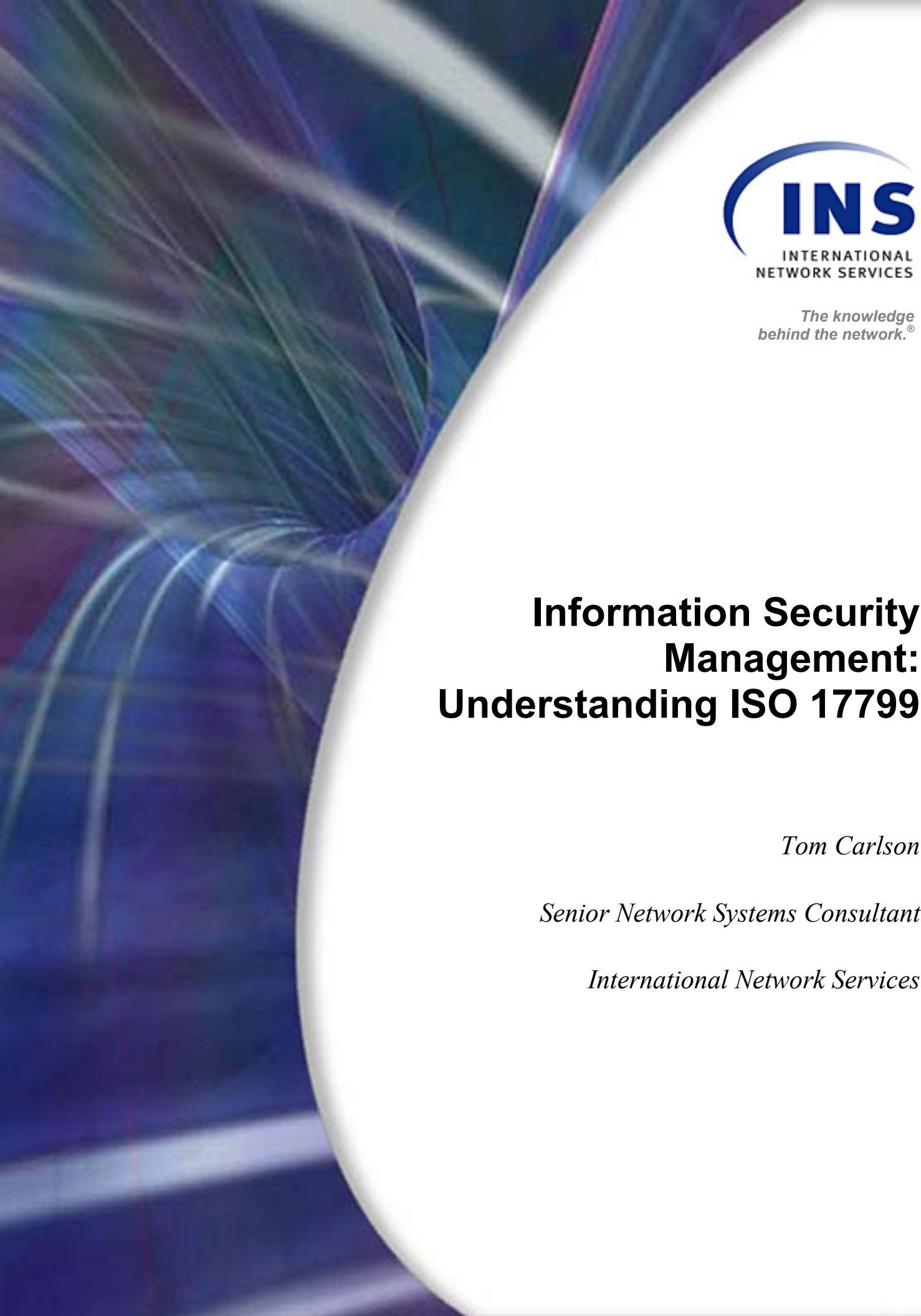


INS
INTERNATIONAL
NETWORK SERVICES

The knowledge behind the network.®

Information Security Management: Understanding ISO 17799

Tom Carlson

Senior Network Systems Consultant

International Network Services

Information Security Management: Understanding ISO 17799

By Tom Carlson, Senior Network Systems Consultant, CISSP

What is ISO 17799?

ISO 17799 is an internationally recognized Information Security Management Standard, first published by the International Organization for Standardization, or ISO (www.iso.ch), in December 2000. ISO 17799 is high level, broad in scope, and conceptual in nature. This approach allows it to be applied across multiple types of enterprises and applications. It has also made the standard controversial among those who believe standards should be more precise. In spite of this controversy, ISO 17799 is the only "standard" devoted to Information Security Management in a field generally governed by "Guidelines" and "Best Practices."

ISO 17799 defines information as an asset that may exist in many forms and has value to an organization. The goal of information security is to suitably protect this asset in order to ensure business continuity, minimize business damage, and maximize return on investments. As defined by ISO 17799, information security is characterized as the preservation of:

- Confidentiality – ensuring that information is accessible only to those authorized to have access.
- Integrity – safeguarding the accuracy and completeness of information and processing methods.
- Availability – ensuring that authorized users have access to information and associated assets when required.

As a standard that is primarily conceptual, ISO 17799 *is not*:

- A technical standard
- Product or technology driven
- An equipment evaluation methodology such as the Common Criteria/ISO 15408 (www.commoncriteria.org), which deals with functional and assurance requirements of specific equipment
- Related to the "Generally Accepted System Security Principles," or GASSP (http://web.mit.edu/security/www/gassp1.html), which is a collection of security best practices
- Related to the five-part "Guidelines for the Management of IT Security", or GMITS/ ISO 13335, which provides a conceptual framework for managing IT security

While ISO 17799 only covers the selection and management of information security controls, these controls may:

- Require utilization of a Common Criteria Equipment Assurance Level (EAL)
- Incorporate GASSP guidelines
- Implement GMITS concepts

Background

ISO 17799 is a direct descendant of the British Standard Institute (BSI) Information Security Management standard BS 7799. The BSI (www.bsi-global.com) has long been proactive in the evolving arena of Information Security.

In response to industry demands, a working group devoted to Information Security was first established in the early 1990's, culminating in a "Code of Practice for Information Security Management" in 1993. This work evolved into the first version of the BS 7799 standard released in 1995.

In the late 1990's, in response to industry demands, the BSI formed a program to accredit auditing firms, or "Certification Bodies," as competent to audit to BS 7799. This scheme is known as c:cure (www.c-cure.org). Simultaneously, a steering committee was formed, culminating with the update and release of BS 7799 in 1998 and then again in 1999. The BS 7799 standard now consists of *Part 1: Code of Practice*, and *Part 2: Specification of Information Security Management Systems*.

By this time, information security had become headline news and a concern to computer users worldwide. While some organizations utilized the BS 7799 standard, demand grew for an internationally recognized information security standard under the aegis of an internationally recognized body, such as the ISO. This demand led to the "fast tracking" of BS 7799 Part 1 by the BSI, culminating in its first release by ISO as ISO/IEC 17799:2000 in December 2000. As of September 2001, only BS 7799 Part 1 has been accepted for ISO standardization because it is applicable internationally and across all types of organizations. Movement to submit BS 7799 Part 2 for ISO standardization has been withdrawn.

BS 7799 Part 1 (ISO 17799) versus BS 7799 Part 2

It is important to understand the distinctions between Part 1 and Part 2 of the BS 7799 standard in order to later understand the dilemma facing conformance assessment. Part 1 is an implementation guide, based on suggestions. It is used as a means to evaluate and build sound and comprehensive information security infrastructure. It details information security concepts an organization "should" do. BS 7799 Part 2 is an auditing guide based on requirements. To be certified as BS 7799 compliant, organizations are audited against Part 2. It details information security concepts an organization "shall" do. This rigidity precluded widespread acceptance and support.

Benefits of ISO 17799

Arguably, perfect security may be achievable only for networkless servers located in rooms without doors. Information security is always a matter of trade-offs, balancing business requirements against the triad of confidentiality, integrity, and availability. The information security process has traditionally been based on sound best practices and guidelines, with the goal being to prevent, detect, and contain security breaches, and to restore affected data to its previous state. While this cumulative wisdom of the ages is valid, it is also subject to various interpretations and implementations. ISO 17799 offers a benchmark against which to build organizational information security. It also offers a mechanism to manage the information security process.

ISO 17799 is a comprehensive information security process that affords enterprises the following benefits:

- An internationally recognized, structured methodology
- A defined process to evaluate, implement, maintain, and manage information security
- A set of tailored policies, standards, procedures, and guidelines
- Certification allows organizations to demonstrate their own and evaluate their trading partners' information security status
- Certification shows "due diligence"

For some organizations, such as those requiring high degrees of assurance, ISO 17799 certification may become mandatory. To other organizations, certification may be a marketing tool.

Controls

Organizations daily face threats to their information assets. At the same time, they are becoming increasingly dependent on these assets. Most information systems are not inherently secure, and technical solutions are only one portion of a holistic approach to information security. Establishing information security requirements is essential, but to do so, organizations must understand their own unique threat environment. Threat environments are determined by the execution of a methodical security risk assessment. Once risk areas are identified, appropriate controls may be selected to mitigate these identified risk factors.

ISO 17799 consists of 10 security controls, which are used as the basis for the security risk assessment.

Security Policy

Security Policy control addresses management support, commitment, and direction in accomplishing information security goals, including:

Information Security Policy document – a set of implementation-independent, conceptual information security policy statements governing the security goals of the organization. This document, along with a hierarchy of standards, guidelines, and procedures, helps implement and enforce policy statements.

Ownership and review – Ongoing management commitment to information security is established by assigning ownership and review schedules for the Information Security Policy document.

Organizational Security

Organizational Security control addresses the need for a management framework that creates, sustains, and manages the security infrastructure, including:

Management Information Security Forum – provides a multi-disciplinary committee chartered to discuss and disseminate information security issues throughout the organization.

Information System Security Officer (ISSO) – acts as a central point of contact for information security issues, direction, and decisions.

Information Security responsibilities – individual information security responsibilities are unambiguously allocated and detailed within job descriptions.

Authorization processes – ensures that security considerations are evaluated and approvals obtained for new and modified information processing systems.

Specialist information – maintains relationships with independent specialists to allow access to expertise not available within the organization.

Organizational cooperation – maintains relationships with both information-sharing partners and local law-enforcement authorities.

Independent review – mechanisms to allow independent review of security effectiveness.

Third-party access – mechanisms to govern third-party interaction within the organization based on business requirements.

Outsourcing – organizational outsourcing arrangements should have clear contractual security requirements.

Asset Classification and Control

Asset Classification and Control addresses the ability of the security infrastructure to protect organizational assets, including:

Accountability and inventory – mechanisms to maintain an accurate inventory of assets, and establish ownership and stewardship of all assets.

Classification – mechanisms to classify assets based on business impact.

*Labelin*g – labeling standards unambiguously brand assets to their classification.

Handling – handling standards; including introduction, transfer, removal, and disposal of all assets; are based on asset classification.

Personnel Security

Personnel Security control addresses an organization's ability to mitigate risk inherent in human interactions, including:

Personnel screening – policies within local legal and cultural frameworks ascertain the qualification and suitability of all personnel with access to organizational assets. This framework may be based on job descriptions and/or asset classification.

Security responsibilities – personnel should be clearly informed of their information security responsibilities, including codes of conduct and non-disclosure agreements.

Terms and conditions of employment – personnel should be clearly informed of their information security responsibilities as a condition of employment.

Training – a mandatory information security awareness training program is conducted for all employees, including new hires and established employees.

Recourse – a formal process to deal with violation of information security policies.

Physical and Environmental Security

Physical and Environmental Security control addresses risk inherent to organizational premises, including:

Location – organizational premises should be analyzed for environmental hazards.

Physical security perimeter – the premises security perimeter should be clearly defined and physically sound. A given premises may have multiple zones based on classification level or other organizational requirements.

Access control – breaches in the physical security perimeter should have appropriate entry/exit controls commensurate with their classification level.

Equipment – equipment should be sited within the premises to ensure physical and environmental integrity and availability.

Asset transfer – mechanisms to track entry and exit of assets through the security perimeter.

General – policies and standards, such as utilization of shredding equipment, secure storage, and "clean desk" principles, should exist to govern operational security within the workspace.

Communications and Operations Management

Communication and Operations Management control addresses an organization's ability to ensure correct and secure operation of its assets, including:

Operational procedures – comprehensive set of procedures, in support of organizational standards and policies.

Change control – process to manage change and configuration control, including change management of the Information Security Management System.

Incident management – mechanism to ensure timely and effective response to any security incidents.

Segregation of duties – segregation and rotation of duties minimize the potential for collusion and uncontrolled exposure.

Capacity planning – mechanism to monitor and project organizational capacity to ensure uninterrupted availability.

System acceptance – methodology to evaluate system changes to ensure continued confidentiality, integrity, and availability.

Malicious code - controls to mitigate risk from introduction of malicious code.

Housekeeping – policies, standards, guidelines, and procedures to address routine housekeeping activities such as backup schedules and logging.

Network management - controls to govern the secure operation of the networking infrastructure.

Media handling – controls to govern secure handling and disposal of information storage media and documentation.

Information exchange – controls to govern information exchange including end user agreements, user agreements, and information transport mechanisms.

Access Control

Access Control addresses an organization's ability to control access to assets based on business and security requirements, including:

Business requirements – policy controlling access to organizational assets based on business requirements and "need to know."

User management – mechanisms to:

- Register and deregister users
- Control and review access and privileges
- Manage passwords

User responsibilities – informing users of their access control responsibilities, including password stewardship and unattended equipment.

Network access control – policy on usage of network services, including mechanisms (when appropriate) to:

- Authenticate nodes
- Authenticate external users
- Define routing
- Control network device security

- Maintain network segregation or segmentation
- Control network connections
- Maintain the security of network services

Host access control – mechanisms (when appropriate) to:

- Automatically identify terminals
- Securely log-on
- Authenticate users
- Manage passwords
- Secure system utilities
- Furnish user duress capability, such as “panic buttons”
- Enable terminal, user, or connection timeouts

Application access control – limits access to applications based on user or application authorization levels.

Access monitoring – mechanisms to monitor system access and system use to detect unauthorized activities.

Mobile computing – policies and standards to address asset protection, secure access, and user responsibilities.

System Development and Maintenance

System Development and Maintenance control addresses an organization’s ability to ensure that appropriate information system security controls are both incorporated and maintained, including:

System security requirements – incorporates information security considerations in the specifications of any system development or procurement.

Application security requirements – incorporates information security considerations in the specification of any application development or procurement.

Cryptography – policies, standards, and procedures governing the usage and maintenance of cryptographic controls.

System Integrity – mechanisms to control access to, and verify integrity of, operational software and data, including a process to track, evaluate, and incorporate asset upgrades and patches.

Development security – integrates change control and technical reviews into development process.

Business Continuity Management

Business Continuity Management control addresses an organization’s ability to counteract interruptions to normal operations, including:

Business continuity planning – business continuity strategy based on a business impact analysis.

Business continuity testing – testing and documentation of business continuity strategy.

Business continuity maintenance – identifies ownership of business continuity strategy as well as ongoing re-assessment and maintenance.

Compliance

Compliance control addresses an organization's ability to remain in compliance with regulatory, statutory, contractual, and security requirements, including:

Legal requirements – awareness of:

- Relevant legislation
- Intellectual property rights
- Safeguarding of organizational records
- Data privacy
- Prevention of misuse
- Regulation of cryptography
- Collection of evidence

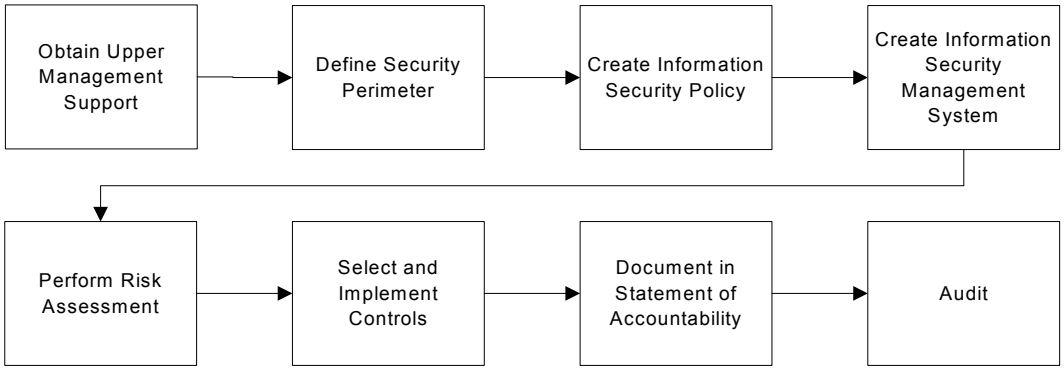
Technical requirements – mechanism to verify execution of security policies and implementations.

System audits – auditing controls to maximize effectiveness, minimize disruption, and protect audit tools.

Process

The process for implementing information security management using ISO 17799 proceeds as shown in Figure 1.

Figure 1: ISO 17799 Process



Step 1: Obtain Upper Management Support

Whether driven by regulation, the marketplace, or wisdom, the most crucial component to the success of an ISO 17799 program is gaining upper management support. The process of setting up a compliant infrastructure may be onerous, and enthusiasm and dedication may fade with time. A successful ISO 17799 implementation will instill security as an organizational lifestyle driven from the top. Information security is not a program; rather, it is a process.

Step 2: Define Security Perimeter

One of the most difficult initial tasks is to define the security perimeter, or security domain, which, conceptually, must be certified to ISO 17799. The security perimeter may or may not encompass the total

organization; however, the security perimeter must be under an organization's control. If an organization cannot control it, it cannot effectively manage it.

Step 3: Create Information Security Policy

Information security policies may take multiple forms. They may be contained in one policy document, multiple documents tailored to different audiences, or policy statements incorporated within standards. Nevertheless, the intent is the same: a high-level, implementation-independent statement showing upper management's support of information security concepts and goals.

Step 4: Create Information Security Management System

A framework – Information Security Management System (ISMS) – must be created to implement, manage, maintain, and enforce the information security process. Chartered and empowered by the upper management support evidenced in the Information Security Policy, ISMS defines the security perimeter and provides a roadmap detailing information security strategies for each of the 10 ISO 17799 control areas. These strategies may call for the creation of policies, standards, procedures, plans, committees, and teams, or for the hiring of specific personnel. It is important early in the ISMS creation process to identify and empower a Security Lead or Information System Security Officer to coordinate, oversee, and ultimately take ownership of the ISMS.

Step 5: Perform Security Risk Assessment

ISO 17799 is about management of risk, which is accomplished by developing a risk management and mitigation strategy, whereby assets, threats, and vulnerabilities are identified and the commensurate risk is quantified. Controls can then be selected to avoid, transfer, or reduce risk to an acceptable level. Security risk assessment is a method to maximize use of finite organizational assets based on measurable risk and organizational risk tolerance. Risk assessment steps are as follows:

Identify assets within the security perimeter – an asset can be a tangible item, such as hardware, or intangible, such as an organizational database. By definition, an asset has value to the organization, hence requires protection. Assets must be identified, and ownership must be established. A relative value must also be established for each asset so importance can be established when risks are quantified.

Identify threats to the assets – threats exploit or take advantage of asset vulnerabilities to create risks. Threats to each asset must be identified. There can be multiple threats for each asset. Identification of threats must be realistic. Only those threats that have a significant probability, or extreme harm should be considered. For example, a threat to the organizational database may be theft or alteration.

Identify vulnerabilities to the assets – vulnerabilities are recognized deficiencies in assets that can be exploited by threats to create risk. An asset may have multiple vulnerabilities. For example, the vulnerability to an organization's database may be a poor access control or insufficient backup.

Determine realistic probability – probabilities for each threat/vulnerability combination should be determined. Combinations with statistically insignificant probability may be ignored.

Calculate harm – harm (sometimes referred to as impact) may be quantified numerically to reflect damage from a successful exploit. This value allows the rating on a relative scale of the seriousness of a given risk independent of its probability. Harm is not related to probability.

Calculate risk- evaluation and mitigation of risk is the goal of the ISO 17799 ISMS. Mathematically, risk can be expressed as: **Probability x Harm = Risk.** This calculation results in a numeric rating of asset-based risk for a given set of threats and vulnerabilities. This numerical interpretation allows prioritization of finite risk-mitigating resources.

Note that the effectiveness of the ISO 17799 process is reliant on the accuracy and thoroughness of the Security Risk Assessment. Risk cannot be mitigated if not identified.

Step 6: Select and Implement Controls

Controls mitigate risks identified in the Security Risk Assessment. The selection of controls is predicated on availability of assets and management's ability to accept certain risks in lieu of implementing controls. This can be prioritized by the risk value identified in Step 5.

Step 7: Create Statement of Applicability

A Statement of Applicability is the portion of the ISMS that documents how risks identified in the Security Risk Assessment are mitigated by the selection of controls. This document addresses the 10 ISO 17799 control areas, and tabulates the selection or absence of controls, along with rationale as required. Whereas the ISMS says what organizations are *going* to do, the Statement of Applicability is where organizations document that it *did* what it said it would do.

Step 8: Audit

Auditing allows a review of the implementation of the information security infrastructure. Audits may be:

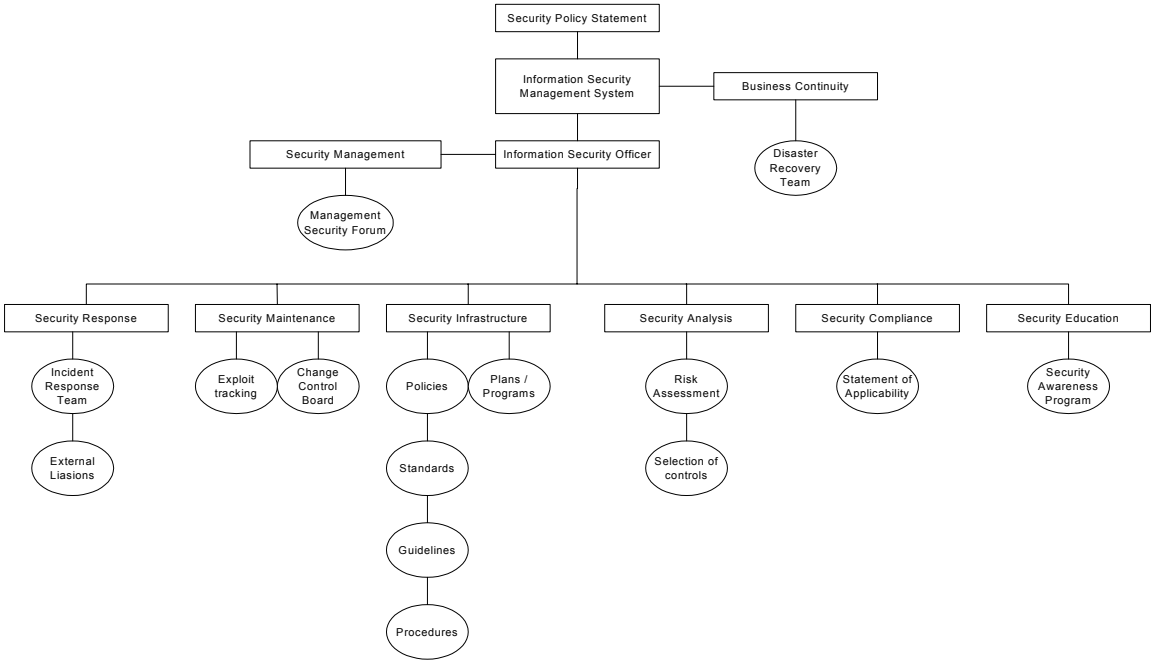
- 1st party – an organization performs the audit itself
- 2nd party – a customer or partner performs the audit
- 3rd party – an independent auditor performs the audit

Third-party auditing is required for conformance certification.

Security Organization Structure

Figure 2 is an example of an organizational security structure resulting from application of the ISO 17799 process.

Figure 2: ISO 17799 Security Organization Structure



Security Policy Statement

The Security Policy Statement is a general, top-level statement of intent for upper management, similar to a security-oriented "Mission Statement." Its intent is to show upper management's commitment to information security goals, and hence, empower the Security Organization Structure. The Security Policy Statement includes statements to the effect that the policy of the organization is that:

- Confidentiality of information will be assured
- Integrity of information will be maintained
- Availability of information to authorized users will be met.
- Regulatory and legislative requirements will be fulfilled
- Information security training will be available to all staff
- Breaches of information security, actual or suspected, will be reported to, and investigated by the Information System Security Officer.

The non-specific nature of the Security Policy Statement makes it appropriate for public disclosure.

Information Security Management System (ISMS)

ISMS is the risk management strategy of the organization. It is chartered and empowered by the Security Policy Statement, and managed by the Information System Security Officer. Within ISMS, the security perimeter is defined, the 10 ISO 17799 control areas are addressed, and a risk management strategy detailed for each control area. ISMS also serves as a reference to external supporting documentation correlating risk management documentation to the 10 ISO 17799 control areas. ISMS is an organization-specific, information security roadmap.

ISMS documentation includes:

- Security Structure Organization Chart
- Risk Management Strategy
- Information System Security Officer job description
- Management Security Forum charter
- ISMS Document Control Plan
- Security Risk Assessment
- Statement of Applicability
- Customer Code of Conduct
- ISO 17799 Document Matrix listing all applicable documents
- Security Perimeter Demarcation drawings

Business Continuity

Business Continuity Plan – an organizational impact analysis that produces a comprehensive business continuity plan, which specifies ownership and a yearly review schedule.

Disaster Recovery Team – formed as a means of testing and implementing the business continuity plan.

Information System Security Officer

An Information System Security Officer should be identified, appointed, and empowered. A formal job description defines the Information System Security Officer's principal duties, which include:

- Lead the Management Security Forum
- Lead the Incident Response Team
- Prepare Management Security Forum security briefs
- Record and resolve security incidents
- Maintain ISMS
- Establish and review the Security Risk Assessment
- Select controls and risk mitigation
- Maintain the Statement of Applicability
- Monitor ongoing compliance with security standards
- Establish and maintain contacts with external security resources
- Evaluate changes in asset base and resultant security implications
- Consult and advise on general information security issues

Security Management

The Management Security Forum consists of the Chief Information Officer, Engineering Manager, NOC or Data Center Manager, and the Information System Security Officer. Other members are included as required.

Management Security Forum duties include:

- Provide ongoing management support to the security process
- Serve as an alternative channel for discussion of security issues
- Develop security objectives, strategies, and policies
- Discuss status of security initiatives
- Obtain and review security briefings from the Information System Security Officer
- Review security incident reports and resolutions
- Formulate risk management thresholds and assurance requirements
- Yearly review and approval of the Information Security Policy
- Yearly review and approval of the ISMS

Security Response

Incident Response Team – formed to create and carry out an Incident Response Plan. The team should include diverse skill sets covering all aspects of an organization's Information Processing Systems. Tools are procured, members trained, and rosters established. The team is chartered with the Incident Response mission to:

- Prepare for an incident
- Identify an incident
- Contain the incident

- Eradicate the intruder
- Recover from the intrusion
- Learn from the incident

Methodologies include processes to:

- Identify, escalate, and de-escalate security events
- Assess organizational security
- Maintain organizational security

External Liaisons- established with local law enforcement agencies, as well as with legal and public relations entities.

Security Maintenance

Exploit Tracking - qualified specialists in different organizational networking elements are tasked with tracking relevant exploits and reporting information of concern to the Information System Security Officer.

Change Control Board – chartered and empowered to manage change. The change control process includes change submission request and evaluation, as well as recovery and back-out procedures. In addition, a Document Control plan is initiated to control the ISMS documentation.

Security Infrastructure

Policies – established to express conceptual information security organizational goals in the Information Security Policy.

Standards – established to support implementation of Information Security Policy. Standards can address:

- Personnel security
- Employee conduct
- Data classification
- Data labeling
- Data handling
- Data transmission
- Data encryption
- VPNs
- Data recovery
- Data routing
- Access control
- Firewall standard
- Network security
- Network application
- Data switching
- Logging
- Asset management
- Alarm
- Physical security

- Security maintenance

Guidelines – established to formalize adoption of information security best practices. Guidelines can address:

- Access control
- Data protection
- Router configuration
- Organizational security

Procedures – established to detail information security implementation in support of relevant standards and policies. Procedures can address:

- Risk management
- Backup/Restore
- System user add/delete/modify
- Customer provisioning
- Equipment maintenance
- Asset control
- Alarm
- Security maintenance
- Terminal server add/modify/delete
- Password/shared secret change
- Firewall setup
- Incident response

Plans/Programs – established to meet information security goals. Plans and programs can address:

- Information security awareness
- Change control
- Incident response
- Intrusion detection
- Business continuity
- Acceptance test

Security Analysis

Security Risk Assessment – performed to identify relevant assets, threats, and vulnerabilities, comprehensively and qualitatively. The Security Risk Assessment is reviewed on a schedule set by the Information System Security Officer. Figures 3, 4, and 5 provide examples of scales to quantify harm.

Figure 3: Probability of Event Scale

Probability of event	**Frequency**	**Rating**
Negligible	Unlikely to occur	0
Very Low	2 – 3 times every 5 years	1
Low	< = Once per year	2
Medium	< = Once every 6 months	3
High	< = Once per month	4
Very High	= > Once per month	5
Extreme	= > Once per day	6

Figure 4: Harm of Event Scale

Harm of event	**Degree of harm**	**Rating**
Insignificant	Minimal to no impact	0
Minor	No extra effort required to repair	1
Significant	Tangible harm, extra effort required to repair	2
Damaging	Significant expenditure of resources required Damage to reputation and confidence	3
Serious	Extended outage and / or loss of connectivity Compromise of large amounts of data or services	4
Grave	Permanent shutdown Complete compromise	5

Figure 5: Risk Scale

Risk calculation (Probability x Harm)	Rating
0	None
1-3	Low
4-7	Medium
8- 14	High
15-19	Critical
20--30	Extreme

Selection of Controls – selected based on risk rating, availability of risk mitigation assets, and management's willingness to accept residual risk.

Security Compliance

A Statement of Applicability addresses all 10 ISO 17799 control areas, detailing how risks identified in the Security Risk Assessment were either mitigated via selection of controls, or accepted. Due to the broad and general nature of the ISO 17799 standard, not all control areas are applicable to every organization. Furthermore, management may decide that acceptance of some risks is preferable to the cost of mitigation. The Statement of Applicability is where security decisions are rationalized and documented. It documents due diligence and rational decision-making.

Security Education

Security Awareness Program – personnel must have the knowledge to understand the significance of their actions. Human interaction may act in ways that undermine security controls, causing security breaches. A Security Awareness Program is chartered to:

- Clarify why security is important and controls are needed
- Clarify employee security responsibilities
- Serve as a forum to discuss security questions

The Security Awareness program should include "new hire" orientation, and ongoing refresher activities.

Conformance Certification

ISO does not participate in conformance assessment activities. However, its standards and guides harmonize conformity assessment worldwide through independent third-party auditors. ISO promotes the international harmonization of conformance assessment activities and the worldwide acceptance of the results through ISO/CASCO, its general policy committee on conformance assessment. CASCO has an international membership representing 87 countries in both participant and observer status. CASCO also has liaisons to many other international testing and accreditation agencies and technical committees. The

U.S. representative to the ISO is ANSI (www.ansi.org). ISO 17799 falls under the aegis of the ISO Joint Technical Committee 1 Sub Committee 27 (JTC 1/ SC 27).

Conformance Audit

At the present time, a mechanism to audit an organization for conformance to ISO 17799 does not exist. The standard is based on suggestions in lieu of requirements, hence is unsuitable for audit. Until a supplement based on requirements emerges, there is nothing against which to audit. This will undoubtedly change in the future as demand rises, but at present, organizations requiring certification are implementing to ISO 17799 and certifying to the requirements of BS 7799 Part 2. We can surmise that an ISO 17799 audit mechanism will eventually appear similar to the BS7799 Part 2 model.

BS 7799 Certification Model

In the BS 7799 certification model, authority starts with the National Accreditation Board of each respective country. Examples are UKAS in the United Kingdom, and RvA in the Netherlands. The respective National Accreditation Boards accredit individual auditing firms, and in some cases individuals, as a Certification Body, authorized and competent to audit against BS 7799 Part 2 standard requirements. The Certification Body then audits the organization against BS 7799 Part 2, leading to BS 7799 Certification. The validity of the certificate is ultimately derived from the National Accreditation Board of the respective country.

Non-Accredited Certification

In some areas, including the U.S., the National Accreditation Board does not accredit a Certification Body to BS 7799. Without an accredited Certification Body, it is impossible to certify to BS 7799. An organization may choose to have a non-accredited Certification Body perform the certification, in which case, the validity of the certificate is derived from the reputation of the non-accredited Certification Body. Alternatively, an organization may elect to be certified by an accredited Certification Body, accredited by a National Accreditation Board from another country. The validity of the certificate is derived from the National Accreditation Board of the other country. International auditing firms have taken this approach.

Conformance Maintenance

Based on the BS 7799 model, we can surmise that conformance maintenance will follow the same or similar requirements. In BS 7799 Part 2, a nationally accredited Certification Body that issued the original Certificate of Conformance must approve changes to the security infrastructure defined within the Statement of Applicability. Minor changes may be submitted in writing, furnishing the evaluator with enough detail to determine impact. Major changes may require re-auditing. Surveillance visits are performed every six months, and a re-certification audit is required every three years.

Conclusion

Internationally accepted information security standards are still in their infancy, and undoubtedly ISO 17799 will evolve over time as deficiencies are addressed. The recently formed Center for Internet Security (www.cisecurity.org), a consortium of more than 100 organizations chartered to deal with due diligence, among other issues, has adopted BS 7799 as a foundational standard. The flexibility of ISO 17799 is such that work done toward it should transfer to any emerging information security standard that may be deemed preferable in the future. ISO 17799 is, after all, nothing more than applied and documented “best practices.”

We expect to see an ever-increasing demand for information security certification. This phenomenon will be driven by many factors, including:

- Regulatory requirements, such as HIPAA
- Marketing incentives, particularly in e-commerce and finance
- Financial incentives, such as insurance premium reductions
- Corporate "due diligence" concerns

All of these examples represent growth opportunities and challenges to all practitioners and students of information security.

About INS

INS (International Network Services Inc.) is a leading global provider of vendor-independent network consulting and security services. We offer a full range of consulting services to help companies build, optimize, manage, and secure their network infrastructures to enable their business initiatives and achieve a sustainable operating advantage. INS is a recognized leader in complex, multi-vendor network consulting, having helped more than 75% of the Fortune 500 and delivered more than 15,000 engagements over the past decade. Headquartered in Santa Clara, CA, INS has regional offices throughout the United States and Europe. For additional information, please contact INS at 1-888-767-2788 in the U.S., 44 (0) 1628 503000 in Europe, or 1-650-318-1020 worldwide, or visit www.ins.com.