption export regulations that made it much easier for companies and individuals in the US to widely export strong encryption in common products, regardless of their strength or the type of technology they use. HIPAA in the US mandates the use of encryption when transmitting protected health information.
- The pressure of technology vendors, end users and general public opinion may lead all governments to higher levels of liberalisation of the use of cryptology.

3. ENCRYPTION TECHNOLOGIES PROCEDURE

3.1 Communication Environment

3.1.1 Encryption technology is to be used in a communication environment when at least one of the following is true:

- No data can be arbitrarily added.
- The information passing through the network is confidential and must be protected.
- The requested service is granted only to allowed users.
- A user cannot deny receiving a specific message (addressee authentication).
- Every addressee is sure of the originator's identity (sender's authentication).
- It is required by regulation or considered to be industry best practice.

3.1.2 The following checklist covers specific topics:

Aspects of Encryption	Suggested Procedures Evaluation of Management Control Over Encryption Methodologies	√
Organisational management	Verify that written procedures/policies exist, including clear definition of roles and responsibilities for key management control measures, including key generation/creation; loading, including a controlled elevation process (to the production environment) for changes; transporting, storage; recovery; retirement/destruction; theft and frequency of required use. Included with these procedures should be requirements over securing the key and controlling the elevation of the key into the production processing environment.	
Organisational management continued	Ascertain if there is a clearly defined written procedure defining what data are considered sensitive, requiring encryption. In addition, ascertain if this procedure included requirements for when and how the encryption is to be applied. Specifically, determine if the encryption should be applied to data residing in static database or file form or only when transmitted over the Internet. In conjunction with the above, ascertain if a list has been made and approved of the data to be protected and its characteristics. Furthermore, determine if an estimate has been made of the financial value of each data item to be protected and of the costs of protection? Note: Consider the following in reviewing the list of information assets requiring full confidentiality via encryption. Data transmitted over the unsecured network (Internet) requires more security than a controlled database residing on an internal network segment that relies only specific static internal workstation IP addresses. In addition, verify that there is no duplication of encryption where data is encrypted in the database and then encrypted a second time during transmission, unless there is a risk assessment to validate the additional need for this. In summary, the IS auditor should verify that policies and procedures exist to determine what information is to be encrypted, the level of encryption and methods to determine who has access to decrypt the information. The IS auditor should communicate to the auditee that the success of encryption technologies is based on effective organisation, appropriately formalised.	

Aspects of Encryption	Suggested Procedures Evaluation of Management Control Over Encryption Methodologies	√
	Verify that management has instituted controls over the number of manual procedures and people involved in cryptographic system management, and at a minimum: • Dual control should be maintained on all keys that require physical handling. • The strength of cryptographic systems depends upon the secrecy of the keys. Ideally, no one should be allowed to handle encryption keys or see them. • Keys should be comprised of two separate key components and should only be known under the concepts of split knowledge and dual control. • Keys should be maintained on a computer that is not accessible by any programmers or users, such as router controls for logical access and strong physical controls with an air gap in a secured area/room.	
Design criteria of a cryptographic system	Verify that the process the enterprise uses to make its selection of an encryption algorithm is the most effective and efficient. In determining which is the best algorithm to choose, management should consider the environment where the cryptographic system is to operate: • Type of processing and transmission system to ensure satisfactory integration • Transmission paths, including compression requirements to ensure performance service levels • Users' and operators' skills and training to use the system and key • Integration with the operating environment to ensure communication is secure and reliable • Algorithm is effective with regards to the application and the objectives	
	Obtain and review documentation from management attesting that the chosen algorithm ensures all the protections at the desired level (according to the risk analysis) and is cost effective and convenient. For example, a stronger encryption system may be expensive and computer resource consuming and may not be necessary given the protection needed for internal organisation transmissions.	
	Verify that management has collaborated with other IT functions to ensure minimal effect on interfacing and other systems. When selecting such a cryptographic system, all of the major functional areas, such as systems programming and UNIX administration within IT, should be considered—along with data confidentiality and integrity needs—regarding the importance (and economic value) of data being protected. Verify the integration with system architecture. The encryption system should not interfere with normal operation affect the system architecture.	
	Obtain management documentation attesting to whether the chosen algorithm takes the deciphering cost by an authorised user to a sufficiently cost-prohibitive level. As computers become faster, new algorithms and longer keys are needed. The cost to decipher the encrypted message should not exceed the value of information itself.	
	Determine if management has applied respected standards in making the cryptographic system compatible with the applications. Standards exist for encryption systems, such as SSL, which ensure compatibility among various hardware/software platforms.	
	Ascertain if management has considered and respected all local and international laws and regulations (where applicable). Many countries have established laws and regulations to discipline the use of encryption technologies. Many vendors have operating rules as well.	
	Obtain from management and review documentation attesting that the system is strong and not attackable. Knowledge by the interceptor of encryption algorithms or hardware/software used does not impair reliability. It may be more effective to use a known and tested algorithm to generate the key, rather than to create an algorithm for the organisation. Security of good (strong) encryption systems does not depend on the secrecy of the algorithm, but only on the secrecy of the keys.	
Change control over the cryptographic system including key management	Verify, via audit testing, whether changes and updates to the cryptographic system are controlled and performed only by authorised individuals in accordance with existing written policies and procedures. Verify that key transmission is controlled according to a specific procedure. The risk of having a key disclosed is higher when the key has to be transmitted to the recipient(s). • Determine if the retirement of keys based on time is in accordance with policy or best industry standards. Incorrect or unnecessary changes and updates may impair the effectiveness of the cryptographic system. • Caution should be used when inputting keys into an application, as this presents security weaknesses. Specifically, keys should only be stored in tamper-resistant modules and never in clear text of programs or operating systems, where keys could become compromised without management's awareness. • Elevation of keys into production should occur by select security personnel and only during time periods where security over elevation is maintained. • Copies of keys should not be maintained within the testing environment or any environment accessible by programmers and users. • Verify that users and operators do not handle keys. Automatic key management systems can reduce the risk of disclosing an encryption key.	
	Verify that the key of the cryptographic system ensures all the required properties, including the length, composition and management of the key.	
	Ascertain if the key of the cryptographic system is easy to generate and modify, so the key can be changed expeditiously if suspected to have been compromised, as well as changed periodically based on requirements.	
	Ascertain that management employment of the key to access the cryptographic system (or the password to unlock its use) is not easily guessable.	
	Ascertain, via discussion with the security engineer or applicable auditee, that the key of a cryptographic system is easy to modify given the ease of use of the cryptographic system (algorithm). Given the risk of unauthorised viewing of data, there may be a requirement to change the key often.	

Aspects of Encryption	Suggested Procedures Evaluation of Management Control Over Encryption Methodologies	√
Digital Signature	Determine if management has instituted controls to verify that private keys are never backed up. By backing up a private key, exposure is increased. However, the public keys should be backed up to verify old signatures after expiration or revocation.	
	Ascertain if management uses different key pairs for encryption and digital certificates. Governmental units may require the private encryption key. However, verify, if applicable, that the governmental unit does not receive the key for the digital signature simultaneously.	
Validity conditions of a cryptographic algorithm	Ascertain if management has considered the need for the mathematical equations and formulas to be so complicated that they prevent its resolution by means of exhaustive, analytic and statistic attacks. Robustness is the propriety which, although the algorithm part of the clear text and its corresponding cipher text are known by the intruder, it is impossible to recover the whole text without using the encryption key.	
	Verify that management has taken into consideration, where mathematically less-complicated algorithms are used, that the cost and the time necessary to recover the message should be prohibitive, in terms of programming steps or computer memory utilisation. The cost of deciphering should exceed the value of the information the encryption system is supposed to protect.	

4. EFFECTIVE DATE

4.1 This procedure is effective for all information systems audits beginning 1 January 2005. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

APPENDIX

Reference

Piper, Fred; Simon Blake Wilson; John Mitchell; *Digital Signatures Security & Controls*, IT Governance Institute, USA, 1999

Business Application Change Control P10

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, 'IS audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met. During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.1 Linkage to COBIT

1.2.1 High-level control objectives AI2 (*acquire and maintain application software*) states, 'Control over the IT process of acquiring and maintaining application software that satisfies the business requirement to provide automated functions that effectively support the business process is enabled by the definition of specific statements of functional and operational requirements, and a phased implementation with clear deliverables and takes into consideration:
Functional testing and acceptance
Application controls and security requirements
Documentation requirements
Application software life cycle
Enterprise information architecture
System development life cycle methodology
User-machine interface
Package customisation'

1.2.2 High-level control objective AI3 (acquire and maintain technology infrastructure) states, 'Control over the IT process of acquiring and maintaining technology infrastructure that satisfies the business requirement to provide the appropriate platforms for supporting business applications is enabled by judicious hardware and software acquisition, standardising of software, assessment of hardware and software performance, and consistent system administration and takes into consideration:

- Compliance with technology infrastructure directions and standards
- Technology assessment
- Installation, maintenance and change controls
- Upgrade, conversion and migration plans
- Use of internal and external infrastructures and/or resources
- Supplier responsibilities and relationships
- Change management
- Total cost of ownership
- System software security'

1.2.3 High-level control objective AI6 (*manage changes*) states, 'Control over the IT process of managing changes that satisfies the business requirement to minimise the likelihood of disruption, unauthorised alterations and errors is enabled by a management system which provides for the analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure and takes into consideration:

- Identification of changes
- Categorisation, prioritisation and emergency procedures
- Impact assessment
- Change authorisation
- Release management
- Software distribution
- Use of automated tools
- Configuration management
- Business process redesign'

1.2.4 Detailed control objective P09 (*assess risks*) states, 'Control over the IT process of assessing risks that satisfies the business requirement of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors is enabled by the organisation engaging itself in IT risk identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks and takes into consideration:

- Risk management ownership and accountability
- Different kinds of IT risks (technology, security, continuity, regulatory, etc.)
- Defined and communicated risk tolerance profile
- Root cause analyses and risk brainstorming sessions
- Quantitative and/or qualitative risk measurement
- Risk assessment methodology
- Risk action plan
- Timely reassessment'

1.2.5 Detailed control objective P010 (*manage projects*) states, 'Control over the IT process of managing projects that satisfies the business requirement to set priorities and to deliver on time and within budget is enabled by the organisation identifying and prioritising projects in line with the operational plan and the adoption and application of sound project management techniques for each project undertaken and takes into consideration:

- Business management sponsorship for projects
- Program management
- Project management capabilities
- User involvement
- Task breakdown, milestone definition and phase approvals
- Allocation of responsibilities
- Rigorous tracking of milestones and deliverables
- Cost and manpower budgets, balancing internal and external resources
- Quality assurance plans and methods
- Program and project risk assessments
- Transition from development to operations'

1.2.6 Detailed control objective P011 (*manage quality*) states, 'Control over the IT process of managing projects that satisfies the business requirement to set priorities and to deliver on time and within budget is enabled by the organisation identifying and prioritising projects in line with the operational plan and the adoption and application of sound project management techniques for each project undertaken and takes into consideration:

- Business management sponsorship for projects
- Program management
- Project management capabilities
- User involvement
- Task breakdown, milestone definition and phase approvals
- Allocation of responsibilities
- Rigorous tracking of milestones and deliverables
- Cost and manpower budgets, balancing internal and external resources
- Quality assurance plans and methods
- Program and project risk assessments
- Transition from development to operations'

1.2.7 Detailed control objective DS1 (*define and manage service levels*) states, 'Control over the IT process of defining and managing service levels that satisfies the business requirement to establish a common understanding of the level of service required is enabled by the establishment of service-level agreements which formalise the performance criteria against which the quantity and quality of service will be measured and takes into consideration:

- Formal agreements
- Definition of responsibilities
- Response times and volumes
- Charging
- Integrity guarantees
- Non-disclosure agreements
- Customer satisfaction criteria
- Cost/benefit analysis of required service levels
- Monitoring and reporting'

1.3 CobiT Reference

1.3.1 Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT's control objectives and associated management practices

1.3.2 The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment. To meet the requirement, the selected and adapted processes in CobiT likely to be the most relevant are classified as:

- Primary:
  - PO1—*Define a strategic IT plan.*
  - PO5—*Manage the IT investment.*
  - PO9—*Assess risks.*
  - PO10—*Manage projects.*

- PO11—*Manage quality.*
- AI1—*Identify automated solutions.*
- AI2—*Acquire and maintain application software.*
- AI5—*Install and accredit systems.*
- AI6—*Manage changes.*
- DS1—*Define and manage service levels.*
- DS3—*Manage performance and capacity.*
- DS4—*Ensure continuous service.*
- DS5—*Ensure systems security.*
- DS9—*Manage the configuration.*
- DS10—*Manage problems and incidents.*
- M1—*Monitor the processes.*
- M2—*Assess internal control adequacy.*

- Secondary:
  - PO3—*Determine technological direction.*
  - PO6—*Communicate management aims and direction.*
  - DS7—*Educate and train users.*

1.3.3 The information criteria most relevant to change control are:

- Primary: effectiveness and efficiency
- Secondary: reliability, availability, compliance, integrity and confidentiality

1.4 Purpose of the Procedure

1.4.1 Primarily intended for IS auditors—internal as well as external auditors—this document can be used by other IS professionals with responsibilities in the capacity of information systems availability, data integrity and information confidentiality.

1.4.2 Modern businesses are organised as a set of core processes. Almost every organisation in the world is faced with increasing pressure for effectiveness and efficiency (i.e., higher quality requirements for products and services, increased revenue, cost reduction, new product development), a pressure for better, faster and cheaper software change control processes that provide high-quality software for the business owners.

1.4.2 As with all IT audits, not all testing steps defined in this procedure would be applicable due to the level of risk associated with the individual development project under review. The cost and level of effort associated with each testing step should be continually evaluated to provide reasonable assurance that there is a value add to the enterprise in ascertaining if the control is operating effectively. Based on a decision by audit management responsible for the engagement that is subject to a risk assessment, controls mitigating risks considered to be immaterial or insignificant typically may not be tested as denoted in this procedure. Accordingly, it is recommended that a risk assessment be performed to evaluate which controls should be tested and which of the audit steps defined in this procedure are applicable.

1.4.3 Due to the voluminous testing steps defined in this procedure, the IT audit management should consider adopting the five steps utilised in the Project Management Institute's (PMI's) project management approach to effectively plan and execute the audit.

2. SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)

2.1 Overall Purpose

2.1.1 The purpose of an SDLC audit is to assess the extent to which the acquired or developed system(s) fully meets the deliverables identified in the project request approved by management, assess the extent to which the actual costs of acquired or developed system(s) are in line with budget, and report to executive management and/or the audit committee of the board of directors as to whether the project accomplishes the identified deliverables and is within costs.

2.1.2 Internal audit department's (IAD's) overall objectives when performing an SDLC audit are to assess whether:

- Business processes and systems are designed and implemented with adequate internal controls
- Project management is adequate to provide reasonable assurance that project objectives are achieved
- Budgetary estimates are realised
- Required business functionality is achieved
- The project team is using a controlled and structured approach for monitoring system development activity, system quality and adherence to organisation policies

2.1.3 A detailed process has been developed to assist the SDLC team in providing the following for each phase of the system development:

- Timely identification of control issues (system, business, methodology or project management)
- Proactive participation in assessing the internal control structure throughout the project life cycle
- Improved future audit coverage due to increased knowledge of the business processes and functions

2.2 SDLC Phases

2.2.1 The SDLC phase objectives will utilise specific audit programs for each development phase of the system development life cycle. In addition, a general project methodology framework audit program covering all phases of the project life cycle will be used. Major phases of an SDLC audit typically include:

- Business requirements definition
- Project initiation
- Design and development (construction)
- Testing
- Implementation
- Post implementation

2.2.2 However, given the development mechanism, including user interface (UI) design, additional control processes may be required and included in the scope of the review. In conjunction with this process, the IS auditor should test the adequacy of co-ordination between the UI design and the application codes throughout the SDLC process.

2.2.3 The names of the phases may vary by SDLC methodology; however, the critical objectives and deliverables are consistent. In addition, the phases of a system development project may run concurrently and the break points are not always clear. Therefore, the completion of specific phase deliverables may run into subsequent phases.

3. NONESTABLISHED OR NONADHERENCE TO KEY CONTROL RISKS

3.1 Examples

3.1.1 The examples in 3.2 are not all inclusive. This information is provided to highlight the risk of not establishing controls.

3.2 General and Project Management

3.2.1 Key required deliverable documentation (including functional requirements definition, technical specification, design, development, testing, elevation documentation) should be approved by the business owner to establish accountability of the software change and the resources expended for the change. Without this approval, there is the risk that IT and the business owners may not be in agreement with the work performed and final outcome.

3.2.2 The project or IT manager should call a cross-functional meeting with other IT areas and business owners to evaluate the effect of the software change. There should be minutes to these meetings, and the effects should be injected in the requirements and design. Without this impact assessment, other business units may be negatively affected or a loss of design efficiencies may result.

3.2.3 Due to the ability to modularise (separate) software development efforts, acceleration of various components through the various gates (design versus development) can result. While this may not pose a risk, there is often the need to create issue or problem lists that may not contain consequential problems that could result in delaying the progression of work. This list should be approved by all parties from software developers to the business owner to high-level management within the development group.

4. SDLC METHODOLOGY

4.1 Business Requirements Definition

4.1.1 Requirements for the business owner either to create or fully review with a formal sign-off are denoted in 3.2.1. Without this control, business units may disagree with the requirements of the project/request—IT may not build functionality that is needed by the business unit.

4.2 Project Initiation

4.2.1 All projects/requests relating to business applications must be initiated from the business area, which includes software defects and enhancements. The scope of and estimated resources needed for this project should be defined and/or agreed to by the business area. If this control does not exist, IT may update, change and implement new functionality without the business unit's knowledge.

4.2.2 The problem/help desk determines the severity of the open issue, based on discussions with the business owners, and routes accordingly. If problem tickets (problem issues) are not appropriately prioritised and routed, IT resources for software changes or maintenance may not be effectively applied.

4.2.3 IT must use a tracking system to track all projects/requests from the business owner. Help desk tickets and version control references must be cross-referenced. If this control does not exist, project initiation may not be recorded appropriately and may not be visible to the IT management.

4.2.4 Given the size and complexity of the change, the project or IT manager should decide what documentation to produce. If this control is not in place, too little or too much (that is not cost effective for a small project less than 30 hours to design and develop), documentation regarding evidencing adherence to controls may be required.

4.3 Design and Development (Construction)

4.3.1 Determine that proper access security has been put in for the functionality, including having the business owner identify roles that can access this new functionality. If security is not considered and it is applicable, inappropriate access to view and change business information may occur.

4.3.2 Determine that version control is in place. If version control is not in place, there is increased risk that a new module/functionality could be built in the production environment without the knowledge of IT management and/or overwriting

of code or lack of baseline management.

4.3.3 Determine that written authorisation from business users, the requestor and other affected areas is received prior to implementation. If this does not occur, there is increased risk that implementation of the new and/or in inappropriate code may occur without knowledge of all stakeholders within the project/request.

4.4 Testing

4.4.1 Business users or their assigned designees, who are outside the application development group, should review test conditions and the test plan to ensure that there is proper coverage within the overall testing cycle. In addition, depending on the size and complexity of the requirements, a cross-reference or traceability matrix should be employed. A traceability matrix should match the requirements to the test cases, including use cases. Without the proper review of the test conditions and, if be missed in testing.

4.4.2 Business users should review test results (e.g., user acceptance testing) to verify that this is what they wanted. Without a complete review and sign off of the test results from the business users (or their representatives outside of the IT application development group), there is no true validation/confirmation of the testing, resulting in the project/request not being satisfied.

4.4.3 The application developer's IT manager (or appropriate supervisory personnel of the programmer) should review and approve the code (changes) to be moved into production. If this control is not in place, IT management may not be aware of the request for new functionality to be moved into production. Note: This control should not be relied upon to detect fraud.

4.5 Implementation

4.5.1 In addition, application developers should not be able to promote code into production. If this control does not exist, unauthorised changes to software could result. In addition, uncontrolled and/or unauthorised changes to business information may lead to fraud and irregularities. Finally, malicious programs can be introduced into the production environment, affecting system availability, data integrity and information confidentiality issues.

4.6 Post-implementation

4.6.1 Problem/help desk tickets should be closed on a timely basis with root cause and method of resolution documented. If this control is not implemented, repetitive problems could occur without identifying the need for software changes and/or the perception that the problem on the ticket is still open.

4.6.2 Other activities could include review to determine if objectives are achieved and review of the application of key internal business controls and rules for the application.

5. PRODUCTION PROCESSING AFFECTING SDLC

5.1 Emergency Change Process

5.1.1 Unplanned and emergency change subprocesses collectively control the means and methods for exceptions to the standard change control process. The unplanned change subprocess controls changes caused by a missed lead time and/or missed goal calendar. The emergency change subprocess establishes the controls around the means and methods used in remediation of system outages directly affecting customer service levels. Accordingly, an emergency change is an application program modification within 24 hours to prevent or avoid reoccurrence of any significant outage.

5.1.2 The emergency change process should be closely managed so there is an approval to bypass the standard change process. Activities occurring during the emergency change are logged and reviewed by management with application development and security services groups (e.g., due to the powerful user IDs granted to the programmer to complete the emergency change for resumption of system availability). Upon resumption of the system by the business user, the following steps should be taken:

- Remove the programmer's access to the production environment.
- Complete a full post mortem with root cause analysis.
- Perform full regression testing to ascertain if the emergency program fix affected other system elements (database, interfacing applications, other applications within the same suite where the change occurred, etc.).
- Verify that the programming fix is executed from a controlled program library that is backed up and retained with source code for a required period of time based on the business and legislative risk of the change.
- Include the program change, if permanent, into the baseline software version to provide reasonable assurance that changes are not overwritten in the succeeding program modifications.

5.2 Problem Management Subprocess

5.2.1 The problem management subprocess provides a guided, systematic and controlled approach to managing problems affecting IT services during an application modification. The process includes all tasks necessary for managing problems throughout the life cycle. These tasks include planning, testing, implementing and recovery procedures during restoration of service in the event of a failure. The goal of this control is to minimise or eliminate repeat problems affecting customer service. The output of this process typically includes the emergency and unplanned change subprocess. This process should be examined in detail, including whether:

- Accountability is established where specific management is assigned the problem and each system has its own problem queue
- Emergency changes are first fully documented in this subprocess
- Certain requests associated with customer complaints are first documented and evaluated within this process before a formal system modification request is submitted
- Resolution, including post mortem performed on problem changes, is fully documented, includes a root cause analysis, and the means and methods of correcting the problem in a timely manner

- Problem tickets are closed by the manager responsible for resolution/system

5.3 One-time Run Programs

5.3.1 From time to time, programs are created and executed once based on a specific and unique business. For example, the need for these programs may include specific data management services. These programs should be subject to the same level of rigor, based on the risk of the program and on the integrity of the data and system availability, within the change process of any other program creation or modification. See section 7.3, Application of Controls Defined Within the Testing Program, for further refinement and application of these controls based on a risk assessment.

5.4 Critical Control Over the Production Processing Environment

5.4.1 A strong change control process may be instituted. However, the IS auditor should consider taking additional steps to make sure it is followed (e.g., programmers cannot bypass this process all together). The following are considerations for the IS auditor to validate compliance with the change control process, not just for large IS projects.

5.5 Detective Control

5.5.1 Despite all of the above controls, programmers are sufficiently knowledgeable enough to find ways to execute programs in the production processing environment outside or around the change control process. Accordingly, it is recommended that the computer operations or some independent group outside of the application development group monitor activities in the production processing environment to detect the execution of programs (e.g., jobs) by programmers (e.g., jobs where the user IDs that initiated them belong to a programmer). It is recommended that this detective control be instituted to protect the integrity of information.

5.6 Preventative Control

5.6.1 The IS auditor should review access to the production data files and databases to ascertain if update access is available to the programmers. In addition, there should be no compilers in the production environment, no access to source code in the production environment, and restricted access over application developers to source code checkout.

5.6.2 Depending on the organisation, “read” access to generate business- and system-related reports might be an acceptable risk, if production service or computer operations preapprove these activities. However, strong preventive controls would prohibit the execution of programs in the production processing environment outside a job scheduler or some automated means that controls program execution (e.g., business programs are not typically started manually by a computer operator). The review of the creation of program execution setup within of the job scheduler (e.g., programs executed) should be the final step in auditing the change process, including verifying that all changes to the job scheduler are approved by production services/computer operations management.

5.7 Risks Associated With a Poor SDLC Process

5.7.1 Controls are applicable given the size of the IT group and organisation and the size and complexity of the individual changes. Accordingly, there is a need to create and adhere to a decision matrix where various controls are correlated to specific type of changes (e.g., strategic or large, small, tactical or emergency changes). This decision matrix should be approved by senior management of the organisation as this will provide the level of controls commensurate with the **acceptable** level of **business** risks from program changes.

5.7.2 A periodic review (IT self-assessment) of the SDLC is required to examine if the process is being followed or needs to be updated. If this control is not in place where the SDLC is updated continuously to seek process improvements for developing and implementation solutions, the IT group may not follow it or may not be efficient and effective in controlling risks.

6. RECORDS

6.1 Keeping Records

6.1.1 Records should be in sufficient detail to support the findings and conclusions reached as a result of the audit.

6.1.2 The retention of audit evidence supporting adherence to the change control process should be based on various factors, including the:

- Volume of information and associated cost of archiving it
- Regulatory requirements
- Importance of the change to the overall business needs
- Need for project documentation for later review to refine the SDLC process and manage personnel performance

7. SPECIAL SDLC REVIEWS

7.1 Scope of Reviews That Are Not Included in This Procedure

7.1.1 Due to the unique nature of various software changes and the associated technical requirements, specialised SDLC review requirements, including identification of specific elements within the change process, are not included in this procedure. For example, the following area of software and hardware may be considered unique though a large portion of the following controls may be applicable:

- Web applications SDLC (e.g., for vulnerabilities such as cross-site scripting or SQL injection)
- Software source code reviews (e.g., review software for malicious or fraud code)
- Business software for specialised technical systems (EFT systems)

Business Application Change Control P10 cont.

7.2 Testing Agreement

7.2.1 There should be agreement on the type of change control testing to be carried out. This agreement may be based on or driven by common problems with software, such as the lack of adequate quality assurance or testing resulting in business disruptions, collectively with the cost/benefit of the change control process.

7.3 Application of Controls Defined Within the Testing Program

7.3.1 It is imperative for the IS auditor to balance the size of the project (level of effort needed) required completion timeline and criticality of the change with the appropriate level of controls to be applied in the process. Therefore, not all of the following suggested procedures may be applicable to all software changes, especially if the project is small. However, these controls should be discussed and evaluated with management to verify the associated risk of not having these controls in place.

8. CHANGE CONTROL TESTING PROGRAM

	Suggested Change Control Testing Procedures	√
Planning and Administration Planning and Administration continued	Define the scope based on the nature, timing and extent of the evaluation. A formal risk assessment from a business and regulatory perspective should be performed on the various software changes. Sample selection should be based strictly on risk values, which includes business environment, regulatory requirements, cost, benefits, IT environment effects, etc.	
	Not all key controls apply to all software changes. Specifically, the size of the software changes may affect the level of rigor of documentation needed to evidence the quality review process. Create a decision matrix to identify the conditions where creation of documentation is required. The size of the organisation and complexity of the change may dictate the level of controls. However, the overall process must have adequate controls relating to segregation of duties and full testing prior to elevation of programs to the production processing environment.	
	Ascertain if documentation is created that includes all outstanding problems/issues among the various SDLC phases. Verify that this listing of outstanding problems (e.g., punch list) is approved by senior IS management prior to moving to the next phase.	
	Include in engagement memorandum that this audit should not be relied upon to detect fraud, including malicious code, due to the exhaustive nature of a code review that may be required for many thousands of line of code could be cost-prohibitive unless the engagement specifically addresses this risk.	
Skills Required	Understand the design, development, testing documentation, standards, means and methods used by IS personnel. The IS auditor should be provided sufficient training and guidance by audit management to achieve this.	
	Collaborate with the IS staff in evaluating specific information, including terminology and specific means and methods of achieving the control objectives.	
Project Method-ology Framework	The overall objective is for the organisation to establish a general project management framework to manage a project throughout the project's life cycle. This framework should include, at minimum, the allocation of responsibilities, task breakdown, budgeting of time and resources, milestones, checkpoints, and approvals. Determine that a project management methodology framework is established for managing and monitoring the project. This framework should include, at minimum, the project scope, the allocation of responsibilities, task breakdown, time and resource budgeting, milestones, checkpoints, and approvals. Discuss project methodology with project manager and ascertain what SDLC methodology is being followed. If management has approved an SDLC methodology and policy requires use of the methodology, is this SDLC methodology being followed? If not, determine the reasons for not using the approved methodology.	
	Validate that the methodology being followed includes the following items: ■ Documentation of project scope and boundaries ■ Allocation of responsibilities ■ Task breakdown ■ Time and resource budgeting ■ Project milestones ■ Checkpoints ■ An approval process ■ Risk assessment and mitigation procedures ■ Communication management	
	Business management (stakeholders/project sponsors) actively participates in the system development life cycle. Verify that business management: ■ Reviewed and approved the business requirements and project scope ■ Approved and is actively monitoring the project budget ■ Receives project status minutes and/or participates in project status updates ■ Is actively involved in critical problem resolution	

	Suggested Change Control Testing Procedures	√
Project Method-ology Framework (continued)	A project master plan is created to maintain control over the project throughout its life. Determine that: ■ A project master plan has been documented ■ The project plan is consistent with the cost-benefit analysis, time estimates and project deliverables ■ Management has approved the project plan ■ The project manager periodically updates the plan to reflect changes in the project by obtaining copies of the project plan at different points in the project ■ The plan includes those items referenced in the above methodology and the following: Completion criteria and benchmarks Critical path interdependencies Anticipated start and completion dates for each task Individuals assigned to each task	
	A methodology is implemented to monitor costs incurred during the project. Determine that: ■ A process has been implemented to monitor costs incurred during the life of the project. This process includes: Procedures to capture all project expenses A method to compare actual cost vs. planned costs ■ This process includes: Procedures to capture all project expenses A method to compare actual cost vs. planned costs	
	The basis for assigning members to the project ensures all affected areas have representation and the project team has an adequate knowledge base. In addition, the responsibilities and authorities of the project team members are defined. Determine: ■ What criteria management followed to appoint members to the project team to ensure the project team has an appropriate level of technical and business expertise. If the appropriate level of expertise does not reside in-house, what provisions are being made for training and/or obtaining expertise? ■ If the project team includes representatives from the areas affected by the project ■ Whether the project plan clearly specifies the roles and responsibilities of each individual project team member ■ If individual team members understand their roles and responsibilities ■ Vendor or third-party roles and responsibilities are clearly defined, if applicable	
	Management representatives from both the business side and the IT areas are designated to approve the results of each phase prior to continuing work to the next phase. Determine: ■ If representatives from the affected area have been designated to sign off on deliverables ■ Whether the project plan contains provisions for approval of deliverables by the designated business, quality assurance (QA) and IT personnel	
	Quality assurance steps should be integrated into the project master plan and formally reviewed and agreed to by all parties. Assurance tasks support system accreditation and should assure that internal controls and security features meet related requirements. Determine that: ■ QA steps have been integrated into the project plan by reviewing the project plan ■ The quality assurance process includes steps to review the project deliverables at strategic points of the development to provide reasonable assurance that the end results will meet or exceed: – Business requirements – Legal requirements – Organisation standards – Security standards – Internal control requirements – Reliability requirements – Performance standards ■ The QA plan includes provisions for: Issue tracking and logging Change/defect tracking and logging Development of a master test strategy	
Project Method-ology Framework (continued)	Formal project risk management should be established to identify, eliminate or minimise risks associated with the project. Determine: ■ Whether the project team has identified and documented risks associated with the project ■ Whether there has been a review of project status reports for adherence to risk management process and issues management ■ What steps have been taken to mitigate known project risks by interviewing the project manager ■ Whether risks have been clearly communicated to management	

	Suggested Change Control Testing Procedures	√
	A process should be in place to provide reliable and timely reporting on the project status to management. This reporting mechanism should also include reporting of discrepancies from plan and problems encountered. Determine: ■ How project status is assessed. Based upon the IS auditor's knowledge of the project, review the status reports and/or attend status meetings to determine if this assessment mechanism is adequate to give an accurate status of the project to management. Verify that discrepancies from plan and problems are also reported. ■ The method and the timing of project status reporting to management. Is the reporting mechanism adequate to provide management with reliable and timely information? ■ Whether there are thorough interviews, whether management receives and reviews status reports and/or attends status meetings and follows up on action items, and whether the reporting mechanism used by the project team provides them with adequate information ■ Whether changes in the project plan and/or discrepancies from the plan are reported and whether management is involved in problem resolution	
	Processes should be established to ensure close co-ordination and communication among all parties involved in the project. Determine: ■ If all members of the project team are involved in project meetings at the appropriate level and whether representatives from IT, QA and business areas attend the project meetings ■ What formal communication channels have been developed. Through discussions with the team members, determine if the communications appear to be timely and effective. ■ If project documentation is maintained and available to all appropriate individuals. Verify that only authorised individuals have the ability to modify this documentation. ■ Whether the following documentation (as appropriate) is available: – Project scope and deliverables – Cost benefit and feasibility studies – Risk analysis – Project organisation chart – Project status – Project plan – User requirements – Design specifications – Issues log and resolutions – Test strategy – Conversion approach – Implementation plan – Training plan – Post-implementation review ■ If the project team is dealing with a vendor or other third party, communication channels have been implemented to provide reasonable assurance that communications between the third party and the project team are effective.	
	A process should be established to identify and report issues for corrective action. Determine: ■ If procedures exist to identify, measure and correct issues/problems ■ What mechanism is in place to provide reasonable assurance that issues are resolved in a timely manner by the appropriate person ■ If a mechanism exists to escalate critical issues to management in a timely manner ■ Whether management reviews and approves solutions to issues/problems	
	Determine that all exceptions are documented and reported to management for corrective action. Documentation of remediation should be included in the audit workpapers.	
Project Initiation (Request and Approval)	The overall objective is that the organisation should utilise a methodology to identify and prioritise projects in line with the operational plan. Determine that the methodology used includes a process to evaluate the business requirements, project costs, potential risks and projected benefits. In addition, the listing of software change requests should be centralised and should highlight their sources, including business owner from additional strategic functionality, help desk (e.g., problem tickets), tactical enhancement (day-to-day minor changes), etc.	
Project Initiation (Request and	Representatives from affected business areas and IT areas should participate in the definition and authorisation of a project. Determine if: ■ The team established to evaluate the project includes representatives from all affected business areas and IT areas ■ These representatives have the required business knowledge and/or technical knowledge to perform this assessment. Determine if subject matter experts are used to supplement team knowledge when necessary.	

	Suggested Change Control Testing Procedures	√
Approval) (continued)	The nature and scope of the project should be clearly defined in writing for management approval before the project is initiated to help ensure that the project meets business requirements and strategic direction. Determine whether: ■ The project request came from an authorised source and the request is consistent with the business strategic direction ■ High-level business and operational requirements (e.g., availability expectations) have been defined for the project, including: – Expected benefits and/or business rationale – High-level business requirements – Identification of business areas and systems expected to be affected by the project – Expected customer base – System availability considerations – Expected system volume – Expected response time – Recovery expectations – Usability requirements – Legal and other compliance requirements ■ The project scope is clearly defined and the project scope documentation defines the project boundaries and specifically defines what should be included in the project and what should not be included. ■ Project requirements have been evaluated to provide reasonable assurance that they support the strategic direction of the business unit as well as the strategic direction of the company.	
	Alternate solutions satisfying the business requirements should be identified to help ensure that the optimal solution is selected. Determine if: ■ A process was followed to provide reasonable assurance that all possible solutions to the business problem were identified for consideration ■ The following solutions have been considered: – Enhancements to the current system – Manual solutions and/or workarounds – Vendor solutions – In-house design and development ■ Each solution has been evaluated for how well it might support the business requirements ■ Conclusions about each of the identified solutions have been documented and if those selected for further research and analysis are identified	
Project Initiation (Request and Approval) (continued)	The feasibility of each alternative should be evaluated as a basis for the decision to proceed with the project. Determine if: ■ A feasibility analysis was performed on each proposed solution and the results of this study were documented for management ■ The feasibility study included the availability of critical personnel, including: – Business personnel – QA personnel – Technically proficient development staff ■ The time frame required to implement the solution is within the time frame specified by the project requirements ■ The software and hardware have been analysed to provide reasonable assurance of the following: – Current technology will support the project. – The organisation will support the technology. – The technology is in line with the organisation's technical strategy and architecture.	

	Suggested Change Control Testing Procedures	√
	The costs and benefits associated with each alternative should be evaluated as a basis for the decision to proceed with the project. The costs and benefits should be examined in monetary and non-monetary terms. The monetary cost savings and benefits should be measurable, attainable and verifiable. Determine whether: ■ A cost-benefit analysis has been performed on each proposed solution and that the results have been documented for management ■ The cost benefit analysis includes all direct, indirect, declining and reoccurring costs: – Labor costs, including infrastructure and operations personnel, doing-business-as (DBAs), developers, QA and business personnel assigned to the project – Annual license and contract fees – Costs associated with the installation of upgrades to maintain hardware and software at current levels and/or performance of system maintenance over the life of the system – Hardware costs (including depreciation) – Training ■ The cost-benefit analysis includes benefits of the project, including: – Time savings – Labor savings – Hardware and/or operational savings – Anticipated increases in income due to business benefits (i.e., new business, increased customer base) ■ Observe the computed ROI and payback for this initiative to determine whether the costs and benefits identified appear reasonable, measurable and attainable. Determine if the calculations appear reasonable. Has the cost-benefit been projected over the realistic life of the system (i.e., five years) and does it include technology obsolescence?	
	Risk management is performed to identify, eliminate or minimise risks associated with the project. Determine if: ■ A risk assessment was completed for each possible alternative and if project assumptions and project risks have been documented and communicated to management ■ Management has developed possible solutions to mitigate known risks	
	The project should be approved and endorsed by an appropriate level of management to ensure that resources are allocated to the project. Determine if management has: ■ Reviewed the project documentation and understands the scope, feasibility, cost benefit and risk of the project ■ Approved the budget for the project and if this approval contains checkpoints for re-evaluation as the project progresses ■ Taken ownership and accountability for this project	
	Determine whether all exceptions are documented and reported to management for corrective action. Documentation of remediation should be included in the audit workpapers.	
Business Requirements Definition	The overall objective is that the organisation should utilise a methodology that ensures business requirements are defined and documented to support overall project objectives.	
	Appropriate personnel should participate in developing business requirements. Verify whether: ■ All business areas affected by the project are involved in defining business requirements ■ Personnel have an adequate knowledge base to define the business requirements	
	Business requirements are clearly documented and are accurate, complete and current. Verify whether: ■ The project team has addressed all business requirements. ■ The project or IT manager has called a cross-functional meeting with other IT areas and business owners to evaluate the effect of the software change to their functional duties. There should be minutes to these meetings and the effects should be injected in the requirements and design. Without this requirement/control, other business units may be negatively affected or loss design efficiencies can result. ■ Business requirements have been documented and include: – Functional/technical process requirements – Legal requirements – Security requirements – Interface requirements – Timing and response time requirements – Reporting requirements – Input requirements – Audit requirements ■ The project team has ensured that the final business requirements are communicated to users and management ■ Business risks have been identified and addressed in the business requirements	
Business Requirements Definition (continued)	Problem management issues should be identified, logged and resolved. Determine: ■ What method is used to capture and log issues identified during business requirements development ■ Whether issues have been analysed and resolved	

	Suggested Change Control Testing Procedures	√
	A methodology should be used to ensure that all potential vendor products are considered and evaluated against the business requirements. Determine: ■ Whether a method of assessing the potential vendors and products has been developed ■ What analysis of vendor financial stability was done ■ How customer satisfaction with vendors was assessed ■ Whether the request for proposal (RFP) process was logical and based on product, price, technical platform, reliability, vendor reputation and conformance to business requirements ■ Whether vendor responses to the RFP were evaluated against common criteria (i.e., the business requirements)	
	Vendor relationship and contracts should be appropriately managed. Verify whether: ■ The vendor contracts have been reviewed by legal ■ Contracts with third parties were reviewed and approved by the vendor and business management ■ The contract includes the following: – Specific measurable deliverables – Payment schedules – Penalties for late delivery or non-delivery of product – Specific responsibilities for technical and user documentation and training – Definitions of modifications to be made to the software, if any – Clear delineation of change management criteria – Definition of what is included in the scope of contract and what is outside of the contract – Specifications of what activities or work are subject to additional charges beyond the contract, and how those charges will be billed (flat rate, time and materials, etc.) – System maintenance obligations, update frequency and payment fees ■ The contract provides for source code escrow An appropriate confidentiality agreement is included A formal review and sign off of business requirements should be performed. Determine whether: ■ The formal review occurred and results were documented ■ Participants in the formal review process represent all facets of the business area, such that all business requirements can be fairly assessed	
	Review the IT strategy/policies to understand the objectives of software change (i.e., in-house development, third-party solutions, best of breed, no customisations) to provide reasonable assurance that the audit is focused appropriately and the IS auditor is looking for the right controls.	
	Determine whether all exceptions are documented and reported to management for corrective action. Documentation of remediation should be included in the audit workpapers.	
System Design and Develop-ment	The overall objective is that the system design is fully defined and documented, and final specifications are reviewed and approved prior to full-scale development to provide reasonable assurance that the specifications meet the user requirements. *Note*: It is suggested that a team consisting of both IT and business internal auditors complete this section. The auditors should identify business risks inherent to the application being designed. The system design documentation should be reviewed to provide reasonable assurance that controls to address these risks have been designed during this phase.	
System Design and Develop-ment (continued)	A process should be implemented to ensure that design specifications are documented in sufficient detail to ensure that they are adequately communicated to the developers. Determine: ■ If design specifications are thoroughly documented. Detail specifications should include, but are not limited to: – System security requirements – System flow diagrams – System hardware specifications and design requirements – Screen specifications (including screen edits and security scenarios) – Interface definitions (including completeness and edit checks) – Files/database design – System update, calculations and processing requirements – Historical data storage and conversion – Report specifications (including frequency and print location) – Source document requirements – Program specifications – Internal and external system interfaces – System/application audit requirements ■ Whether manual procedures are designed and documented in conjunction with the system design to provide reasonable assurance that: – Adequate segregation of duties can be maintained – Adequate approval processes are developed – Error correction procedures are designed – System balancing procedures are developed	

	Suggested Change Control Testing Procedures	√
System Design and Develop-ment (continued)	Appropriate personnel should be involved in the design specification process. Determine whether: ■ Personnel involved in design specifications have an adequate knowledge base and disciplines (i.e., business subject matter expert, database administrator, network technician) ■ A representative from each area affected by the system is included during the design process	
	A process should be implemented to identify, record and resolve issues that arise during detail design. Determine: ■ Whether a process has been implemented to track issues arising during detail design ■ Whether the appropriate people are involved in issue resolution ■ Whether resolutions are documented and appropriately communicated to the entire team, especially program developers who must implement changes ■ If the resolution is reviewed to provide reasonable assurance that business needs are still met and resolutions are within project scope	
	A procedure for managing source documents should be designed. Determine if: ■ The source document management design includes: – Retention technology – Retention practices – The ability to retrieve source information – A process to verify completeness and accuracy ■ The process designed to receive, approve and input source document information provides an adequate segregation of duties ■ The source documentation handling process, as currently designed, complies with legal requirements	
	Manually entered data methods should be defined, documented and validated. Determine whether: ■ Input specifications include edits on input data ■ Procedures have been designed to detect, report and/or correct errors ■ The project team has developed a standard for screen presentation, to provide reasonable assurance that: – The same look and feel throughout the system – Common functionality, such as consistent organisation logo/branding, function keys, page up/page down methods and scrolling – Screens have been reviewed for usability and “user friendliness” ■ Online user help has been included in the system design	
	Processing requirements for system interfaces (both input and output) should be defined and documented. Determine whether: ■ Rules/procedures are documented to balance and reconcile results from one program/job/interface to the next ■ If system design includes modifications to existing systems/interfaces, these modifications are reviewed and approved by the appropriate people from those systems affected by the new system ■ Policies and procedures have been designed for problem escalation and resolution of interface failure	
	Data definitions and requirements should be defined and documented. Determine: ■ Whether project specifications include information on file formats, data dictionaries and data flow diagrams ■ Whether the following have been defined for each file/database included: – Data storage requirements – Back-up strategy – Security requirements ■ If a database expert is needed/required. Verify with the database administrator that the overall database design has been evaluated for data redundancy and data integrity. ■ If data conversion is anticipated and if a conversion strategy has been designed, documented and includes: – A review of the data in the source system to they are complete and accurate – A process for management to verify that electronically converted information is complete and accurate, utilising edit checks, referential integrity checks, record counts and hash totals – A process for management to verify that data are complete and accurate, if the new system data will be entered manually ■ If the application is a vendor package that requires the entry of data-specific parameters to control the functions of the software, whether the selected parameters have been documented	
	Processing, updating and maintaining standing data should be defined and documented. Verify whether: ■ Business rules, requirements and workflows have been defined ■ Detail program specifications have been developed and agree with the business specifications ■ Balancing procedures have been designed to provide reasonable assurance that standing data are maintained correctly (i.e., Internal balancing routines) ■ Business owner signs off on standing data reports to ensure that they are complete	

	Suggested Change Control Testing Procedures	√
System Design and Develop-ment (continued)	Business output requirements should be defined and documented. Determine whether: ■ Design specifications include documentation of output files and formats, reports, and documents (i.e., checks or organisation statements). Verify whether the following have been addressed: – Output frequency – Security over output – Printing location and distribution ■ Rules to balance/reconcile output results have been defined ■ Procedures to recognise, monitor, report and correct error/problems have been defined	
	System architecture requirements should be defined and documented. Verify whether: ■ System personnel have considered all transaction volumes, number of users, expected response time and overall performance in the architecture design ■ The architecture is consistent and compatible with the organisation infrastructure ■ Other constraints have been considered, such as: – Reporting requirements – Batch cycles – Back-up requirements – Feeds to and from other systems – System availability requirements – System and hardware maintenance – System growth (volume of transactions and users) – System maintenance and cyclical upgrades ■ The system architecture is compatible with the database and program design	
	A strategy for implementing security over the system and application resources should be designed and documented. Verify whether: ■ Logical and physical security over hardware and system software have been designed and documented ■ Logical security over source and object code has been designed and documented ■ Logical security over application files/databases has been designed and documented ■ Functional application security has been defined and provides an adequate segregation of duties	
	A quality assurance process should exist to review the system design. Review the system design to determine whether: ■ Adequate audit trails have been designed into the system ■ Internal controls are designed to minimise and/or eliminate identified business risks ■ Adequate balancing, reconciliation and error routines have been designed to provide reasonable assurance that the completeness and accuracy of system data ■ The system, as designed, will conform to legal requirements ■ The system, as designed, will conform to organisation standards, including the security policies and infrastructure standards ■ The design addresses any control weaknesses in the prior business solution	
	Final specifications should be reviewed to provide reasonable assurance that system design specifications meet the business requirements and are approved by management, end-user representatives and areas affected by the project. Verify whether: ■ The development team and the business area have thoroughly walked through the design to provide reasonable assurance that it is complete and meets all business requirements ■ System design specifications are reviewed, understood and approved by business management	
	Procedures should be developed to manage source code and object code in the development environment. Determine: ■ If a procedure exists for managing source code ■ If a strategy has been developed and documented to coordinate source code management and version control (e.g., version control tool) through the development and testing phases ■ How the vendor will manage source code and determine how updates to object code will be managed by the project team if application is a purchased system ■ That only those with a business need have access to production libraries where application source and stored procedures reside. In addition, if the software changes require changes to the database structure, provide reasonable assurance that access to database triggers are secured and are part of this SDLC process, including version control.	
	A test environment/infrastructure should be designed and developed. Determine: ■ If a test environment has been designed and built to support testing of the new application ■ Whether this environment is a copy of the anticipated production environment. If this environment is not a duplicate of the anticipated production environment, identify the differences and what effect these differences might have on the validity of testing results.	

	Suggested Change Control Testing Procedures	√
	Standards for system and program documentation should be recorded and communicated to IT staff and enforced. Verify: ■ Whether procedures/standards for creating, maintaining and storing documentation have been established. Review any documentation created so far (i.e., flowcharts, data flow diagrams, data dictionaries and record layouts). ■ That source code documentation standards provide reasonable assurance that programs are self-documenting and enforced ■ That the project plan includes time frames dedicated to documentation ■ If the application is a purchased system, what documentation will be provided/maintained by the vendor. Determine who will maintain documentation of customised code changes.	
	Determine whether all exceptions are documented and reported to management for corrective action. Documentation of remediation should be included in the audit workpapers.	
Testing	The overall objective is that a testing methodology is defined, documented and executed to provide reasonable assurance that the developed solution meets the defined business requirements, meets technical requirements, handles the expected transaction volume and response time, produces accurate results, and operates reliably.	
	A test plan/methodology should exist for managing and monitoring the testing effort to provide reasonable assurance that the system functionality is fully tested. Determine: ■ Whether the test plan exists and is documented ■ If a schedule for completing the testing is developed and documented ■ If test criteria are clearly defined and documented ■ If complete test cases have been developed, defined and documented. Ascertain if there is a cross-reference matrix (e.g., traceability matrix) that matches each specific requirement in the formal, detailed and documented "requirements document" generated and/or signed off by the business owner and the actual test plans. If this cross-reference matrix does not exist, obtain support and documentation from management in how they would verify that all requirements are being tested. ■ Whether the test plan defines who is reviewing and approving test results ■ Whether procedures for issues/problems resolution exist and are reasonable ■ Whether entry and exit strategy is tested ■ Problem resolution and turnaround time for incidents identified during testing	
	The test plan is completed prior to the start of testing. Review the test plan to determine whether: ■ The test plan adequately addresses all functionality (i.e., business requirements) of the application. The test plan should include: – Data entry – Editing (positive and negative reporting) – Reports (including printing and distribution handling) – Updates, calculations and processing – Error handling and reporting – Interfaces – Security functions – Controls to provide reasonable assurance that data are complete, accurate and non-redundant – Application audit trails and system checks ■ Technical components are considered in the test plan, including: – Performance testing – Stress testing (including printing) – Volume testing (normal and highest predicted volumes at peak times) – Network stability ■ Management simulates testing in a production or production-like environment ■ Management monitors the testing process to ensure the testing methodology is followed	
Testing (continued)	A procedure should be in place to manage changes (including error correction) throughout the testing process. Determine: ■ What procedures have been implemented to control errors/change management/problem resolution ■ The methods to identify, report, monitor and track problems ■ Whether management is involved in the problem resolution escalation and changes that may affect the scope or functionality of the system ■ Whether problems are being tracked according to the methodology defined ■ Whether standards are in place to address changes	

	Suggested Change Control Testing Procedures	√
Testing (continued)	A procedure should be in place to manage software to provide reasonable assurance that versions of programs are appropriately managed. Verify: ■ Whether testing libraries are established and that programs to be tested are stored there ■ Who has access to testing libraries for adding, deleting and changing programs ■ Whether procedures for managing software and code asset management (CAM) are being followed ■ Whether changes to programs by multiple users are managed so as to not overlay code completed and tested by other programmers ■ Whether a method exists to provide reasonable assurance that coding changes reintroduced into the test environment are controlled and fully retested ■ Whether all functionality is retested when coding changes are implemented	
	A separate test environment should be established. Determine: ■ What testing environment has been created to provide for all phases of testing, including: – Baseline – Unit – System – Integrated – Parallel – Regression – Acceptance ■ What provisions have been made for testing with internal and external systems ■ Whether the test environment is adequate to provide full volume testing to mirror the live production environment ■ Whether the technical components of the test environment provide for performance testing, stress testing (including printing), volume testing (normal and highest predicted volumes) and network stability	
	The level of testing requirements should be assessed, and coverage should be appropriate to this assessment. Determine how changes to the test cases are introduced, documented and tested, and verify whether: ■ Individuals from all affected business areas are represented in testing, from developing test cases to reviewing and approving test results ■ The project team ensures all possible system functions, transactions, data combinations and error scenarios are included in testing ■ Month-end, quarter-end and year-end processes and data requirements are included in testing ■ All test cases and expected outcomes are documented ■ All test cases are tied to the business requirements and all business requirements have test cases ■ The integrity of test data is maintained throughout the testing process ■ A method to track testing discrepancies and subsequent resolutions is in place ■ Any exception process functions are included in test cases	
	Logical and physical security requirements should be included in the test plan. Determine: ■ That physical and logical security functions are defined and in place for the testing phase ■ Who manages security during the test phase ■ That the security in place for testing includes access to screens, functionality, data and reports	
	Process and procedures should provide training on new systems so users can actively participate in the testing. Determine: ■ If the vendor will provide the training to the end users, as defined by the test plan, within the time frames specified in the plan ■ Whether training for in-house developed systems has been developed ■ Whether training material is distributed to end users ■ Whether training is delivered to end users in a timely manner to allow active participation in the testing activities ■ Whether project team management ensures that training is adequate and appropriate by obtaining feedback from end users and taking corrective action as appropriate	
	A process should be in place to define and conduct final acceptance testing and obtain management signoff. Verify: ■ If all testing was completed, based on the test plan ■ Whether test results are/were reviewed and approved by management, as indicated in the project plan/test plan ■ Whether contracts with third parties were reviewed and approved by both the vendor and business management ■ Whether all test results are approved and signed off by appropriate management	
	A process should be in place to ensure performance sizing (optimisation) is conducted to forecast the human resources required for operating new and significantly changed software. Determine: ■ Whether the project plan includes a training phase ■ If0 end users can handle the workload (too much work, need to hire more staff) if a process exists to monitor performance ■ If procedures exist for updating manuals and/or online help facilities	

	Suggested Change Control Testing Procedures	√
	Document all test results. Verify that all test results are documented, including expected results, actual results and corrective action taken if needed.	
	Determine whether all exceptions are documented and reported to management for corrective action. Documentation of remediation should be included in the audit workpapers.	
Implement-ation	The overall objective is for implementation of the system to be established and executed according to plan to provide reasonable assurance of the successful transfer into the production environment.	
	Training and system documentation should be completed prior to implementation. Determine that: ■ Users have been trained and are aware of their new responsibilities prior to implementation ■ Adequate reference material is available to users, operations personnel and programmers, including: – User manuals, which may include business rules and processing, balancing and reconciliation procedures, input processing, error correction procedures and, a summary of system output and disposition – Operations manuals, which may include abend procedures, backup schedule, batch schedule, interface listing and procedures, on-call lists, and escalation procedures – Programmer manuals, which may include listing and descriptions of programs, screen layouts, file/database descriptions, flowcharts and job listings/schedule	
	Service level agreements and operational requirements should be defined and developed prior to implementation. Determine: ■ If vendor or in-house service level agreements and/or operational requirements are agreed to before implementation ■ Whether the following operational needs have been addressed prior to implementation: – Help desk support (vendor or in-house) – Disaster recovery and business continuity planning – Change management (vendor or in-house) – Backup schedule – Batch scheduling (if applicable) – Interface scheduling (if applicable) – Routine and periodical hardware and system software maintenance	
	An implementation plan should be documented, communicated and approved. Determine: ■ If a step-by-step cutover plan has been developed prior to implementation. Verify that this plan contains all tasks required to implement the system, including task timelines, task inter-dependencies and the person assigned to complete each task. ■ If the implementation is phased, how management ensures the phases are completed and approved prior to starting the next implementation phase ■ Whether representatives from all affected areas have been involved in the development of the plan and that the plan includes tasks for all affected areas (affected business areas, production control, system software and network engineers, and database administrators). This review includes an evaluation of the release management process to provide reasonable assurance there are no conflicts with other changes, such as interacting systems or infrastructure elements. ■ Whether the plan has been communicated to all affected business and technical areas ■ Whether management has approved the plan	
	A methodology to approve and communicate the go-live decision should be developed. Determine: ■ Whether management ensures the system is ready for production ■ The procedure for the decision to go-live, including who is responsible for making the final decision ■ Whether a method has been implemented to provide reasonable assurance that all affected areas are notified of the go-live decision	
Implement-ation (continued)	A procedure for communication and resolution of implementation issues should be documented and communicated to all affected parties. Verify that a: ■ Plan for communication and resolution of implementation issues has been documented and communicated to all affected parties (i.e., implementation help desk, escalation procedures and call trees) ■ Mechanism for addressing implementation problems has been developed to provide reasonable assurance that production processing is minimally affected in the event of problems ■ Back-out strategy has been developed and documented. Verify who is responsible for implementing the back-out strategy decision and if the criteria for implementing back-out has been documented.	
	A procedure for cutover/conversion of production data should be developed, documented and approved. Verify that: ■ The cutover of data is documented as part of the implementation plan ■ Management will verify that cutover has not affected the data, and that the new and old systems have processed accurately, completely and non-redundantly ■ The data cutover process will provide reasonable assurance that all data have been converted accurately and completely. If errors and/or data fall-outs are to be entered manually, determine if the method assures that all errors are accounted for and the system is balanced/reconciled after entry of errors.	

	Suggested Change Control Testing Procedures	√
	A procedure to migrate the system code from final acceptance to the production environment should be developed. Determine: ■ Whether a procedure exists to migrate the system code from final acceptance to the production environment ■ If the final acceptance and production environments are secured ■ Whether the corporate code asset management process is utilised	
	Determine whether all exceptions are documented and reported to management for corrective action. Documentation of remediation should be included in the audit workpapers.	
Postimple-mentation Review	The overall objective is that a post-implementation review should be performed to ascertain whether the project has satisfied user expectations, budget and time frame. In addition, post-implementation review would include: ■ Process integrity—application of internal business controls within the system ■ Application security	
	Management should consider conducting a post-implementation review to verify adherence to the project plan. Determine whether: ■ A post-implementation review has been performed. Verify that this review covered: – Comparison of budget to actual and an explanation of variances – Comparison of initial planned timeline to actual development timeline and an explanation of the variance – Comparison of original scope to scope of system delivered and an explanation of the variance ■ 'Lessons learned' and 'what worked well' have been documented or, at minimum, discussed by the project team to help future project teams from repeating mistakes	
	Management should review the extent to which the implemented system has achieved the project objectives. Determine: ■ The method that management is using to obtain feedback about the success/failure of the system ■ How management is measuring whether projected benefits of the system are being realised ■ If differences between expectations and the final system deliverables are noted, how management intends to investigate and reconcile these differences ■ How satisfied the users are with the system. If the users are dissatisfied, determine the reasons for their dissatisfaction (i.e., screens are not user friendly, slow response time, lack of adequate training).	
	Procedures should be in place to monitor and address post-implementation issues. Determine: ■ If a procedure has been implemented to track, prioritise and resolve post-implementation issues ■ Whether users have adequate resources to resolve problems (i.e., help desk, system experts within their area) ■ Whether training for end users was appropriate, enabling users to successfully use the system	
	A methodology should be in place to transition from system development to system maintenance/production support. Determine: ■ If procedures are in place to track and prioritise requested application enhancements (e.g., problem/help desk tickets, formal project submission, including executive management approval for large projects) ■ If a process has been established to mange source code ■ Whether security privileges that may have been necessary to develop and implement the system will be revoked in a timely manner ■ If the package is a vendor package, whether vendor maintenance services are clearly defined ■ Whether problem/help desk tickets are closed on a timely basis (e.g., within 48-72 hours of an emergency change) with root cause analysis. In addition, trend analysis of problems regarding the application changes may be appropriate.	
	Management should monitor the performance of the new system until all cyclical activity has processed successfully at least once. Verify whether management is reviewing performance reports, including: ■ Response time ■ Transaction volume ■ Errors ■ System availability ■ Vendor performance	
	Determine whether all exceptions are documented and reported to management for corrective action. Documentation of remediation should be included in the audit workpapers.	
Unplanned Emergency Change **Unplanned Emergency**	The overall objective of emergency changes is for the times when they are required to resolve system problems and enable critical processing to continue. IS auditors should review the existence of and adherence to procedures that provide reasonable assurance emergency fixes can be performed without compromising the integrity of the system. Determine: ■ The emergency change process and document it ■ Whether emergency changes are appropriately documented and approved ■ If emergency changes are ultimately tested and reviewed by a change control board prior to making the changes permanent ■ What the process is for using and monitoring emergency change user IDs	

	Suggested Change Control Testing Procedures	√
Change (continued)	There may be times when emergency changes are required to resolve system problems and enable critical processing to continue. Verify whether procedures exist to provide reasonable assurance that emergency fixes can be performed without compromising the integrity of the system by: ■ Performing a walk-through of the emergency change control process to confirm an understanding of the process ■ Documenting the help desk responses to emergency conditions that may require programming changes ■ Ascertaining if these changes were processed through the change control process	
	Management of controls includes the emergency change process, which should be managed so there is an approval to bypass the standard change process. Verify whether: ■ Activities occurring during the emergency change are logged and reviewed by management with application development and security services groups (e.g., due to the powerful user IDs granted to the programmer to complete the emergency change for resumption of system availability) ■ Upon resumption of the system for use by the customer, the programmer's access to the production environment is removed, a full post mortem is completed with root cause analysis, and full regression testing is performed to ascertain if the emergency program fix affected other system elements (e.g., database, interfacing applications, other applications within the same suite where the change occurred) ■ The programming fix is executed from a controlled program library that is backed up and retained with it source code for a required period of time based on the business and legislative risk of the change	
	Verify that all emergency changes with the associated root cause are reviewed by senior IS management on a timely basis.	
	Audit trails and logs are created to document the emergency at the time of the occurrence. Verify whether: ■ The emergency is fully documented in the problem management system (e.g., help desk) with a high severity, indicating immediate programming modifications are required ■ This problem management process includes audit evidence from at least one business owner that a severe business system disruption has occurred or business information has been corrupted. Verify that notations are made in the problem management system, including the time and date when the emergency change/fix was completed.	
	Depending upon the size of the IS organisation, programmers may be able to submit emergency programs. If programmers cannot use their standard method of access used in the development environment to change elements in the production processing environment, verify that the programmer must obtain an emergency user ID, under control of production services/computer operations or security services (e.g., a group independent of the application development group) to access the production environment.(e.g., programming library).	
	Determine whether activities occurring during the emergency change are logged and reviewed by management with application development and security services groups (e.g., due to the powerful user IDs granted to the programmer to complete the emergency change for resumption of system availability). The password for the emergency user ID should be reset by security services to prevent re-use without the appropriate approval.	
	Verify that the programmer's access to the production environment (program and data libraries and databases) is removed after resumption of the system by the customer.	
Unplanned Emergency Change (continued)	Review corrective controls to prevent reoccurrence of the change. Verify whether: ■ A full post mortem is required and completed, including the identification of a root cause analysis ■ As a result of the post mortem, additional preventive controls are instituted, if applicable (e.g., additional management controls over testing may be needed if the root cause was deemed to be the lack of adequate testing of a prior change). There typically is a high correlation of system outages and a weak change control process to the production environment. ■ The adequacy of and adherence to procedures to verify that subsequent (e.g., after the emergency change was completed) required and completed full regression testing to ascertain if the emergency program fix affected other system elements (e.g., database, interfacing applications and other applications within the same suite where the change occurred)	
	Review controls over the execution of the emergency programs, including: ■ Verify programming fixes are executed from a controlled program library that is reviewed by production control group. Verify that all applicable system logs are reviewed by production control to provide reasonable assurance that only those changes related to emergency change were made. ■ Program libraries where emergency programs reside (both source and load) are backed up and retained with it source code for a required period of time based on the business and legislative risk of the change. ■ Where practical, all emergency fixes are required to be submitted (executed) in the production process environment by computer operations personnel rather than the programmers.	

	Suggested Change Control Testing Procedures	√
	Determine that the integrity of baseline management is maintained by reviewing the baseline management process to ascertain if emergency program changes, which will be permanently part of the baseline, are included to avoid overwriting of the emergency change and immediately preceding program modifications (to be elevated into the production environment).	
	If a formal process is in place where a emergency change request is required, verify whether: An audit trail exists, including a standard change request form requiring documentation of a business need (for the emergency, unplanned and override change), install plans and back-out plans for the unplanned changes on a change record There is an adequate retention period for change request forms There is a reconciliation of these changes to a problem record (ticket) as part of the follow review Change record documentation requires specification of risk (severity) level justifying the change to be completed bypassing the standard process Business owners' (at the appropriate level of management) approval is required for these changes after the fix is made	

9. EFFECTIVE DATE

9.1 This guideline is effective for all information systems audits effective 1 October 2006. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary*.

P11 Electronic Funds Transfer (EFT)

1. INTRODUCTION

1.1 CobiT Reference

1.1.1 Refer to CobiT for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this procedure. Selection of the most relevant material in COBIT applicable to the scope of the particular audit should be based on the choice of specific COBIT IT processes and consideration of COBIT information criteria.

1.1.2 The primary information criteria most relevant to an electronic fund transfer implementation and audit process are:

- Efficiency
- Effectiveness
- Confidentiality
- Integrity
- Availability
- Reliability
- Compliance

1.1.3 CobiT guidance for the following processes is relevant when performing the implementation and audit:

- Integrity and security of transactions and documents:
  - PO2—Define the information architecture
  - PO9—Assess and manage IT risks
  - DS5—Ensure systems security
  - DS10—Manage problems
  - DS11—Manage data
  - ME2—Monitor and evaluate Internal control
  - ME3—Ensure regulatory compliance
- Efficiency and reliability of support systems:
  - AI1—Identify automated solutions
  - AI3—Acquire and maintain technology infrastructure
  - AI6—Manage changes
  - AI7—Install and accredit solutions and changes
  - DS1—Define and manage service levels
  - DS2—Manage third-party services
  - DS3—Manage performance and capacity
  - DS4—Ensure continuous service
  - DS7—Educate and train users
  - DS9—Manage configuration
  - DS12—Manage the physical environment
  - DS13—Manage operations
  - ME1—Monitor and evaluate IT performance

1.2 Electronic Funds Transfer

1.2.1 The electronic funds transfer (EFT) is a widely used method to transmit transfer instructions electronically throughout the world. These transfers could be payment instructions to financial institutions (for employees, companies or entities) or movement instructions to change the institution custody of the customer's money. 'Customers', in this context, could be an individual consumer or corporate customer.

1.2.2 EFT processes are generally designed to ensure adequate disclosure of basic terms, costs and rights relating to electronic fund transfer services provided to consumers. Institutions offering EFT services must disclose to consumers certain information, including the:

- Initial and updated EFT terms
- Transaction information
- Periodic statements of activity
- Consumer's potential liability for unauthorised transfers
- Error resolution rights and procedures

1.2.3 EFT services include but are not limited to:

- Automated teller machines
- Telephone bill payment
- Point-of-sale (POS) transfers in retail stores
- Fund transfers initiated through the Internet
- Preauthorised transfers to or from a consumer's account

1.2.4 For the purpose of this audit procedure, the scope—type of transactions are as follows:

- EFT is any transfer of funds between parties or depository institutions through electronic data systems located in the same or different countries. EFT could be amongst accounts of the same holder or different holders (interbank, intercompany).
- Although EFT does not consider e-commerce, it could be seen as an implementation of the business-to-business model.
- All other models of e-commerce (business-to-consumer, consumer-to-business, etc.) that generally include card transactions are considered cash management transactions.
- Throughout this document, reference to financial institutions also includes banks, and other such similar institutions where EFT is adopted.

1.2.5 Depending on each implementation, the origin of the transaction could be from:

- An automated teller machine (ATM) device, where the customer performs a transaction that is inside the country from a bank associated with the ATM network. The destination customer account is used.
- Wire transfer instructions and online banking application from a bank that provides this option as part of its web services
- A bank counter, where the customer completes a transfer receipt to another bank in the same country or another country
- A bank treasury assistance service or customer service where the customer instructs a bank employee to perform a transaction electronically with another bank
- Automated clearing house (ACH) Network—a batch-oriented electronic funds transfer system that provides for interbank clearing of electronic payments for participating depository financial institutions
- POS device that allows the retailer to manage cash, inventory and customers
- An enterprise resource planning (ERP) system or similar implementation where a company generates an EFT file, which is transmitted to the bank system
- A telex transaction or fax transaction with a key book

1.2.6 For all implementations in 1.2.4, there is a front-end service or application that manages the customer interface, generates the instruction and passes it to the back-end application (core application) that is managed by the bank through a global transaction network, such as SWIFT, MERVA or FED Wire.

1.3 Type of Applications—Technology Platforms

1.3.1 The front-end technology depends upon company application (i.e., ERP interfaces) and bank services (i.e., ATMs, help desk, counter transactions and online banking).

1.3.2 The application/platforms or middleware may be based upon client-server architecture (LAN/WAN, i.e., ERPs), legacy applications (all platforms), web applications (Internet) or specific applications (ATM networks).

1.3.3 The back-end or core application is the most critical component in the EFT process, as this application finally transfers the money between different accounts, different banks and generally different countries. For that reason, banks do not generally permit web technology platform implementations and use a more robust technology platform implementation based on a mainframe, such as IBM OS400, which has a relational database embedded in its operating system, adding more security and performance.

2. EFT PROCESS

2.1 Definition

2.1.1 EFT is the exchange or transfer of money electronically from one account to another, either within the same enterprise or across different enterprises**.**

2.1.2 EFT is a complex process wherein fund transfers could occur in various methods and in different currencies. EFT requires highly efficient controls built into the systems, and the process is controlled both at the sender and recipient sides. Controls need to exist at the intermediary stages wherever information is passed, stored or processed.

3. RISK ASSESSMENT AND CONTROLS

3.1 Risks—General IT Controls

3.1.1 In general, the EFT process should ensure confidentiality, integrity and availability (CIA). But for the special type of implementation, the order of priority may be IAC—integrity, availability and confidentiality—instead of CIA. This requirement should be addressed by controls implemented in different levels of the EFT implementation, such as business process controls, application controls and platform controls.

3.2 Business Process Controls

3.2.1 In a general way, the business processes should ensure the CIA of EFT processes.

3.2.2 No one person should handle all of the transaction. This is achieved by proper segregation of duties between the maker/checker and sender.

3.2.3 Integrity and accuracy of transaction instructions should be maintained from source to destination. Appropriate control could include settlement and reconciliation, verification for appropriate accounts and the date/time the transaction was generated, verifying with customers to ensure account and transaction details, etc. For fax transactions, primary considerations are the:

- Key books procedures
- Requirement (authentication)
- Generation of the key
- Custody of the key and the change/revocation
- Communication of the key's procedures

3.2.4 The transaction should be requested, generated and completed in accordance with agreed-upon service level agreements (SLA).

3.2.5 Relevant personnel should be adequately trained ensure that customer requirements are met as per the SLA.

3.2.6 The financial institution should have sound background verifying the process prior to recruiting and have sufficient coverage via confidentiality and non-disclosure agreements.

3.2.7 The bonding of employees and rules to deter against internal frauds should be considered.

3.2.8 The impact of the statutory and regulatory requirements of the sending and receiving countries should be considered, and compliance should be met for all requirements regarding cross-border transactions.

3.2.9 Business continuity and alternate modes of transmitting EFT transactions should be available in case of system or network outage.

3.2.10 Business process controls include capturing appropriate data to measure performance against the agreed-upon SLA. Ideally, EFT metrics should be computed and analysed for all processes of EFT transactions. Contract impacts and SLA definitions should be considered for metric analysis.

3.3 Application Controls

3.3.1 Application level controls should ensure confidentiality, integrity and availability (CIA) of transmit instructions.

3.3.2 Identification and authentication should consider:

- Login to the specific EFT terminals (terminals restrictions)
- Static/dynamic passwords (strength of the password)
- Digital certificates and session time-out restrictions

3.3.3 Access controls and authorisation entitlements and approval steps (entitlements reviews) should be documented and monitored.

3.3.4 Changes to EFT transaction details should be from the application that originated the transaction. Any changes initiated otherwise should be properly controlled by means of appropriate identification, authentication and authority to enable the change.

3.3.5 Realistic maximum transaction and maximum daily total limits should be implemented for individual EFT application users. Limits for corporate clients depend on SLA and respective client policy.

3.3.6 In addition to the printed receipt, every transaction should be acknowledged by an e-mail or short message script (SMS) to the mobile phone to confirm or alert the user of the transaction.

3.3.7 Appropriate application level change management controls should be in place.

3.4 Platform Controls

3.4.1 Controls to consider should include:

- Encryption
- Algorithm strength
- Key strength
- Key management
- Communication
- Type of encryption
- Hardware vs. software
- Level of ISO model where encryption is implemented

3.4.2 Non-repudiation of transactions, such as digital signatures, should be considered.

3.4.3 Data residence should comply with cross-border regulations.

3.4.4 Communications to consider should include:

- Peer-to-peer lines vs. public network
- Communications protocols
- Encryption protocols
- Communications features, especially for long distance

3.4.5 Integrity controls, such as cyclic redundancy check (CRC), hash function and keys algorithm should be considered.

3.4.6 Hardware that ensures availability and accuracy, high performance and tolerance (multitasking and multisessions) should be used.

3.4.7 Hardware, software and platform-level change management controls should be considered.

3.4.8 Administrator functions involving changes to security, administration and user account parameters should require co-authorisation.

3.5 Fraud Detection and Preventive Controls

3.5.1 Globally, transactions on EFT systems are subject to high risk and exposure to fraudulent activities. Financial gain is one of the key motivations behind frauds, other than the desire to master the EFT process, the thrill of the deed, intellectual challenge and employee revenge. The simplicity of modifying a basic text file to obtain large payments is an inducement to commit fraud. By fraudulent alteration of EFT, an individual could steal large sums of money. According to statistics, public companies lose huge sums each year due to fraudulent EFT payment instructions.

3.5.2 Any unauthorised alteration of data (fraud) or even a data input error produces (if not immediately detected or corrected) an alteration of a customer's account balances; hence, preventing unauthorised alteration is vital for these systems.

3.5.3 Generally, for money transfers involving different customers, banks and countries, it is vital that the process should assure (preventive controls) that the transaction data are validated prior to processing.

3.6 EFT Audit Procedure

3.6.1 The following table is a suggested audit process to review an EFT process (internal applications, such as ERPs and online banking, provided by financial institutions).

P11 Electronic Funds Transfer (EFT) cont.

Requirements	Suggested Audit EFT Procedures
General controls	• Define objectives and scope of review and obtain documentations. • Obtain a current list of personnel who work in the EFT department. • Obtain the description of retail EFT systems operated including ATM, POS, debit/credit/smart cards, and online banking, including network and mercantile memberships. • Obtain complete detailed process and control descriptions related to the EFT process. • Obtain policies and standards related to the EFT process, including: • Information security requirements relevant for the EFT business process • Procedures about audit trails in products and applications • Obtain all regulations applicable to the EFT process. • Obtain a complete inventory of hardware, software and telecommunications protocols used to support the EFT process and select EFT components to review. • Define audit and scope strategy according to risk assessments, existing controls and previous reviews. • Review prior the audit report and findings and determine the action to be taken by management. • Review the record retention policy and determine its adequacy. • Review insurance coverage for ATM liability, business interruption and fidelity. • Determine whether the terminals are insured from theft, burglary and other exposures. • Determine whether the documented user training material is available and displayed at the point of use. • Determine whether the documentation for business continuity and disaster management plans are available.
Physical controls	• Determine whether the terminals, such as ATM and POS, are located in secure premises. • Determine whether the terminals are securely locked with access control mechanisms installed. • Determine whether the terminal is accessible only by authorised persons. • Determine whether there is restriction on the maximum number of persons in the premises at any given point of time. • Determine whether people in the queue are NOT able to view information in the screen provided by the user. • Determine whether there is adequate management supervision over the terminal. • Determine the level of physical security surrounding the wire room or work area designated for the operation. • Determine whether the system uses physical tokens (debit card/smart card, etc.) to control access. If so, are there satisfactory controls over receipt, storage and issuance of physical tokens? • Determine whether there is a system to capture, store and retrieve an image of the user with corresponding activity details. • Determine whether there is adequate security and protection for transferring/uploading cash into the ATM and carrying cash from the POS. • Determine whether the terminals are visible or obscured to the outside world. There are pros and cons to both and appropriate compensating controls should be in place.[3]
Process controls	• Determine whether general ledger accounts related to EFT are reconciled on a timely basis. • Determine whether reconciliation exceptions are reviewed and action is taken regularly. • Determine whether the EFT system and origination site reconciliation is adequately controlled and reviewed. • Ascertain if daily settlement with each shared EFT network is current and controlled. • Determine whether documented procedures are available and current for balancing and settling transactions. • Review all manual controls in the operating process (i.e., telex, key book). • Review effectiveness of reconciliation and non-repudiation procedures. • Identify inherent IT risks and the overall level of control points in the EFT process. • Analyse the security assigned to the resources where logs are stored and managed (e.g., online, offline, onsite, offsite). • Review the audit trail toward recreating activity or error analysis as needed. • Review the parameters installed in the equipment/software regarding activation/deactivation or deletion. • Obtain and assess the risk assessment documents for each audit trail generated. • Check for the existence of controls over the EFT audit trails (e.g., equipment, network, procedures). • Monitor routines to analyse audit trail availability. • Review the access control audit trails on the security software or key management reports. • Review and evaluate communication controls (encryption, authentication) to assure CIA. • Evaluate storage of critical data and documents and retention of logs. • Evaluate compliance with internal and regulatory requirements. • Evaluate outsourcing services (if applicable). • Review the level of access applied to the EFT text file generated by the ERP. • Review the level of 'modify' access within the EFT client software.

[3] While obscure terminals provide privacy to the user, they also provide cover for a perpetrator of fraud. Visible terminals do not provide cover to fraudsters; however, they carry the disadvantage that an outside person can observe the events taking place with in the terminal.

Requirements	Suggested Audit EFT Procedures
Process controls cont.	• Review the controls over the security, administration and user account parameters within the EFT client software.
Transmission and system failures	• If there is an interruption during transmission, determine whether the system provides a record of accepted messages. • Determine whether there are written procedures for the retransmission of non-accepted messages. • Determine whether an incident log is kept for all interruptions to normal processing. • In the event of a hardware failure, determine whether processing can be switched to an alternate terminal. • Determine whether there are controls to prevent duplication of message processing following system recovery. • In the event of line failure, determine whether a redundant/backup communication media is available.
System logon controls	• Determine whether the system validates all authorised users. • Determine whether the ability to establish a session path is restricted to authorised persons. • Determine whether the system records by whom the session path/logon is established. • Determine whether the system provides a record of all attempts to work outside authorised functions. If so, determine whether this record is reviewed periodically and appropriate action taken. • Determine whether the system provides a record of all password/logon violations and that it is reviewed regularly. • On establishing the session, determine whether the system validates the terminal ID. • Determine whether the system requires the use of a secure key to validate the client as an authorised user. • Before transmission, determine whether the system ensures that all messages are authorised. • Determine whether the system prevents transmission of unauthorised messages. • Determine whether the system validates the user as being authorised to transmit the message type in question. • Determine whether there are procedures for reporting unauthorised messages at transmission time. • Determine whether all input documents are checked for proper authorisation by the originator. • Determine whether there are controls to ensure that extensions to the daily/individual value limit for messages are property authorised.
Messaging controls	• Determine whether unbroken sequential serial numbers are assigned to each message. If so, determine whether they are recorded on input documents/register. • Determine whether interruptions are reviewed. • Determine whether a permanent record is kept of all transmitted messages. If so, determine whether this is checked against a record of all accepted/rejected messages. • Determine whether it is possible to retrieve individual message data. • Determine whether an audit trail is produced of all input messages and that it records: – A unique message reference number – Date and time of input – By whom input is verified/authorised – Who established session path – Date and time of transmission – Whether message accepted/rejected – Details of message contents • Determine whether the audit log is delivered to someone independent of input function. • Determine whether the audit log is accessible by authorised people only. • Determine whether the audit log is scrutinised by management. • Determine whether there is a regular reconciliation between transmitted messages and bank statements. Determine whether all originators are notified when their input messages are accepted.
Transfer controls	• For incoming transfer controls, determine whether: – All messages are sent in a standard format. – Alteration to the standard format is prohibited. – The system ensures that all validated fields are entered. – The system ensures that all fields are entered in the required format. – The system highlights/reports amounts outside of the expected range. – There are controls to ensure that no values beyond the expected limits are accepted. – There are controls to ensure that the total value of messages is within an agreed (daily) limit. – The system provides acknowledgement of satisfactory validation of transmitted messages. • For outgoing transfer controls determine whether: – They are rekeyed when messages are input. – The authorising officer checks all messages to originating documents. – The originating documents are appropriately endorsed at time of input and authorisation. – The system enforces re-input and requires proof of any differences. – Written procedures are reviewed for handling errors. – The system generates control totals for number and value of message input, and checks them against input records. – The system provides a report of all accepted and rejected messages with appropriate control totals and checks them against input records.

Requirements	Suggested Audit EFT Procedures
	– There are written procedures for dealing with rejects. – The system generates any check-sums, etc. – The communications protocol uses error-detection/correction techniques.
PIN controls	• Review the personal identification number (PIN) issuance procedure. • Determine whether PINs are adequately protected during storage and transmission. • Review encryption procedures on PIN storage. • Review procedure of PINs during delivery. PINs should be masked during delivery and not appear in printed form, be easily visible or associated with customer account numbers. Personnel in charge should not be able to see or retrieve a customer's PIN. • Determine that PIN mailers are not mailed together with the customer card. The most desirable control is to send PIN and card through different service providers. • Determine that the PIN system restricts access to a customer account after a small number of unsuccessful access attempts. • Review unsuccessful logon attempts and action taken by the customer/organisation. • Review the process for forgotten PINs and issue of new PINs.
CARD controls	• Review card issuance procedure, including the: - Adequacy of control over procurement of cards - Written agreement with the card manufacturer - Audit report of the card manufacturer - Controls over mailing and delivery of cards to customers • Determine that cards are mailed with a return address in case of non-delivery and are not mailed together with PINs. • Review the: - Process for handling returned cards and lost cards - Process of cards captured or inadvertently left at EFT terminals - Control over test or demonstration cards - Controls over issue of any system for instant cards • Review card usage: - Card activation - Cards issued and not activated - Customer data and account-related information - Closed accounts, dormant accounts, deceased accounts • Review contract with card manufacturer, quality assurance process by manufacturer, controls over non-generation of unauthorised cards by manufacturer or the employees of the manufacturer, and adequate protection due to lapse by manufacturer.
Fraud prevention	• Review the following to ensure a mechanism exists for prevention of fraud relating to EFT: - EFT process and control points - EFT policies and procedures - Standards transactions formats - Physical security surrounding all EFT components - Effectiveness of EFT application security - Effectiveness of network operating system security - Effectiveness of security surrounding EFT data - Effectiveness of system logging - Effectiveness of segregation of duties (maker/checker/sender) - Reconciliations - Co-athorisation for administrator functions within EFT application maximum transaction and daily total limits - Usage pattern tracking (such as frequency of logins, money withdrawals, same day withdrawals, number of hours of use) for possible money laundering or intent to commit fraud
Back-end application	• Back-end applications are generally platform specific. Determine whether back-end applications assure: - Atomicity—Work unit not divided, all actions succeed or failed - Consistency—If the transaction cannot generate one stable status, it must return to its initial status - Isolation—The behaviour of one transaction cannot affect other transactions that are executing at the same moment - Durability—The transaction effects are permanent; they cannot be affected by system failures
Front-end application/ perimeter security	• If front-end applications are web-based, review exposure to additional risks, such as: - Denial of service - Viruses, spying and phishing - Lack of vulnerability patch procedures - Web server security - Incorrect architecture and configuration (firewalls, IDSs, DMZ)
	• For ATM front-end applications, consider PIN weaknesses, insufficient awareness, lack of encryption, etc.

Transaction journal	• Determine that the transaction journal information includes the: - Incoming inquiry transaction - Incoming update transaction - Transaction type - Transaction number - Currency - Exchange rate - Amount - Account numbers - Routing bank details - Originating terminal - Originating operator - Time and date - Response to inquiry transaction - Response to update transaction - Indication that response was received correctly - Procedural violation on input - Record of start and end of file reconstruction - Note of completion of update
	• Also consider: - Custody of journal transactions - Retention and backup - Legal, statutory and regulatory requirements
Audit trail	• Determine whether the system has journal and log records. • Determine that the audit trail can be used to: - Allow an auditor to follow the history of a transaction - Permit recovery when it is found that a user has incorrectly updated or deleted a record - Investigate the causes when a record is found to be erroneous - Assist recovery from massive file destruction - Assist in correcting the file where data damage is program caused - Correct false information that has been sent to system users - Monitor procedural violations to highlight possible breaches of security - Assist in correct recovery from a system failure - Monitor the way the system is being used - Recover from the loss of other journal logs - Source for reconciling reports - Consider regulatory requirement and services' purposes for retention time

4. EFFECTIVE DATE

4.1 This procedure is effective for all information systems audits beginning 1 May 2007. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary.*

APPENDIX
Reference

ISACA, *Information Systems Control Journal*, USA, November 1999, January 2000, September 2002, July 2003
IT Governance Institute, COBIT 4.0, USA, 2005
Peltier, Thomas R.; *IS Risk Analysis,* Auerbach, USA, 2001

IS Control Professionals Standards

Issued by Information Systems Audit and Control Association

510. Statement of Scope

510.010 Responsibility, Authority and Accountability

The responsibility, authority and accountability of the information systems control functions are to be appropriately documented and approved by an appropriate level of management.

520. Independence

520.010 Professional Independence

In all matters related to information systems control, the information systems control professional is to be independent in attitude and appearance.

520.020 Organizational Relationship

The information systems control function is to be sufficiently independent of the area being controlled to permit objective completion of the information systems control professional's duties.

530. Professional Ethics and Standards

530.010 Code of Professional Ethics

The information systems control professional is to adhere to the ***Code of Professional Ethics*** for Information Systems Control Professionals issued by the Information Systems Audit and Control Association.

530.020 Due Professional Care

Due professional care and observance of applicable professional standards are to be exercised in all aspects of the information systems control professional's work.

540. Competence

540.010 Skills and Knowledge

The information systems control professional is to be technically competent, having the skills and knowledge necessary to perform the control professional's work.

540.020 Continuing Professional Education

The information systems control professional is to maintain competence through appropriate continuing professional education.

550. Planning

550.010 Control Planning

The information systems control professional is to use risk assessment and other tools as appropriate in planning and prioritizing the information systems control work to address the control objectives.

560. Performance of Work

560.010 Supervision

Information systems control professionals are to be appropriately supervised and coordinated to provide assurance that control objectives are accomplished and applicable professional standards are met.

560.020 Evidence

The information systems control professional is to maintain sufficient, reliable, relevant and useful evidence of activities and tasks performed to achieve the control objectives. Control assessments are to be supported by appropriate analysis and interpretation of this evidence.

560.030 Effectiveness

In carrying out their duties, information systems control professionals are to establish appropriate measures of the effectiveness of their activities in achieving both the objectives of their role and the objectives defined in the Statement of Scope.

570. Reporting

570.010 Periodic Reporting

The information systems control professional is to report periodically to an appropriate level of management on the extent to which control objectives have been achieved.

580. Follow-Up Activities

580.010 Follow-Up

The information systems control professional is to monitor the performance of control procedures and review feedback on the efficiency and effectiveness of control activities and is to ensure appropriate corrective action is taken where necessary.

Effective Date

This material was issued on 1 May 1999 and is effective for information systems control activities carried out on or after 1 September 1999.

History

Statements on Information Systems Auditing Standards (SISAS)

Documents withdrawn

Title	Withdrawal date
SISAS 3 (Evidence Requirement)	19 June 1998
SISAS 7 (Audit Reports)	19 June 1998
SISAS 9 (Use of Audit Software Tools)	19 June 1998
SISAS 4 (Due Professional Care)	1 October 1999
SISAS 6 (Audit Documentation)	1 October 1999
SISAS 2 (Involvement in the System Development Process)	1 March 2000
SISAS 8 (Audit Considerations for Irregularities)	1 March 2000
SISAS 1 (Attitude & Appearance - Organisational Relationship)	1 September 2000
SISAS 5 (The Use of Risk Assessment in Audit Planning)	1 September 2000

IS Auditing Standards effective 25 July 1997-Withdrawn 1 January 2005

ISACA Standards Documents Comments

In our continuing efforts to serve you better, your feedback is requested on standards documents.

Your responses can be returned by e-mail (*standards@isaca.org*), fax (+1.847. 253 .1443) or mail (ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008 USA) to the ISACA International Headquarters to the attention of the director of research, standards and academic relations.

Please attach any additional comments, typed or legibly written. In commenting please be as concise as possible. When recommending additions or deletions, we ask that you refer to the specific paragraph number to which your comment applies and provide suggested wording where appropriate. Please indicate the basis or rationale for your opinion to help us in understanding your point of reference.

Please indicate below any topics (such as emerging issues or problem areas) or other bodies' standards that you believe would be helpful for the Standards Board to consider in the future.

_____

Optional Information for Internal Use Only—used to acknowledge receipt of your response, clarify any of your comments, and summarise the geographic areas from which comments were received.

Name_____ E-mail, Fax or Phone_____

Organisation_____ Title_____

Address_____ Country_____

Thank you! Your comments are invaluable in helping ISACA codify professional guidance.