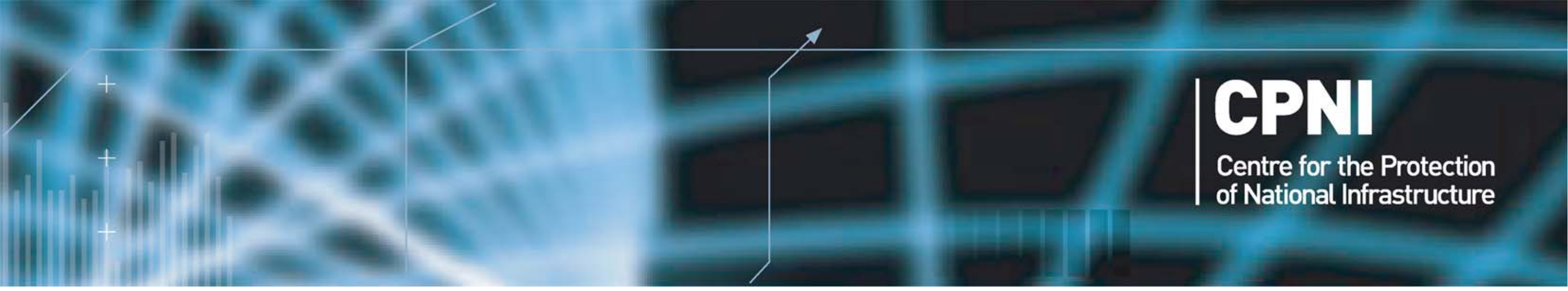

# RISK MANAGEMENT AND ACCREDITATION OF INFORMATION SYSTEMS

## ALSO RELEASED AS HMG INFOSEC STANDARD NO. 2

**AUGUST 2005**

This paper was previously published by the National Infrastructure Security Co-ordination Centre (NISCC) – a predecessor organisation to the Centre for the Protection of National Infrastructure (CPNI).

Hyperlinks in this document may refer to resources that no longer exist. Please see CPNI's website (www.cpni.gov.uk) for up-to-date information.

### Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

# RISK MANAGEMENT AND ACCREDITATION OF INFORMATION SYSTEMS

**Contents** **Page**

| | |
|---|---|
| Approved by IIC | March1998 |
| IAPC approved review process begun | March 2003 |
| Issue 2.0 Approved by IAPC | May 2005 |

# CUSTOMER FEEDBACK FORM

As this Guide has undergone a significant revision, **it will be subject to review in January 2006** (6 months after publication) by the Security Accreditation Review Committee, on behalf of the IA Policy Committee. Thereafter the Guide will be reviewed on an annual basis.

It is important that we receive your feedback, especially during the initial 6 month period, to inform the 1st review and would encourage you to forward any comments and suggestions you may have to NISCC using this form.

Infosec Standard No. 2 Review
Customer Support
CESG
A2j
Hubble Road
Cheltenham
GL51 0EX

Tel: +44 (0)1242 709 141

Fax: +44 (0)1242 709193

E-mail: enquiries@cesg.gsi.gov.uk

PLEASE PRINT

| |
|---|
| **Name:** |
| **Department/Company Name and Address:** |
| **Your Contact Details:** |
| **Comments:** |

Please continue overleaf if required

**Comments (continued):**

# EXECUTIVE SUMMARY

1. **Information Assurance** (IA) is the confidence that information assets will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

2. This new **NISCC Guide** provides policy and guidance on the **IA risk management and accreditation of Information Systems (IS)**. Accreditation is the process by which an IS is assessed against its security requirements resulting in a decision to accept the risks arising from its operation.

3. The Guide contains very little that does not already represent best practice and plain common sense in this field. However, what it does provide for the first time is a single source of policy and guidance which:

- draws the different strands together and places IA in core business;
- provides advice and guidance on the process of risk management;
- targets a wide audience (not just security specialists and not just central government).

4. **IA risk management and accreditation offer significant benefits** to organisations in terms of informed decision making, resource savings and efficiency, business advantage and reputation. This does not come without cost: compliance with the standard may require additional resources, particularly in organisations where there has been under-investment in IA in the past.

5. **IA is a fundamental requirement of business today.** Information is an essential asset – loss or failure of an IS can have catastrophic consequences and some organisations may not recover from such an event. This Guide places IA centrally within core business and explains the principles and process of IA risk management and accreditation in terms of current business practice. It provides clear linkage to the stages of projects (aligned to the OGC Gateway $^{TM}$ Review Process) and to business processes throughout the lifecycle of the IS.

6. **Risk management involves everyone in an organisation** and continues throughout the lifecycle of the IS. It is equally important for government and non-government organisations. This Guide is intended for a wide audience, not just central government departments or security personnel. It is not prescriptive and recognises that organisations have different requirements and structures, so it focuses on functions not posts and provides practical advice on the implementation of a cost effective and efficient risk management regime.

7. **Risk ownership resides at the very top of an organisation**, in line with the Cabinet Secretary's requirement for all government departments to have a Senior Information Risk Owner (SIRO) on the senior management board. The Guide reinforces this requirement and places the SIRO function in context. It provides practical guidance on procedures for escalating decisions to higher levels.

8. **Legal compliance is a corporate responsibility**. It should be treated as an integral element of the proper management of IS and all IA measures. It is also a core element of good corporate governance. Non-compliance is likely to have significant impact on an organisation's business objectives and damage to its reputation. The Guide highlights this and gives guidance on relevant laws.

9. Following best practice as described in this Guide will also help an organisation to demonstrate **compliance with ISO17799** and assist in certification to BS7799 Part 2.

10. **Risk management is for life, not just for Christmas!** It is an iterative process throughout the lifecycle of the IS, from early planning, through development to in-service and eventually decommissioning and disposal. This Guide links to business processes, and makes it quite clear that accreditation is a continuous process – not a snap-shot in time. This will lead to improved IA and avoid costs often associated with late consideration of security requirements.

11. **The policy and processes are applicable to all IS**. In the past IA accreditation focused on IT (computers) has failed to address communications systems and other information assets. This has lead to confusion, duplication of effort and inconsistency. The new "unified" policy and process covering the range of IS, should lead to rationalisation of resources and activities across an organisation.

12. **Confidentiality, integrity and availability are all equally important**. Although integrity and availability have always been key considerations in IA, policy has tended to focus on confidentiality. This Guide ensures that all three are fully addressed and given equal importance. It recognises that many assets may have little or no requirement for confidentiality but availability and integrity may be vital and also that confidentiality extends beyond government protective markings to privacy and other sensitivities.

13. **Risk management and accreditation require a disciplined thought process** but have often been treated as a paper exercise. This Guide promotes understanding of the fundamental concepts, leading to improved flexibility and scalability, and places IA firmly in the business decision making process.

14. **This process must be supported by evidence**. It is not sufficient simply to state security requirements. Compliance must be validated and verified throughout the lifecycle of the asset. This Guide provides guidance on the use of evidence to gain a real understanding of the strengths and weaknesses of an asset and the business impact of compromise, and to provide justification and accountability for risk management decisions and a benchmark for compliance monitoring.

15. **Accreditation should be an informed decision**. In the past, accreditors may have erred towards risk avoidance because they have been left to take responsibility for decisions without adequate support from senior management. Conversely, senior managers faced with reduced budgets may have accepted risks without understanding of the real impact or consequences. This Guide makes it clear that accreditation must be an informed decision, made in full understanding of the implications and taken at the right level of management.

# INTRODUCTION

## How to use this Guide

16. The document is divided into 3 parts:

    Part 1 - Governance and Risk Management Concepts
    Part 2 –Risk Management and Accreditation Process
    Part 3 – Risk Management and Accreditation Documentation

17. Part 1 explains the importance of governance and presents the concepts of risk management, in progressive stages, allowing the reader to develop a clear understanding of the subject, leading to meaningful and considered risk management decisions in the context of Information Assurance.

18. Part 2 steps the reader through the process of risk management in the Information System (IS) lifecycle. This provides clear correlation to the project, procurement and business management processes. It is designed as a guide and aide-memoir and should only be used once sufficient understanding and has been gained from Part 1.

19. Part 3 offers a suggested format and identifies typical content of risk management and accreditation documentation. It also provides linkage between deliverables and the risk management process.

20. This Guide includes a comprehensive Glossary containing terms and abbreviations used within the document.

## Intended Readership

21. This Guide is written for all those involved in the risk management of IS, including information risk owners and business managers, security managers and accreditors, project managers and system or service providers.

22. It describes best practice, which should be applicable and helpful to a wide audience, including central and local government, industry, commerce and the wider public sector.

## Feedback and Review Process

23. This Guide will be reviewed 6 months after publication and thereafter will be subject to a regular annual review. Readers are encouraged to submit comments, amendments and other feedback for input into the periodic reviews and continuing appraisal of this. A Customer Feedback Form is provided at the beginning of this document.

THIS PAGE IS INTENTIONALLY LEFT BLANK

# PART 1: GOVERNANCE AND RISK MANAGEMENT CONCEPTS

## A. General Overview

24. Information Systems (IS) are intrinsically linked to most organisations' ability to perform their business function and hence the protection of these assets is critical to the organisation's duty of care and governance.

25. Information Assurance (IA) is the confidence that information assets will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. This is integral to an organisation's business strategy and business planning and needs to be accepted as the responsibility of senior management strategic and planning bodies, to enable issues to be identified at the earliest stages of business planning. Ultimate responsibility for IA resides with the Chief Executive or equivalent.

26. The risks to an organisation's IS are very real and although many incidents may have only a minor impact, some have the potential to cause much greater damage or loss, significantly affecting the organisation's operational performance and reputation. It is therefore essential that such risks are identified, understood and appropriately managed.

27. An IA risk management strategy will need to involve all areas of the business and incorporate a balance of preventative, contingency and recovery measures commensurate with the business requirements. These measures and the effectiveness of the strategy should be demonstrable within the organisation itself and evident to its business partners and customers.

### What is an Information System?

28. For the purposes of this Guide, an IS may include the following:

- physical environment (e.g. buildings, equipment, cables, etc.);
- information and data;
- software;
- service provision;
- people;
- intangibles (e.g. reputation, goodwill).

### Governance and Risk Management

29. Good corporate governance requires effective risk management structures and processes, which are frequently reviewed, helping to gain the trust of others with whom the organisation wishes to develop current and future business opportunities. ISO17799 is the International Standard that defines the management system required to deliver IA. This Information Security Management System (ISMS) is the management system supporting the security of the assets within the defined BS7799 scope[1]. It will consist of people, meetings and an organisation structure. It will also define where responsibility rests for ensuring that documents within the BS7799 scope link into and are compliant with overarching corporate policy.

[1] ISO17799 is the International Standard for information security management but certification currently only exists to BS7799 Part 2.

30. This Guide acknowledges ISO17799 and provides a framework that is compliant with its requirements. Following this guidance should ease the route to certification to BS7799 Part 2. However, it should be noted that this NISCC Guide is directed at information assets whereas ISO17799 considers business processes. (See also Appendix A "Cross Reference between NISCC Guide and ISO17799 Control Objectives").

31. IA risk management is critical in the discharging of the responsibility for corporate governance. It should aim to prevent incidents wherever possible and to mitigate the adverse effects of unavoidable incidents through measures to detect, respond to and recover from incidents effectively and efficiently. It provides an organisation with the assurance that its IS can be trusted to support its business activities in an effective and reliable manner. Evidence of an effective risk management regime may also be required when interconnecting to IS shared or owned by other organisations.

32. Risk management is a core business function affecting all staff and comes under the overall responsibility of the Senior Information Risk Owner (SIRO). It is an iterative process throughout the lifecycle of the IS, whereby the risks are identified, understood and managed in a manner that satisfies legal and business requirements. Residual risks must be carefully considered and only be accepted on the basis of an informed decision made in full understanding of the implications.

## Accreditation

33. Accreditation is the formal assessment of the IS against its IA requirements, resulting in the acceptance of residual risks in the context of the business requirement. It is a prerequisite to approval to operate.

34. It must be an informed decision made in full understanding of the implications to the business and should take place prior to final acceptance of the IS. Accreditation must be reviewed periodically throughout the service life of the IS.

35. An IS is deemed to be accredited when the accreditor confirms that, by meeting the IA requirements in the following areas, the associated residual risk is acceptable to the business:

- **Confidentiality** – ensuring the information is accessible only to those authorised to have access;
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods - this may include the ability to prove an action or event has taken place, such that it cannot be repudiated later;
- **Availability** – ensuring that authorised users have access to information and associated IS when required.

36. There may be instances where confidentiality, integrity and availability, requirements are in direct conflict. Where conflicting requirements arise, the accreditor must ensure that risk management decisions are escalated to the appropriate level. Where there is significant residual risk, the decision should be escalated to the SIRO.

## Legal Compliance

37. Ensuring compliance with statutory requirements, for example laws such as the Data Protection Act and Human Rights Act, is a significant control used in the corporate governance process and therefore in the risk management of IS. Non-compliance with the law and other relevant regulations is likely to have significant impact on business objectives and reputation. On the other hand, evidence of good corporate governance and risk management may be critical in certain cases to support an organisation in a prosecution or a defence. The main laws relevant to IS are outlined

in Appendix B but this is merely illustrative and organisations should ensure that they obtain timely legal advice specific to their circumstances.

## B. Responsibilities and Functions

38. ISO17799 recognises that governance is key to good Information Assurance (IA) and therefore requires that ownership of the risk must reside at the very top of an organisation with the senior management board. In support of this, a member of the board must assume the role of Senior Information Risk Owner (SIRO) for the organisation.

39. In practice, as shown in Figure 2, governance, risk management and accreditation involve a variety of different types of work, levels of business knowledge and technical expertise. Equally, allocation of different functions will vary between organisations. What is important is that responsibilities are clearly assigned and fully accountable and that those involved are adequately trained and work in close cooperation. Where services are outsourced it is essential that appropriate risk management processes and functions are specified in the contract.

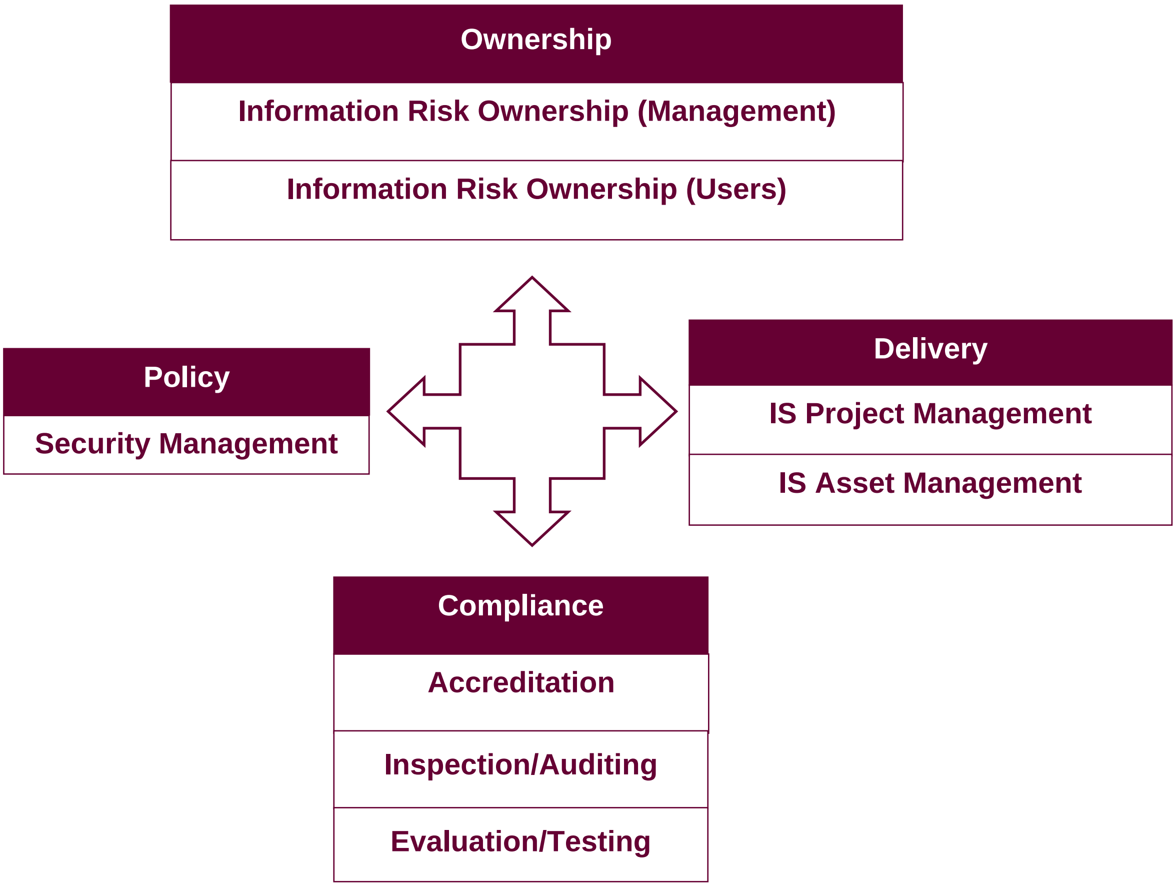

**Figure 1: Risk Management Functions**

### Ownership

40. IA risk management is everyone's business, hence all members of an organisation must take some responsibility for information risk ownership of specific IS, with which they are associated, from the senior management board, represented by the SIRO, to the individual users. Different specific roles may be assigned to ensure effective acceptance of information risk ownership in terms of the management and use of the IS, which include policy, compliance and delivery functions within an organisation.

### Information Risk Ownership (Business Management)

41. The SIRO should understand the strategic business goals of the organisation and how these may be affected by failure of IS, in order to ensure that information risks are weighed alongside other factors, such as financial, legal, operational risks. This determines an organisation's "risk appetite" – effectively determining the acceptable level of risk at corporate level. On the basis of this, IA responsibilities will be assigned to management levels in accordance with its importance to the organisation and will similarly gauge the level of awareness.

42. Management functions include ensuring that:

a. The right organisational structure and funding are established, to deliver appropriate and effective IA and the prerequisite security culture, including an effective process for achieving security awareness and the training and qualification of employees with delegated security responsibilities.

b. IA requirements are addressed in strategic planning and are accepted as an essential and integral part of the business requirement, supported by appropriate corporate security policies, to deliver consistency across an organisation and compliance with relevant laws and standards;

c. An organisation has adequate plans for business continuity, disaster recovery and forensic readiness and these are regularly exercised and reviewed;

d. There is an appropriate assurance process to monitor the effectiveness of all corporate IA policies and plans;

e. All risk management decisions are accountable and appropriate to the business requirements and are made in full understanding of the implications and potential consequences;

f. An escalation process through to the SIRO, in cases of conflict between IA and other business requirements (see also "Escalation" as described in Section F) and that all those responsible are aware and understand this process.

### Information Risk Ownership (Business Users)

43. Business users are responsible for the protection of IS they use in accordance with defined policy and for helping to maintain the effectiveness of policy and procedures in the face of changing business practices. They must ensure that:

a. They are familiar with corporate security and IA policies;

b. They have read and understood the security policies and user guidance specific to the IS they are using (e.g. acceptable use policy, incident reporting procedures) and that they comply with these.

44. Business users should also be encouraged to raise any issues regarding the impact and effectiveness of security policies, technical measures or user guidance promptly.

## Policy

45. Responsibility for management and implementation of an organisation's security and IA specific policies should be assigned to specific personnel, with the appropriate level of knowledge and expertise, under delegated authority from the senior management board.

### IA Policy Management

46. Within the context of an organisation's security management, the functions for IA policy management include:

- Co-ordination of IA on behalf of the organisation, including physical, procedural and personnel aspects where appropriate, and interface and co-ordination with other organisations on IA matters;
- Preparation and management of the corporate IA policy to meet the business requirements and comply with international and national standards, policies and laws, as appropriate;
- Advice within the organisation to all those involved in risk management on IA issues and policy in general and IA in specific implementations;
- Management of IA awareness and training;
- Management of IA incident reporting and recovery operations.

## Compliance

47. IA Compliance is the verification and confirmation that an individual IS meets its specific IA requirements throughout its lifecycle. It is therefore unacceptable that any entities responsible for the delivery of IS undertake compliance functions, which should not be confused with routine checks and inspections conducted as part of the IS management. IA Compliance functions may be assigned to appropriately skilled personnel in any other areas of the organisation.

48. In addition, the decision whether or not to accept the residual risk, also known as accreditation, cannot be outsourced. A contractor may be assigned accreditation functions but an organisation must always reserve to itself the right and responsibility to decide what constitutes an acceptable risk to its business.

### Accreditation

49. IS accreditation on behalf of an organisation confirms that an IS complies with the corporate IA policy and their specific IA requirements and that the residual risk is acceptable. In cases of conflicting requirements, where levels of residual risks are outside the corporate policy, this decision will be escalated as appropriate.

50. Accreditation functions include:

- Advice and guidance on the IA risk management and accreditation requirements of specific IS throughout the lifecycle;
- Advice on preparation of the Risk Management and Accreditation Document Set (RMADS) and approval of the RMADS, including all changes, throughout the lifecycle of the IS - this includes staged approval, as appropriate, of the various sections or documents;
- Confirmation that the proposal, contract and IA risk management plan meet the IA requirements, prior to contract let;
- Specification and management of compliance verification and validation during the IS lifecycle (e.g. periodic inspections or IT Health Checks);
- The accreditation decision based on adequate verification and assessment of residual risk, prior to acceptance of the IS and periodically throughout its in-service life, and issue of the accreditation statement;
- Reporting business impact of residual risks to the appropriate information risk owner;
- Confirmation of IA compliance on decommissioning and disposal.

### Audit and Inspection

51. IS require independent audit and inspection as evidence for accreditation and for continuing risk management throughout their lifecycle. These activities may encompass a number of different disciplines including:

- Quality assurance;
- Physical, personnel and procedural security;
- Communications security;
- Verification of structural, mechanical and electrical installation requirements and ensuring their correct configuration;
- Inventory control;
- Cryptographic key management;
- User audit.

52. This regular audit process will support an organisation's conformance to the BS7799 Plan-Do-Check-Act (PDCA) virtuous circle.

### Evaluation and Testing

53. IS will require independent evaluation and testing, as evidence for accreditation and for continuing risk management throughout their lifecycle. Such activities will be required on a regular basis as part of ISO17799 compliance and may also be required as a result of an incident. As in the case of audit and inspection, activities encompass a number of different disciplines and may include:

- Evaluation of technical implementations and configuration during acceptance testing, changes and upgrades;
- Electromagnetic compatibility and security;
- Vulnerability checks for accreditation;
- Tests, inspections and IT Health Checks for continuing risk management and accreditation in-service or as a result of an incident.

## Delivery

54. There are 2 distinct sets of management disciplines involved in delivery:

- IS project or programme, responsible for the delivery of the IS through to acceptance, and
- IS in-service.

There will be a period of overlap of responsibilities between these disciplines during the acceptance process and until such time as the project or programme team is dissolved.

55. As already stated under “Compliance” above, entities involved in delivery cannot undertake any IA compliance functions, although they will be responsible for monitoring correct IS management and use.

### IS Project or Programme Management

56. During the project, programme and procurement cycles, the project (or programme) manager is responsible for ensuring the successful delivery of the IS to meet the agreed business requirements (including IA) on behalf of the organisation. This requires close co-operation with the accreditor to ensure co-ordination of IA specific and other project activities and timely provision of IA deliverables.

57. In large and complex projects and programmes, IA functions are often assigned to a specialist, for example a security assurance co-ordinator or a programme security executive. Functions include:

- Adoption of a project management and procurement process, which explicitly incorporates IA and meets the organisation's corporate IA policy;
- Preparation, maintenance and timely provision of the appropriate sections of the RMADS in close interface with all stakeholders, especially the accreditor, to ensure correctness and acceptance of deliverables
- Appropriate statement of IA requirements in project and other development plans, contracts and funding requirements (including provision for through life costs) and ensuring that IA requirements are included in bid assessment, contract decision and IS acceptance criteria;
- Immediate notification of non-compliance with the IA requirement and negotiation with accreditor and other parties as appropriate;
- Ensuring IA accreditation is a prerequisite for final acceptance;
- Formal handover of the IA functions to IS management post-acceptance;

58. By taking onboard the above responsibilities and formalising them within an Information Security Management System (ISMS), the project or programme manager will go a long way to achieving compliance with ISO17799. The supporting documentation should provide suitable evidence towards formal BS7799 Part 2 certification.

### IS Management

59. On final acceptance, responsibility for the IS transfers from project/programme to IS management. Throughout its service life to decommissioning and disposal, the IS manager is responsible for ensuring the effective operation of the IS, to meet the agreed business requirements (including IA) on behalf of the organisation. This requires close co-operation with the accreditor, to ensure co-ordination of IA specific and other management activities.

60. Particularly in the case of large and complex IS, a dedicated specialist post may be required to manage the IA requirements. Functions include:

- Management, maintenance and configuration control of the IS and its RMADS, in compliance with the organisation's corporate IA policy and within the terms of its accreditation, as defined in the RMADS[2];
- Ensuring users understand their responsibilities by regular distribution of the approved security operating procedures (SyOPs) and monitoring compliance by regular security audit and inspections of logs and other records;
- Patching of applications and operating systems software, regular updates to security products and ensuring such products are implemented effectively to provide the required level of security;
- Management of incident reporting, investigation and recovery of the IS, reporting within the organisation and to the national schemes as appropriate;
- Preparation of IA deliverables for compliance inspections and accreditation review;

[2] In the case of large and complex IS, it is usual to form a panel or configuration control board with representation from the IS management and the accreditor

- Management of decommissioning and disposal in accordance with IA requirements.

## IA Committees, Panels and Groups

61. Various types of groups, panels and committees may be established to carry out the function of accreditation or assist in the process, for example a security working group and an accreditation panel. Requirements will vary considerably depending on the size, complexity and interconnectivity of the IS concerned. However, at a minimum an Information Security Forum (ISF)[3] should be established, to manage security issues as they arise and develop policy on behalf of the organisation.

[3] The ISF is the BS7799 scope-level security management body.

## C. Corporate IA Policy

62. Corporate security policy is essential to ensure good security governance and consistent implementation of security standards. It supports an organisation's strategic aims and objectives and should enable members of the organisation to identify an acceptable level of risk, beyond which escalation of risk management decisions is always necessary.

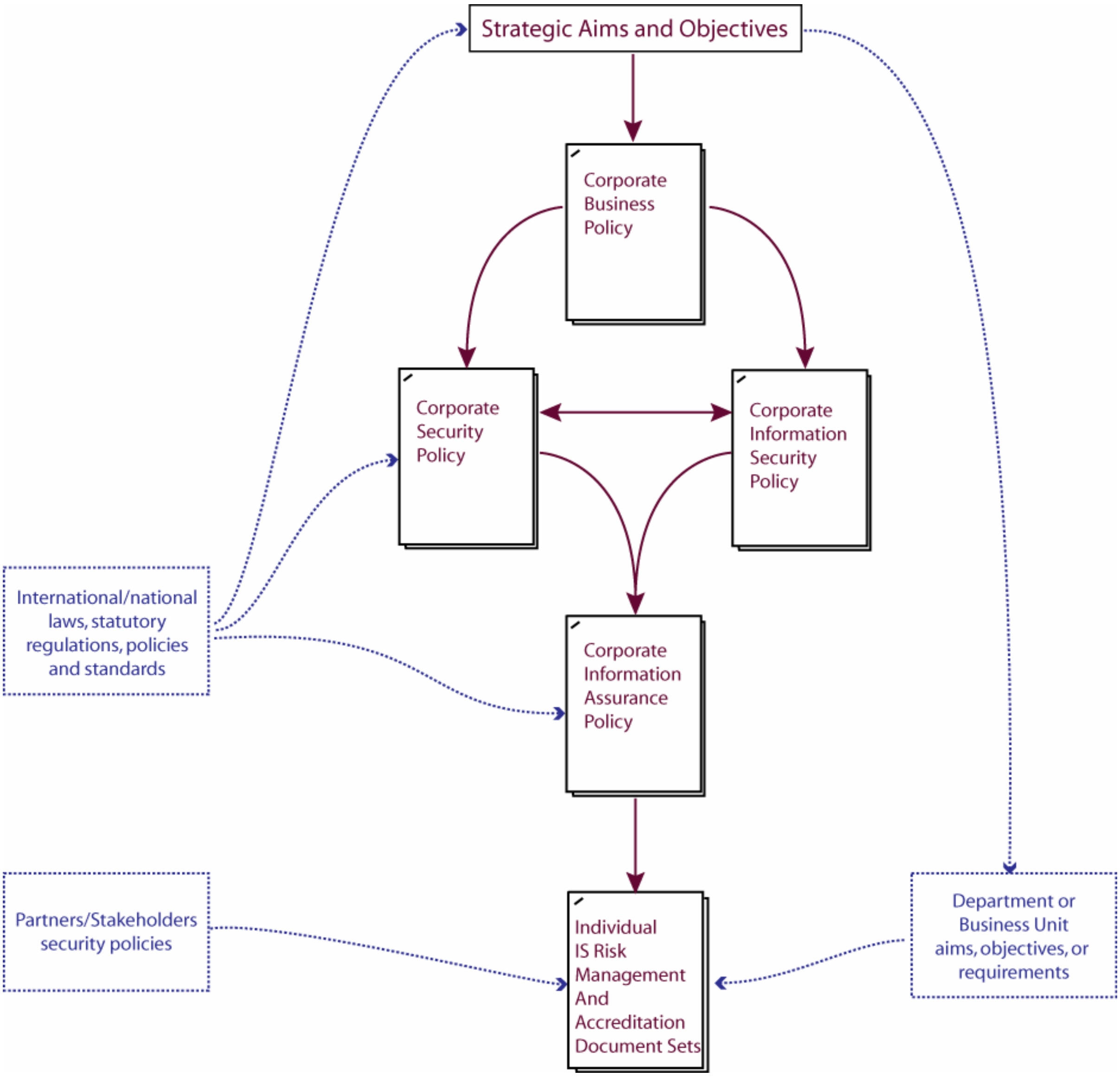
Strategic Aims and Objectives
Corporate Business Policy
Corporate Security Policy
Corporate Information Security Policy
Corporate Information Assurance Policy
Individual IS Risk Management And Accreditation Document Sets
International/national laws, statutory regulations, policies and standards
Partners/Stakeholders security policies
Department or Business Unit aims, objectives, or requirements

**Figure 2: Example Corporate and IA Risk Management Policy Interaction**

63. All corporate policies and strategies are owned by the senior management board. The Senior Information Risk Owner (SIRO), on the board's behalf, is responsible for developing and implementing of those corporate strategies and policies relating specifically to security and for reviewing them regularly, to ensure that they remain appropriate to the changing requirements. The strategies and policies will include a corporate security policy, which establishes an organisation's minimum standards for all aspects of security, and a corporate IA policy. The BS7799 Information Security Management System (ISMS) could provide the foundation on which these corporate policies are based.

64. The corporate IA policy should cascade from the corporate security policy and corporate IS policy to reflect the organisation's requirements and constraints, including laws, statutory regulations, standards and other policies as shown in Figure 2 above, including security policies of partners or stakeholders where applicable. It should include clear links to an organisation's plans for business continuity, disaster recovery and forensic readiness.

65. The corporate IA policy provides a framework for all risk management decisions associated with the organisation's IS and a business view of what constitutes an acceptable level of risk, as well as minimum standards for interconnections. As such, the security standards set in this policy must be sufficiently generic to be applicable across an organisation, whilst providing sufficient detail to ensure consistency across a range of environments and IS within an organisation. Where the threat is constant across an organisation, it may also contain a corporate threat assessment.

66. By ensuring a consistent approach to prioritising and mitigating risks, the corporate IA policy will reduce the need for the SIRO to be involved in low-level risk management decision making. Only where deviation from the policy becomes inevitable should it be necessary to escalate decision making to the SIRO. Well defined and documented corporate IA policy should also reduce effort and costs associated with the accreditation of individual IS by reducing the requirement for extensive, duplicative and often inconsistent risk management documentation at that level.

67. The policy should be held under constant review and should include:

- IA organisational structure with specific roles and responsibilities, where appropriate;
- empirical threat assessment of the organisation;
- IA risk management strategy (corporate approach to risk) and details of the risk assessment method used by the organisation;
- escalation policy and procedures for risk management decisions;
- requirements for security awareness and training;
- minimum requirements for inspections, checking, monitoring and audit;
- incident reporting and recovery policy and procedures;
- configuration control policy including regime for security management;
- minimum requirements for continuing accreditation (accreditation maintenance).

## D. Scope of Accreditation and Interconnection Policies

68. The key objective of risk management is to identify Information Assurance (IA) risks and manage them appropriately within the context of the business requirements. Before embarking on the process, careful thought should be given to the overall scope of the work, in terms of physical and logical boundaries and how best to approach the task, in order to ensure that it is meaningful, effective, efficient and fully accountable. One approach does not fit all and the method adopted should best reflect the business, IA and legal requirements of the particular situation.

### Scope

69. All parties concerned must be clear about what is being accredited and have a realistic understanding of the business context for accreditation. This is a reasonably simple exercise when business function, user group, location, equipment and software boundaries are roughly the same - an individual Information System (IS) may be taken as the scope or “unit” of accreditation. However, most cases are considerably more complex, involving large or distributed networks, disparate user groups and business functions, and a multiplicity of interconnections. Nevertheless, one basic rule will always apply: to be within the scope, entities must be within the management responsibility of the organisation or community**, i.e. entities wholly outside the control of the organisation or community cannot fall within the boundaries of the accreditation**.

70. Similarly, the scope for ISO17799 compliance must be bounded by the area of management responsibility. Whilst Service Level Agreements (SLAs) and contracts will exist with external entities, it is how these interfaces are managed and inspected that will matter.

71. This does not mean that relevant external entities should be ignored. Communication across accreditation boundaries and any relationship with external IS must be considered and will need to be addressed in risk assessment and risk management. For example, the scope of accreditation of a corporate information system connected to the Internet will need to take account of the risks of this interconnection. The responsibility of the organisation (and therefore the boundary of the accreditation) is for its own system and the interconnection (either separately or together) but clearly not accreditation of the Internet itself, which lies outside its management jurisdiction.

72. The accreditation boundary may be defined by describing the limits to the system. These limits may be defined in a number of ways: business (organisational, functional), physical (site, computer, network), logical (connectivity, service, or software), contractual (an outsourced system or service), or a combination of these. The detail of the limits may need to be described in terms of both inclusion and exclusion, such as including a software package but not the PC it runs on.

73. A simple schematic diagram representing the various main components, connections, information flows and boundaries – including any sensitivities – is essential, early in the planning process. It can be further developed as the various factors are considered and should be included with the eventual accreditation documentation.

74. Before determining the boundaries of a particular accreditation, it is useful to consider the following factors:

- Is it better to handle a number of systems, components, locations, etc. as a single accreditation, in order to avoid potential replication of effort and inconsistency, or accredit each one separately?

- When traversing different accreditation management domains, what are the requirements and implications for joint or combined accreditation and how will these impact on the business requirement?

## Approaches to Accreditation

75. This subsection explores some of the possible approaches to risk management and accreditation of IS, which may streamline the process and help to avoid nugatory work or duplication of effort. Even in the case of a single IS, approaches may differ depending on size and commonality with other IS within the organisation and intended business use. A tiered or hierarchical approach to risk management and accreditation documentation will help to avoid a multiplicity of nearly identical accreditations, which waste significant resources in the preparation, review and maintenance of a series of near-identical documents and can also lead to inconsistencies in IA practice.

76. Overarching IA policies and standards and business continuity plans based on a corporate risk assessment, applicable to all networks, systems and services will usually be the most cost-effective approach, but these should not be applied mindlessly and there will usually be some exception requiring specific action.

77. Accreditation documentation developed for any asset or group of assets should include a statement of compliance or otherwise with the corporate IA policy and any other applicable overarching security policies. The documentation will then only need to include the detailed information specific to the individual IS and not covered in the overarching policy. The greater the detail included in overarching policy, the less will be required at individual IS level with corresponding reduction in time expended on individual accreditations.

78. If the IS is non-compliant in any way, this should be detailed in an exception report. The accreditor must then decide not only whether this is acceptable in terms of the IS itself but also whether to request a change to the over-arching policy and/or to escalate the decision-making process.

79. Interconnection of IS is an important consideration. Many organisations have a number of internal networks, most of which are interconnected and many of these will support connections to other networks outside the organisation or management domain. A clear definition of accreditation boundaries and data flows is essential to understand the risk of these interconnections.

80. When scoping or defining these boundaries, consideration should be given to the best methods of managing risk, including ownership, and accreditation. Effective management of IA risks will not only ensure optimum security but also aid business efficiency.

### Individual IS

81. A common type of accreditation is that of an individual IS. However, after scoping, care should be taken to scale the accreditation as appropriate to the IS in question. For example, a large and complex system or network may require a very detailed Risk Management and Accreditation Documentation Set (RMADS), whereas a laptop may only require documented confirmation of compliance with the corporate IA policy.

### Accreditation of Similar IS

82. Many systems are replicated, for example, at a number of branch offices or in similar mobile platforms, such as ships and aircraft. In these cases, a generic or proforma RMADS could be produced, containing all the common details. This could then be

used to produce customised local versions that address the different aspects and requirements of each location.

83. Alternatively, if the same accreditor is responsible for all locations and the IS are under central management, a single generic RMADS could be sufficient, with a number of appendices giving the site-specific information.

84. Generic accreditation documents could prove a useful method for accreditation of mobile systems (e.g. telephones, personal organisers, laptops or combinations of these). However, generic or proforma documents should only be used where there is significant commonality. The usefulness of this approach should be carefully balanced to avoid any tendency towards a tick-sheet exercise without thought for the real issues and should never be treated as a simple cloning exercise.

### Collective Accreditation

85. If hardware is constantly being upgraded and replaced in a specific location, for example a communications facility or exchange, and the threats and vulnerabilities remain unchanged, the hardware could be accredited collectively. This would allow new hardware to be handled under configuration change control instead of carrying out a new accreditation. Proposed changes should be assessed for their security relevance and the accreditor would then decide whether this required re-accreditation.

86. Although potentially useful and efficient in certain circumstances, collective accreditation should be approached with caution, as it requires rigorous management and a good security ethos across an organisation in order to be successful. At the very least, it is advisable to reinforce accreditation maintenance and configuration control with a regime of frequent compliance checks and inspections.

### Accreditation of Dynamic Systems

87. Certain developer, simulation or test systems and temporary systems (often deployed or tactical) will require accreditation. For business and operational reasons, such systems cannot be maintained under strict configuration control and may even change dynamically from day to day. In these cases a stable description of the system and its technical countermeasures is not practical.

88. Accreditation of such systems will need to concentrate on ensuring that the particular risks of a dynamic environment are suitably addressed, and that residual risks (which are likely to be more numerous and significant) are clearly presented and justified:

- A general description of the system, in particular its function and a clear justification for the lack of configuration control;
- A risk assessment and details of countermeasures and general guidelines, e.g. access limited to small group of staff, ability to recover system within required time constraints, isolation from other systems or tight security controls over interconnection;
- Appropriate security operating procedures;
- The importance of effective communication among the user group to identify problems early and clear arrangements for responding to incidents without delay.

89. In cases of high residual risk, escalation will be required to the SIRO for formal approval.

## Interconnection of IS

90. Approaches to the risk management and accreditation of interconnections will vary depending on complexity but in all cases it will be necessary to have a formal agreement on the policy for interconnection. Approaches may include:

a. A simple interconnection security policy for a single point to point connection;

b. A Service Level Agreement (SLA) for one or more interconnections, which will include all IA specific requirements;

c. An RMADS for a defined "core" network of the more significant IS and a Code of Connection (CoCo), detailing the interconnection requirements, to manage the interconnectivity of the remaining IS;

d. A community security policy defining the basic security principles and requirements for a community of interconnected systems – effectively "the rules for club membership".

91. An assessment should always be made of the risk in both directions. For example, connection to a network such as the Government Secure Intranet (GSi) should address both the GSi accreditor's requirements and any additional risks to the internal network and its systems. A risk assessment of the interconnection should be conducted in much the same way as in the case of an individual asset, however particular thought should be given to aspects such as:

- Integrity, non-repudiation and provenance of the information in both directions, including potential traceability to source for forensic readiness and other reasons;
- Malicious software controls both internally and at the boundaries;
- Confidentiality requirements and, where sensitivity markings are applied within one system, whether these are compatible or translatable in the other system;
- Intruder detection systems and defensive monitoring, including meeting legal requirements – especially under the Human Rights Act 1998 and various Acts covering the interception or monitoring of communications - see Appendix B for further information.
- Availability and the potential impact on the IS being accredited if it is reliance upon an interconnected system with a lesser availability requirement.

92. Where different organisations join together to fund and develop a communal IS service, they will each have a vested interest in ensuring that their own IA requirements are met. In such cases, a panel composed of accreditors from all the participating organisations may be appropriate. The alternative is for all participants to approve a common accreditor and agree to be bound by this accreditor's decisions. Whichever route is chosen each organisation will still retain IA responsibility for its own information.

93. Additional considerations are necessary when connecting to networks and other IS owned by other nations and / or international organisations and/or subject to their statutory policies, laws and other standards (e.g. cryptography).

94. In all cases of external interconnection, management and risk ownership of the other IS will reside with another organisation and it will therefore involve interaction with at least the accreditors and IA management responsible for the external IS. The obvious exception is the Internet, which has no identifiable management or risk ownership. In the case of internal interconnections, the IS may be managed and accredited by one or more areas but risk ownership resides with one SIRO.

95. Due to different ownership, connection to external IS is invariably more difficult to manage than connection to internal IS. For example, in the case of dissimilar availability requirements it will usually be possible to revisit the IA requirements for an internal connected system in the context of changed interdependencies but for external systems, contracts may also need to be revisited and in some cases it may be necessary to accept a reduced availability. Indeed, with connections to external IS, there may be no scope for amending the external IS in line with your own organisation's risk appetite.

## Accreditation of Third Party Services

96. IA requirements on services provided by a third party will vary according to the nature of the services. The requirements may generally be considered and handled in accordance with the process for internal assets, but will need to be documented with particular clarity to ensure that they are enforceable. To avoid possible confusion, it is advisable that service contracts and agreements refer to the RMADS requirements and relevant standards for the detail of the security requirements. Third party relationship issues that will need to be addressed include:

- Scope of service accreditation: definition of what is being accredited, and to what standards;
- Asset ownership and custody: defining who owns what assets and, usually applicable to information assets, where the third party has custodial responsibilities for assets owned by the organisation;
- Risk ownership: most risks will still be owned by the organisation, but certain risks (often financial) may be shared with, or transferred to, the third party;
- Security barriers: between the organisation and the third party service;
- Security monitoring arrangements: what the organisation can monitor directly, and reports to be provided by the third party on things the organisation cannot monitor;
- Change control arrangements: to prevent the third party making unexpected changes, and to ensure that the organisation may quickly negotiate changes to meet urgent security requirements;
- Audit and inspection rights: of the organisation over the third party service and related assets;
- Incident reporting and handling: assigning roles and responsibilities between the organisation and the third party, and an escalation procedure;
- Business continuity plans: those of the third party for the continuity of their service provision, and those of the organisation to provide against the failure of the third party service; and
- Secure decommissioning: of the original third party's assets when the service provision is moved to a new third party.

# E. Risk Management

97. The basis of risk management is a firm understanding of the business of an organisation and its risk environment. The process of risk management identifies the potential threats and vulnerabilities, assesses them in terms of likelihood and impact, determines how the resulting risks may be reduced, and decides on the level of residual risk that is acceptable to the business.

98. The overriding business priority may necessitate the acceptance of a high level of risk in order to take advantage of a business opportunity but in all cases the decision will depend on an organisation's risk appetite, legal obligations and impact on partner organisations.

## Risk Assessment

99. An Information Assurance (IA) risk assessment determines the risks to which an organisation exposes itself and the business harm (impact) likely to result from a security failure balanced against the realistic likelihood of such a failure occurring in the light of prevailing threats, vulnerabilities and the controls currently implemented. It is therefore a systematic consideration of:

- Asset values;
- Threat assessments;
- Vulnerability assessments;
- Likelihood of a successful attack;
- Business impact assessments.

100. An effective risk assessment indicates the level of risk associated with the specific IS on a scale appropriate to the organisation and should be sufficiently detailed and consistent[4], to enable risk management decisions. It should be consistent with the corporate policy, including any risk assessment conducted for a higher level business continuity planning and will feed into an ISO17799 risk management process through the Information Security Forum (ISF).

101. There are a variety of different approaches to risk assessment. Organisations should decide which of these approaches is most appropriate for their particular environment and business requirements and specify this in their corporate IA policy (see Section C), in order to ensure a consistent approach.

102. The understanding gained during the risk assessment will underpin all risk management decisions related to the IS, so it is essential that the process is properly documented. An accurate record of the factors contributing to risk will be particularly important later on, when it will be necessary to justify the response to specific risks (see Part 3 of this Guide).

[4] Caution: Risk assessment outputs can rarely be considered to be a precise measurement of risk, even where the result appears to have been derived from a mathematical calculation.

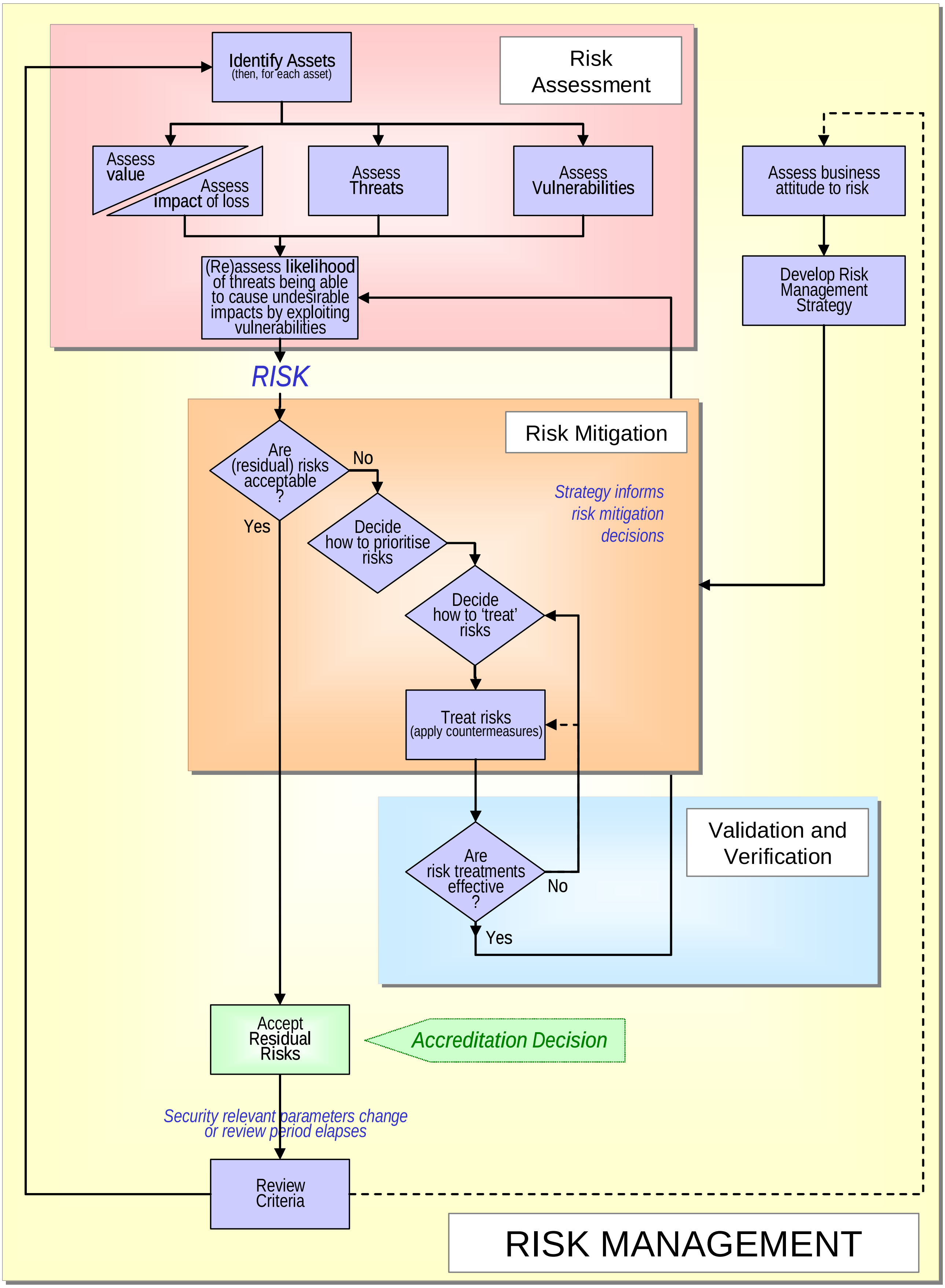
Risk Assessment
Identify Assets
(then, for each asset)
Assess value
Assess impact of loss
Assess Threats
Assess Vulnerabilities
(Re)assess likelihood of threats being able to cause undesirable impacts by exploiting vulnerabilities
Assess business attitude to risk
Develop Risk Management Strategy
RISK
Risk Mitigation
Are (residual) risks acceptable ?
No
Yes
Decide how to prioritise risks
Decide how to 'treat' risks
Treat risks
(apply countermeasures)
Strategy informs risk mitigation decisions
Validation and Verification
Are risk treatments effective ?
No
Yes
Accept Residual Risks
Accreditation Decision
Security relevant parameters change or review period elapses
Review Criteria
RISK MANAGEMENT

**Figure 3: Risk Management Process**

## Asset Values

103. Assets may be valued in a number of ways. The most obvious is the purchase cost but, more importantly, assets should be valued in terms of their contribution to the business of the organisation. The importance of an asset can be based on the potential impacts on the business, resulting from its compromise or loss. Impacts include financial losses from interruption of business, the level of commercial or other sensitivity of the IS and possible damage to business reputation. Asset values may be expressed in various terms (including £s, numbered scores, grades and sensitivity markings) providing these are meaningful to the organisation.

## Threat Assessment

104. Potential threats to assets need to be identified and assessed and these should include natural, accidental, and deliberate threats. Both direct and indirect threats should be considered: for example, an organisation may not be a target for a particular pressure group but, if located next door to an organisation that is a target, it may suffer disruption or collateral damage from an attack on its neighbour. For each threat identified, the basic information required for an assessment will include the:

- Threat source (river prone to flooding, business competitor, own staff);
- Target of attack (individual asset or group of assets);
- Type of attack (water incursion, hacking, user error);
- Capability of the attacker (technical expertise, ease of physical access);
- Likelihood of an attack (strength of motive, record of previous activity).

## Vulnerability Assessments

105. An assessment should be made of the potential vulnerability to attack of each asset and the resulting impact of a successful attack. Both direct and indirect vulnerabilities should be considered: for example, an asset on the top of a hill may not be directly vulnerable to a nearby river flooding but essential services, such as power and communications lines, may be vulnerable.

106. The impact of a successful attack on the availability, integrity, and confidentiality of an asset should be assessed in terms of immediacy of impact, extent of compromise, and estimated time to recovery. As well as the direct impact of an attack on individual assets, the possible knock-on effects on other assets should be considered.

## Likelihood of a Successful Attack

107. Using the threat and vulnerability assessments, a realistic judgement should be made of the likelihood that each possible attack scenario might successfully impact on an asset.

For example, a high level of threat from a motivated and capable source with a record of successful attacks (such as viruses from the internet) combined with a low vulnerability to attack due to proven countermeasures (good quality frequently-updated anti-virus software, and effective incident reporting and handling arrangements), despite a high potential for impact on short-term availability, could produce a low likelihood of a successful attack with significant impact for more than a short period of time.

## Business Impact Assessments

108. The judgements on the likelihood of successful attacks, when combined with the relevant (mostly impact-based) asset values, will enable assessments of the probability and extent of the risks to which the business will be exposed by its use of

IS in support of business activities. This should also take account of any adverse impact on existing corporate policies resulting from an individual IS, in particular any potential impact on business continuity plans.

### Risk Treatment

109. There are a number of options available when considering how to handle a risk. At one extreme an organisation may choose to accept the risks identified in the risk assessment. This may be appropriate where the risks are relatively small in relation to the business benefits derived from using the IS. At the other extreme, an organisation may decide that the risks are so severe that the business should avoid them entirely. Between these extremes, it is necessary to prioritise the remaining risks and determine how to reduce them to acceptable levels.

110. Hence, IA risk treatment is the process to determine whether to:

- **Mitigate:** consider countermeasures to reduce the likelihood and impact of the risk.
- **Avoid:** consider alternative methods of achieving the business objective or consider the business impact of not providing the service.
- **Transfer:** consider methods of transferring responsibility. However even if responsibility for limiting the risk is transferred outside an organisation, the risk will still rest wherever the business impacts are actually felt.
- **Accept:** accept risk (usually where risk is low impact and low likelihood).

The process will usually require a number of iterations until the residual risks have been reduced to an acceptable level.

111. There must be an accountable management process for the formal acceptance of which risks are to be mitigated, avoided, transferred or accepted. This process should include the acceptance of all the costs implied by those choices, and justification and formal agreement of any deviation from corporate policy, together with acceptance of any potential business impacts resulting from such deviation.

112. This formal process is usually recorded in the risk treatment plan, described in Part 3, which demonstrates that the risks have been properly identified, assessed and countermeasures allocated. It will also record the implementation status of each countermeasure. The plan should demonstrate that countermeasures are traceable, proportionate and cost effective and it provides business justification and accountability for all such financial costs. All IA risks should also be incorporated into corporate, business or project risk registers, as appropriate. The risk treatment plan may be used by internal auditors or IA inspectors and feeds into the Statement of Applicability (SOA) for BS7799 auditors.

### Risk Mitigation

113. Risk mitigation is the process of reducing a specific risk (or set of risks) to an acceptable level by changing the operational environment and/or applying technical and non-technical countermeasures, for example:

a. Physical: e.g. a perimeter fence;

b. Procedural: e.g. an authorisation form is signed by an appropriate person before a new account is set up;

c. Personnel: e.g. credit or other security checks against potential employees;

d. Technical: e.g. use of an approved or certified product.

114. Cost-effective risk mitigation is likely to incorporate layers of supporting defences, including a mixture of technical and non-technical countermeasures, which should be considered carefully in terms of impact, usability, effectiveness, initial and through-life costs and may result in trade-offs between different types of counter-measure. Equally, a number of different controls may be required to mitigate a specific risk (or set of related risks), known as Defence-in-Depth, in order to reduce the residual risk to an acceptable level.

115. Existing business continuity, disaster recovery and forensic readiness plans should be considered as part of risk mitigation and, in the case of IA requirements for availability, a robust business continuity plan may represent a major countermeasure in its own right.

116. Risk management is an iterative process. As decisions are made on appropriate countermeasures, the risk assessment should be reviewed. In addition to confirming that the controls are reducing the assessed risks to more acceptable levels, organisations will need to confirm that they are actually working as expected (see Section G “Assurance and the Accreditation Decision”).

117. This iterative process should take note of changes to the threat and forms part of the "Security Improvement Process" supporting ISO17799 compliance. ISO17799 refers to this as the “Plan-Do-Check-Act” (PDCA) process.

### Risk Avoidance

118. It may be possible to avoid taking certain risks entirely, by various means:

- Choosing not to undertake the aspect of the business activity that attracts the particular risk, such as not providing direct customer access from the internet;
- Using alternative assets or methods to undertake the business activity, such as selecting different hardware or software;
- Relocating assets away from known areas of physical risk, such as flood zones; or
- An organisation may decide to abandon a project because the risks outweigh the potential benefits.

119. Where avoidance is used as a risk treatment, it must be documented fully so that later change proposals are not allowed to accidentally undo the treatment.

### Risk Transfer

120. Whilst an organisation will retain ultimate responsibility for all risks, it may be able to transfer certain aspects of risk to other parties. Examples include:

- Through insurance, where financial losses may be recovered from an insurance company, provided the premiums represent an acceptable cost;
- Through contracting-out, where the operational and financial risks of providing a service are borne by another party, although an organisation still bears final responsibility for the service provision.

121. Where risk transfer is used as a risk treatment, an organisation should consider planning in preparation for the possibility that the third party may later fail them in some way. After a number of insurance claims, for example, an insurance company may increase premiums to an unacceptable level or refuse to renew a policy.

## Risk Acceptance

122. There will always be an element of risk acceptance, as risk can never be removed entirely from any business activity. Risks may be accepted for a number of reasons, including:

- The potential impact is low, and the cost of further protection against the risk is not worthwhile in business terms;
- The likelihood of an incident is low, and the cost of further protection against the risk is not worthwhile in business terms; and
- The risk cannot be avoided, transferred, or mitigated any further within acceptable costs to the business.

123. Risks that are accepted are known as residual risks. It is essential that the business fully understands the residual risks, so that it may make an informed decision on the acceptance of the asset. The accreditation process must document residual risks clearly and record their acceptance. Residual risks may also need to be fed into other corporate risk considerations, such as business continuity, disaster recovery, and forensic readiness plans.

## Traceability

124. Traceability, based on the outputs of the risk management process, is needed to ensure that an organisation can determine why a given risk management decision was taken, and should be able to demonstrate the following:

- The cost of each countermeasure and any effects on the efficiency of the IS is justified by the severity of the risk it addresses.
- A proper risk management decision has been taken for each risk.
- Each risk selected to be mitigated is properly addressed by one or more countermeasures.
- Responsibility for implementing each countermeasure is properly allocated.
- Each operating procedure implements a countermeasure efficiently and effectively.

This may be documented in hard copy or electronically. The precise format and contents will depend on the risk management method chosen.

# F. Assurance and the Accreditation Decision

125. In order to accredit an Information System (IS), the accreditor must gain assurance that the mechanisms and controls needed to manage the risks are in place and operating effectively. This applies to accreditation prior to formal acceptance of the delivered solution and to continuing accreditation throughout the life of the IS.

126. This assurance should be based on well documented evidence which may also help to provide evidence of compliance with BS7799. Based on the evidence, which should highlight any issues of potential non-compliance with stated requirements, the accreditor can decide whether or not the residual risk is acceptable in order to formally accredit the IS on behalf of the organisation or to escalate the decision.

127. Assurance evidence should be prepared and/or verified independently of the vendor or developer, especially in the case of sensitive systems, services and networks.

## Verification, Validation and Evaluation

128. Evidence is needed that physical, procedural, personnel and technical security arrangements meet, and continue to meet, the Information Assurance (IA) requirements from development through to eventual decommissioning. This will come from various forms of testing, evaluation, checks, audits and inspections.

129. Precise requirements for verification, validation and evaluation of the technical countermeasures, including the schedule for this work and requirements for corrective action, should be specified in contracts and funding provision secured. This applies to contracts covering the delivery of the IS and for these activities throughout the in-service life. These requirements should also be detailed in the accreditation documentation. Similar provisions should be made for resourcing in-house development and management of IS.

130. Verification, validation and evaluation activities often involve a number of different technical and non-technical disciplines. These should be co-ordinated, giving thought to combined scheduling of activities such as physical and installation inspections, in order to minimise cost and operational impact.

### Product Assurance

131. Security and resilience products may be used to mitigate identified risks. Wherever possible these products should have been independently tested or evaluated.

132. Where products implementing IA functionality have not been independently tested or evaluated, assurance may be gained by independent testing or assessment during development or as part of the acceptance testing process. The rigour of such testing will depend on the how critical the product is in terms of the IA assurance required. To operate effectively, IA products must be installed, configured and used in accordance with authoritative configuration guidelines and handling instructions.

### Assurance of Integrated Systems, Services and Networks

133. Use of individual assured security products alone will not normally provide adequate assurance that all security risks to the IS have been addressed. The accreditor needs evidence that the products provide the range of security functionality specified, have been configured, patched and integrated properly, work effectively together. Assurance may also be required in the development, integration and project environments, including any support systems.

134. As a minimum, IA requirements should be incorporated into the User Acceptance Test Plan (UATP), to provide evidence that the specified countermeasures are in place and work. The UATP must therefore cover all the relevant countermeasures specified in the countermeasures list and ensure that these are adequately exercised and independently witnessed, if required. The test results must be recorded and checked against expected results.

135. Where the risk is considered to be particularly high, for example a system processing very sensitive information or a network, which is critical to an organisation, further assurance processes may be necessary to supplement user acceptance testing. These could include systems evaluation, assessments and IT Health Checks with associated corrective action.

## Physical Security Inspections

136. Physical site and facilities inspections should cover all relevant IA requirements, especially when physical countermeasures are explicitly identified in the RMADS. They should be carried out by appropriately trained security personnel and may comprise:

- Pre-accreditation physical inspections of sites and facilities, including any fall back location and off site media storage areas;
- Periodic in-service physical inspections of sites and facilities, including any fall back location and off site media storage areas;
- Unscheduled inspections, for example as a result of an incident, change of threat to business operations, or change of or modification to business location.

137. Such inspections may include:

- Confirmation of appropriate site layout, resilience of cross-site communications links, secure areas, storage facilities;
- Confirmation of building structures, intruder detection systems, including CCTV and intruder detection lighting;
- Local geographic and environmental threats outside the organisations control;
- Checking and auditing access control systems and procedures;
- Verifying an appropriate level of site or building guarding and procedures for visitor access, especially to secure areas;
- Confirmation that appropriate fire detection and response systems and appropriate back up power facilities are in place.

## Personnel Security Checks

138. Personnel security checks include verifying procedures for personnel security checks and security clearances as appropriate and procedures for staff joining or leaving the organisation;

## Technical Inspections

139. In certain circumstances, particularly in the case of communications systems or facilities and systems incorporating cryptographic equipment, it may be necessary to inspect against electrical installation standards, which could be an inspection to industry best practice installation standards or to more rigorous electro-magnetic security standards.

### Security Awareness and Training

140. Security awareness and user training are a vital part of corporate security policy and should be addressed before acceptance of the IS and regularly reviewed throughout its service life. The accreditor should confirm that that standards and timing are appropriate to meet the IA requirement.

### Supporting Documentation

141. All relevant information and evidence should be assembled into a portfolio, also called the Risk Management and Accreditation Document Set (RMADS), which will require verification prior to the accreditation decision. (See also Part 3 "Risk Management and Accreditation Documentation".)

## Accreditation Decision

142. This must be an informed decision made in full understanding of the implications to the business and should take place prior to final acceptance of the IS and periodically throughout its service life.

143. Evidence of compliance with the IA requirement, together with all relevant documentation should be presented to the accreditor for comment and staged approval leading up to an accreditation decision. Any aspects of non-compliance should be documented and brought to the notice of the accreditor for assessment of the security implications. Early involvement of the accreditor and agreed mitigation of risks helps to avoid delay in final acceptance.

144. Based on the evidence available, the accreditor may issue an "Accreditation Statement", which will form part of the RMADS, confirming one of the following potential options:

a. **Interim Accreditation**: The accreditor may decide that certain remaining security deficiencies are not sufficiently serious, when considered in relation to business benefits and opportunities, to prevent operation over a short period. Under these circumstances a time-limited provisional or interim accreditation may be issued on condition that the deficiencies are corrected within the specified period otherwise accreditation would lapse.

b. **Full Accreditation**: The residual risks have been accepted or any deviations have been mitigated by alternative countermeasures, for instance more rigorous procedural or physical controls to offset an inadequate technical measure. This could result in a formal amendment to the RMADS and achievement of full accreditation.

c. **Refusal of Accreditation**: At the most extreme, non-compliance would be grounds for refusal of accreditation. This would usually occur in the case of high residual risk and would require escalation (see also below). Refusal of accreditation should lead to non-acceptance of the IS.

### Escalation

145. Where there is conflict between the IA requirement and another business need, which cannot be resolved by delegated responsibility, the accreditation decision must be escalated to the SIRO, who is responsible for balancing business requirements. In all cases where corporate security policy requirements (see Section C) cannot be met, the SIRO must be informed, whether or not the accreditation decision is escalated.

146. Organisations should provide policy and procedures for escalation, clearly identifying roles and responsibilities and the type and format of documentation required. Such documentation should be presented clearly and succinctly in terms of

business impact and options for an informed accreditation decision to be taken at the appropriate level of management.

# G. Risk Management In-Service and Accreditation Maintenance

147. Accreditation does not stop with the issue of the accreditation certificate - business requirements change, risks change and Information Systems (IS) change and evolve. Risk management in-service and accreditation maintenance are vital components of corporate governance and is recognised as such by its inclusion in ISO17799 under the Plan-Do-Check-Act (PDCA) Model.

148. Management of the Information Assurance (IA) requirements throughout in-service life may include a combination of the following activities and all of these are required to support ISO17799 compliance:

a. Corporate Governance Processes:

- maintenance of corporate security policy;
- business continuity planning;
- disaster recovery planning;
- forensic readiness planning.

b. Secure IS Management:

- configuration control;
- software patching;
- malicious software control, intruder detection and intrusion prevention.

c. Secure IS Use

d. Compliance, Verification and Validation:

- compliance checks, audits and inspections;
- content checking;
- monitoring.

e. Incident Management and Response:

- incident management and reporting procedures;
- response and recovery;
- implementation of lessons learned.

f. Maintenance of Risk Management and Accreditation Document Set (RMADS):

- updating and configuration control.

g. Reviews:

- performance and resource review;
- risk assessment review;
- accreditation.

## Corporate Governance Processes:

### Maintenance of Corporate Security Policy

149. The business environment and its associated risks are constantly changing. These changes should be reflected in corporate security policies and risk registers.

### Business Continuity, Disaster Recovery and Forensic Readiness Plans

150. These plans are essential preparations against the times when, despite all risk management efforts, something goes seriously wrong. Business continuity plans aim to keep an organisation’s most essential business processes running, as far as

possible, throughout the duration of any emergency. Disaster recovery plans aim to recover or replace assets, which have been damaged or lost as a result of an incident, so that they may quickly resume their support for business processes. Forensic readiness plans aim to ensure that information relevant to an incident is recorded and securely retained to support later investigation and any possible legal proceedings that may result.

151. These plans must be regularly reviewed and exercised, to ensure that they continue to meet the IA needs of the business. There may be corporate level plans that address the overall business needs and co-ordinate arrangements across all significant business assets, and/or local plans based on individual or particular groupings of assets. In all cases there is a need for two-way consultation to ensure that changes to the plans feed into the risk management considerations of relevant assets, and that changes to the risk assessments of assets feed back into the planning process.

## Secure IS Management

### Configuration Control

152. Configuration control is critical to good IA. In large organisations with complex IS, it is good business practice to establish a Configuration Control Board (CCB), in which case the accreditor should be a permanent member. Often in complex services, the CCB will may act as a security working group and will report to the Information Security Forum (ISF).

153. Any significant changes, enhancements or upgrades to the IS should be reviewed for potential business impacts, including IA, prior to approval by the CCB or other responsible authority. All security critical and security relevant changes will be subject to the approval of the accreditor, for example:

- Major hardware or software upgrade;
- New interconnections and significant changes to existing interconnections;
- Introduction of unproven emerging technology.

154. As a prerequisite to periodic accreditation, adequate configuration control measures must exist and be well documented, regularly monitored and updated. Those responsible for configuration control should:

- Be aware of the security implications of changes;
- Know who to approach to discuss proposed changes;
- Maintain adequate records of configuration changes.

### Software Patching

155. There should be a corporate patching strategy to ensure timely and appropriate testing and subsequent implementation of software patches. This is an important element in the protection of IS against malicious software, hacking and intrusion.

### Malicious Software Control, Intruder Detection and Intrusion Prevention

156. Viruses, trojans, worms, spyware and hacking are a constant threat to IS. In order to protect against these threats, which may have significant or catastrophic impact, there should be a corporate policy for malicious software control and intrusion prevention, detection and response. This policy should ensure regular protection updates, effective updating of user profiles, and constant operational monitoring and review of the protective controls.

## Secure Use

157. Effective day to day management of the IS is vital to information risk management and maintenance of the asset's accreditation status and will provide evidence of ISO17799 compliance. This may include:

a. system lock down and control of privileges;

b. prompt closure of user accounts, when employees change roles or leave;

c. implementation of accounting and audit procedures;

d. inventory control;

e. cryptographic key management.

158. Users must understand that they are individually responsible and accountable for their actions. All users should be well trained and should understand the requirements detailed in the Security Operating Procedures (SyOPs), which must be approved by the accreditor and circulated to all users on a regular basis.

159. SyOPs should be tailored to specific user communities, e.g. IS management personnel and IS users. They describe the procedural countermeasures and therefore each SyOPs provision should be traceable to one or more specific countermeasure(s) and thus to particular risks, in order to justify the cost of implementing the measure. They should reflect local conditions, such as working practices, system configuration and environmental security constraints.

## Compliance, Verification and Validation

### Compliance Checks, Audits and Inspections

160. Compliance checking is vital to provide evidence for the effective implementation of the IA risk management strategy and to support the continuing accreditation of the IS (see also Section F). Compliance checking will usually require a combination of technical, procedural, personnel and physical inspections and audits, for example:

a. Audit of IS, users, cryptographic keys;

b. Annual IS inspections, independent IT Health Checks, physical inspections.

Both these outcomes are a prerequisite of compliance to ISO17799.

161. Most compliance checking will be routine or periodic but unscheduled inspections may be required as a result of an incident, such as the compromise of cryptographic key, or following a significant change to the configuration or environment.

162. As a minimum condition of continuing accreditation, full verification and validation testing, as detailed in the RMADS, should be carried out at least once a year. If an IT Health Check was part of the original accreditation requirement, this should also be repeated at least at the same frequency.

### Content Checking and Monitoring

163. Appropriate content checking and / or monitoring may be implemented as an element of corporate management, to ensure inappropriate information is not stored or transmitted, to block malicious code, and as an element of risk management to protect the confidentiality of an organisation's information. Legal advice should be sought prior to implementation of content checking or monitoring, to ensure measures are legally compliant and properly explained to users.

## Incident Management and Response

164. Coherent incident management procedures should form part of the corporate IA strategy, enabling quick action to minimise potential damage and early identification of wider problems, which need to be addressed.

165. Incident management procedures should include:

a. reporting method(s) with a focal point;

b. response (immediate actions and escalation procedures);

c. documentation and evidential requirements;

d. reporting and review of outcomes (enabling changes to avoid recurrence.)

## Maintenance of the Risk Management and Accreditation Document Set (RMADS)

166. Risk management and accreditation, is an iterative process. The supporting documentation is "living" and will require review and change management. All changes to the documentation should be agreed and endorsed by all stakeholders and should distil into end user and other training as appropriate.

## Reviews

167. Assurance is maintained in the light of changes to an IS and its risk profile throughout in-service life by regular post implementation IA reviews, which also constitute best business practice.

### Performance and Resource Review

168. Approximately six months after commissioning, it is useful to conduct a benefits and resource review to assess the following:

a. Is the IS performing to the IA requirement? Is this effective? Are there any problems in practice?

b. Are there adequate resources to support the IA requirements (e.g. security manpower, training resources)?

169. It is also an opportunity to produce a lessons learned paper, if appropriate, or input into a project paper.

### Risk Assessment Review

170. If any of the risk factors change, the risk assessment should be reviewed and in any case be carried out on a regular basis, as agreed by the accreditor and business owners, based on the risk environment and any other pertinent considerations.

### Accreditation Review

171. Accreditors are involved beyond the project or programme stage right up to eventual IS disposal and can withdraw accreditation at any time during its lifecycle, although in practice such a decision would usually be escalated.

172. The accreditor must ensure that the conditions for review of the accreditation of the IS are clearly stated. It is recommended that a full review of the accreditation status of an IS is undertaken at a minimum every year in accordance with BS7799 identified best practice. The frequency must also comply with other external interface requirements and in all cases, a formal review should take place automatically:

a. as a result of any significant change to the IS or the risk;

b. following any major security incident.

## H. Secure Decommissioning and Disposal

173. When the Information System (IS) reaches the end of its service life in an organisation, policy and procedures should be in place to ensure secure decommissioning and transfer or disposal, in order to satisfy corporate, legal and statutory requirements.

174. Availability and integrity requirements in respect of information stored on IS may persist for legal and other statutory or corporate reasons and require transfer to other ownership or custodianship for archive purposes. This will also require assurance that the data can continue to be accessed when required (availability) and assurance that it remains unchanged (integrity).

175. Confidentiality requirements must also be considered. If an IS has been processing sensitive information or contains sensitive security components, which attract special handling requirements, it will require robust purging and overwrites or destruction. There are a number of methods and proprietary products available for such purposes.

176. Even if there are no apparent sensitivities, organisations should always consider purging IS before disposal or transfer. Software licences should be transferred or cancelled as applicable and, in the case of disposal or transfer of hardware only, should be revoked and applications and code removed.

177. In the case of IS with interconnections, notice of decommissioning should also be issued to all such interfaces and assurance obtained from the remote end that data has been purged where appropriate and all access rights to remote systems have been removed.

178. This demonstrates good governance and avoids embarrassment and potential prosecution as a result of IS transfer with sensitive information still accessible. It will also ensure that information required in the future is effectively transferred and remains accessible.

179. Once all security relevant activities associated with decommissioning and disposal have been completed and verified, a Security Decommissioning Compliance Certificate may be issued by the accreditor.

# PART 2: THE IA RISK MANAGEMENT AND ACCREDITATION PROCESS

**HEALTH WARNING**

Adapt the process to the Information System in question and only exercise those elements of the process, which are appropriate to this specific case.

180. Part 2 outlines the process of risk management and accreditation throughout the lifecycle of an Information System (IS), from early planning, through development and in-service to decommissioning. It should only be used once the concepts presented in Part 1 are fully understood, to ensure that it is a meaningful process and that only those aspects appropriate to the IS in question are addressed at any given stage.

181. In order to ensure integration with core business processes, including project and procurement processes, the different stages (0-7) in IA risk management presented in this Guide are linked to the project and procurement cycle as presented in the Office of Government Commerce (OGC) Gateway Review Process and to general business processes once in-service.

182. The stages are equally appropriate for existing accredited IS, which may require major change or upgrade and for legacy IS requiring accreditation for the first time.

183. Each stage is clearly set out in the following format:

- aim;
- gateway or business process link
- key Notes;
- information required;
- activities
- products (stages of origin and review in parentheses)

184. Whether considering new projects, legacy IS or changes to existing accredited assets, it is vital that co-operation and mutual understanding be established and maintained between all stakeholders. This will include those responsible for ownership, policy, compliance and delivery, underpinned by the Senior Information Risk Owner (SIRO).

185. The RMADS should be archived after decommissioning or disposal for a period to be determined in line with an organisation's corporate policy, taking into consideration potential legal implications, such as evidence for prosecution or defence.

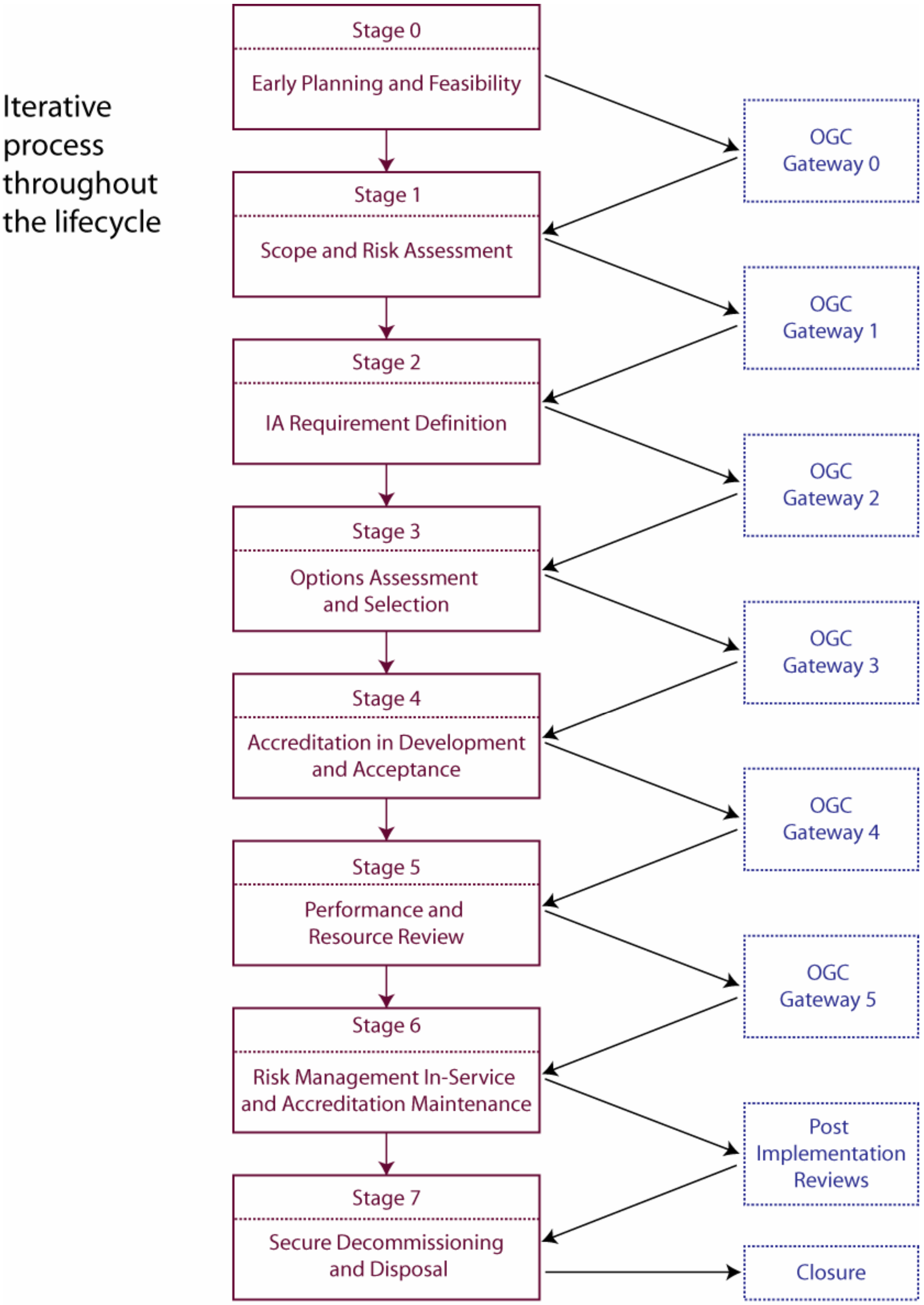
Iterative process throughout the lifecycle
Stage 0
Early Planning and Feasibility
Stage 1
Scope and Risk Assessment
Stage 2
IA Requirement Definition
Stage 3
Options Assessment and Selection
Stage 4
Accreditation in Development and Acceptance
Stage 5
Performance and Resource Review
Stage 6
Risk Management In-Service and Accreditation Maintenance
Stage 7
Secure Decommissioning and Disposal
OGC Gateway 0
OGC Gateway 1
OGC Gateway 2
OGC Gateway 3
OGC Gateway 4
OGC Gateway 5
Post Implementation Reviews
Closure

**Figure 4: Risk Management and Accreditation Aligned to The Business Management, Project and Procurement Process**

# Stage 0 Early Planning and Feasibility

## AIM:

To assess and scope the high level security issues, to provide early identification of risks to the business plans.

***OGC Gateway™ 0 - Strategic Assessment:** Focuses on the programme or project business justification - to investigate the business need, strategic fit, affordability and achievability in principle.*

## KEY NOTES:

- Information Assurance (IA) should be considered as an integral part of the business requirement from the earliest stages in the planning process.
- The business requirement should be reviewed in the context of corporate IA policy and other relevant laws, statutory regulations, standards and policies.
- An initial assessment of security issues should identify risks to the business requirement as a result of IA issues.

## INFORMATION REQUIRED:

- Description of business requirement, including relevant business constraints, e.g. costs and time-scales;
- Corporate IA policy and other policies as appropriate
- Relevant laws, directives and standards;
- Interconnections, flows and relationships with other assets, including details of other (external) stakeholders.

## ACTIVITIES:

### Identify dependencies

List all related policy and other documents (e.g. relevant corporate policies), including appropriate policies and agreements for interconnections to other assets where applicable.

### Identify applicable laws and statutes

As for dependencies, begin to list applicable laws and statutes.

### Identify the basic IA requirements

Based on information available, consider the potential IA requirements in terms of data or other flows across boundaries and other dependencies, business context and Information System (IS) description, any known roles and responsibilities, the corporate risk environment and potential threats. There should be sufficient information to highlight specific IA issues and concerns.

### Assess the impact of IA issues on the business requirement

Having identified the basic requirements and issues, these should be reviewed in the context of the business requirement, in order to assess their potential impact on the business objective and, where applicable, their impact in terms of project, programme or business risk.

If there are any significant risks or concerns, they should be escalated as appropriate.

PRODUCTS:

| **Impact Assessment of IA Issues** | |
|---|---|
| Risk Management and Accreditation Document Set (RMADS): | |
| **Contents List**<br>**Links and Dependencies**<br>**Register of Applicable Legislation**<br>Section 1: Accreditation Status | Section 3: Risk Management<br>**Corporate Risk Environment**<br>**Threat Assessment** |
| Section 2: Basic Information<br>**Business Context of IS**<br>**Description of Asset**<br>**Interconnections and Interfaces**<br>**Responsibilities and Functions** | Section 4: Development, Acceptance and In-Service |

# Stage 1 Scope and Risk Assessment

## AIM:

Scope approach to Information System (IS) risk management and produce Information Assurance (IA) risk assessment.

***OGC Gateway*** $^{TM}$ ***1 – Business Justification:*** *Focuses on the project initiation process, to justify the project based on business needs and an assessment of its likely costs and potential for success.*

## KEY NOTES:

- IA should be integrated into the development of the business requirement.
- Careful scoping of the IA requirements should provide the best approach to risk management and accreditation through the lifecycle of the IS.
- IA risk assessment, based on a realistic threat assessment, will provide the basis for risk management and accreditation.
- IA risks may impact the affordability and achievability of the business need.

## INFORMATION REQUIRED:

- Outputs from Stage 0;
- Additional information as available on business options and preferences.

## ACTIVITIES:

### Scope the IA requirement

Consider initial IA requirement and any new information, to assess the effects of boundaries in terms of the best approach to risk management and accreditation through the lifecycle. This activity may need to be repeated to provide alternatives for consideration, based on initial and in-service costs, usability and security impacts.

### Review the initial IA requirement, dependencies and applicable legislation

Review the details prepared at Stage 0, and develop based on further information available at this stage, including decisions regarding the scope. Provide sufficient detail in terms of a pen picture to use in the risk assessment.

### Identify the individual component parts of the requirement

Check that the project staff is compiling an asset register to record the individual components of the IS and ensure that this includes all IA critical and IA relevant components. The register will be under constant review throughout the life-cycle of the project and provide inventory and configuration control in-service. Applicable reference details should be recorded and updated in the “Dependency List”.

### Conduct a vulnerability assessment

Conduct a vulnerability assessment based on the known IA requirement. Information on vulnerabilities, particularly on commercial software, is widely available from open sources. Where proprietary software or hardware is a potential option, expert assistance may be required. A number of vulnerability assessments may be produced based on different options.

### Conduct a risk assessment

Conduct an IA risk assessment in accordance with organisation’s preferred method using an appropriate threat assessment and the vulnerability assessment. A number of risk assessments may be produced based on different options.

### Decide how risks will be treated

Based on the risk assessment, it should be decided how IA risks are going to be treated (i.e. mitigate, avoid, transfer or accept). This will require formal agreement and results should be recorded in the risk treatment plan.

### Begin planning for risk management and accreditation

Consider the potential milestones and time-scales for IA risk management and accreditation, reconciled with available project, programme and development plans and schedules. It may be useful to produce an early “road map” of IA specific activities.

### Review the impact of IA on the business objective

In the light of the risk assessment and other information now available, review the impact assessment, produced at Stage 0, and provide a revised assessment of the impact of IA on the business objective for input into project, programme or corporate risk registers, as applicable.

### PRODUCTS:

| | |
|---|---|
| **Impact Assessment of IA Issues (0-1).** | |
| Risk Management and Accreditation Document Set (RMADS) | |
| Contents List (0-1)<br>Links and Dependencies (0-1)<br>Register of Applicable Legislation (0-1)<br>**Compliance with Corporate Policies (1)** | Section 3: Risk Management<br>Corporate Risk Environment (0-1)<br>Threat Assessment (0-1)<br>**Vulnerability Assessment (1)**<br>**Risk Assessment (1)**<br>**Risk Treatment Plan (1)** |
| Section 1: Accreditation Status | |
| Section 2: Basic Information<br>Business Context of IS (0-1)<br>Description of Asset (0-1)<br>Interconnections and Interfaces (0-1)<br>**Scope of Risk Management and Accreditation (1)**<br>Responsibilities and Functions (0-1) | Section 4: Development, Acceptance and In-Service<br>**Risk Management Plan (1)** |

# Stage 2 IA Requirement Definition

## AIM:

To produce a definitive Information Assurance (IA) statement of requirement and a risk management plan in support of the business or procurement strategy.

***OGC Gateway $^{TM}$ 2 – Procurement Strategy:*** Assess project's viability, potential for success and readiness to invite proposals or tenders, focusing on establishing a clear definition of the project and a plan for its implementation.

## KEY NOTES:

- Provide a clear and concise definition of the IA requirement in preparation to invite proposals or tenders.
- Establish a framework for risk management process to ensure IA requirements are addressed during the development.
- Consider IA requirements in-service and ensure funding is available.
- Check invitations or proposals or tenders prior to publication to ensure all IA aspects are covered and correct.

## INFORMATION REQUIRED:

- Additional information as available on business options and preferences;
- Draft Invitations to Tender (ITT) or other proposals as appropriate;
- Business change management plan or similar.
- Outputs from Stage 1.

## ACTIVITIES:

### Review basic information already collated and further develop in readiness for Invitation to Tender

Review and revise the information already collated, to further inform the IA requirement in preparation for ITT or operational requirement (OR). In particular, ensure that the description of the IS and all proposed interconnections and interfaces is sufficiently detailed and suitable for including in the ITT or OR. Any additional IA component requirements will need to be included in the asset register. Review security responsibilities, taking into consideration both development and in-service requirements, to ensure adequate funding.

### Review and revise IA risks

Review and revise the IA risk treatment plan established at Stage 1 and consider individual countermeasure options, which should be considered in terms of project and business impact (including through life costs). Establish a method to ensure traceability between individual risks and countermeasures (this should be achieved by means of the IA risk treatment plan using appropriate cross reference).

### Further develop the risk management plan

Further develop the risk management plan started at Stage 1 to reflect the IA process and deliverables through development and acceptance. This should be linked to the project plan, showing milestones and deliverables (including verification and validation activities) and should be available for inclusion with the ITT or OR. In addition, early consideration should be given to in-service risk management and accreditation maintenance planning.

### Review draft ITT or OR

Review the draft ITT or OR to check that it covers the IA requirements – propose amendments and corrections as appropriate.

### Draft IA requirements for business change management

Review the business change management plan or similar in relation to the IA through life resource requirements to ensure that these are adequately covered and that funding is allocated.

### PRODUCTS:

| | |
|---|---|
| **Amendments to Invitation to Tender or Operational Requirement as appropriate;**<br>**Inputs and amendments to business change management plan and applications for funding.** | |
| Risk Management and Accreditation Document Set (RMADS) | |
| Contents List (0-2)<br>Links and Dependencies (0-2)<br>Register of Applicable Legislation (0-2)<br>Compliance with Corporate Policies (1-2) | Section 3: Risk Management<br>Corporate Risk Environment (0-2)<br>Threat Assessment (0-2)<br>Vulnerability Assessment (1-2)<br>Risk Assessment (1-2)<br>**Countermeasures List (2)**<br>Risk Treatment Plan (1-2) |
| Section 1: Accreditation Status | |
| Section 2: Basic Information<br>Business Context of IS (0-2)<br>Description of Asset (0-2)<br>Interconnections and Interfaces (0-2)<br>Scope of Risk Management and Accreditation (1-2)<br>Responsibilities and Functions (0-2) | Section 4: Development, Acceptance and In-Service<br>Risk Management Plan (1-2) |

## Stage 3 Options Assessment and Selection

### AIM:

To assess proposed options against IA requirement, select solution and ensure processes meet requirements for IA risk management, prior to development.

***OGC Gateway TM 3 – Investment Decision:*** *Confirm recommended investment decision is appropriate before contract and assess whether the business needs are being met and that necessary processes are in place to achieve a successful outcome after contract award.*

### KEY NOTES:

- Evaluate proposals against the IA requirement.
- Check IA deliverables required under the development are specified in the contract and those produced "in-house" are allocated adequate resources.
- Align IA and other project and development activities and milestones.
- Ensure funding provision for all identified IA activities.

### INFORMATION REQUIRED:

- Tender proposals (or system development specifications);
- Business or operational requirement, asset register and business change management plans;
- Draft contract and supplier development and implementation plans;
- Risk Management and Accreditation Document Set (RMADS) from Stage 2.

### ACTIVITIES:

#### Evaluate proposals against the IA requirement

Evaluate all proposals against the IA requirement as agreed and stated in the RMADS. This may require a separate IA compliance matrix. Also ensure that risk appetite and governance issues raised by the various proposals are compatible with the organisation's policy. Any deviations should be recorded under each option and deviations in the final selection must be escalated and formally accepted at the relevant level.

#### Check contract for IA deliverables

Once the selection is approved, the draft contract and/or development specifications should be checked to ensure all required IA deliverables are specified during development through to acceptance. In the case of services, the contract must accommodate all IA requirements through life of the service.

#### Ensure funding provision for in-house deliverables

Ensure funding has been allocated for all IA deliverables to be produced "in-house".

#### Revise and agree the risk management plan

Following final selection, the risk management plan should be revised and aligned with project and development plans. Implementation plans should be checked to ensure they reflect the IA specific activities and milestones.

For complex developments, consider producing a separate IA verification and test schedule for the development, acceptance and for periodic checks in-service. Whether or not in a separate schedule or in the risk management plan, it is essential that requirements for routine administrative checks and auditing and periodic compliance tests and checks are identified and also incorporated into business change management plans and are adequately funded

### Revise IA policy documentation

Following final selection, revise all IA policy documentation as appropriate to reflect the chosen solution. In addition to the RMADS, amendments may be required to the corporate IA policy.

### PRODUCTS:

| | |
|---|---|
| **Tender evaluation (compliance matrix, options, preferences and recommendations as appropriate);**<br>**Amendments or additional information into business change management plan and applications for funding.** | |
| Risk Management and Accreditation Document Set (RMADS) | |
| Contents List (0-3)<br>Links and Dependencies (0-3)<br>Register of Applicable Legislation (0-3)<br>Compliance with Corporate Policies (1-3) | Section 3: Risk Management<br>Corporate Risk Environment (0-3)<br>Threat Assessment (0-3)<br>Vulnerability Assessment (1-3)<br>Risk Assessment (1-3)<br>Countermeasures List (2-3)<br>Risk Treatment Plan (1-3) |
| Section 1: Accreditation Status | |
| Section 2: Basic Information<br>Business Context of IS (0-3)<br>Description of Asset (0-3)<br>Interconnections and Interfaces (0-3)<br>Scope of Risk Management and Accreditation (1-3)<br>Responsibilities and Functions (0-3)<br>**Review Process (3)** | Section 4: Development, Acceptance and In-Service<br>Risk Management Plan (1-3) |

# Stage 4 Accreditation in Development and Acceptance

## AIM:

To confirm that the delivered solution is fit for purpose in terms of the security requirement and can be accredited for business use.

***OGC Gateway* TM *4 – Readiness for Service:*** *Confirm whether the solution is robust before delivery and takes place after all testing has been completed and before roll-out or release.*

## KEY NOTES:

- Provide evidence during development that the Information System (IS) meets its Information Assurance (IA) requirement and take decision whether it can be accredited for business use.
- Ensure requirements for change management are addressed.
- In a technical refresh project address requirements for disposal or transfer of superseded assets (see Stage 6).
- Develop appropriate procedures for in-service risk management.

## INFORMATION REQUIRED:

- Additional information as available, including:
- Project, development and IA specific progress reports;
- Results of verification and testing activities;
- Changes and change control information.;
- Risk Management and Accreditation Document Set (RMADS) from Stage 3.

## ACTIVITIES:

### Maintain good co-operation between stakeholders

Maintain good co-operation and interaction between all relevant parties at this stage by means of appropriate representation on project groups etc. (e.g. Information Security Forum (ISF) or security accreditation panel) to ensure that the IS meets its IA requirement.

### Gain assurance by appropriate verification and validation processes

Ensure there is appropriate validation and testing during development to gain assurance that that the IS meets its IA requirements and that the results of validation and verification activities are clearly documented to support the accreditation decision.

### Monitor development to address problems as they arise

Provide processes to monitor the development, including regular review of the IA risk management plan to ensure early identification of problems, so that any issues of non-compliance can be raised to the appropriate authorities for immediate consideration, impact assessment and decision taking.

### Further develop RMADS in preparation for entry into service

Maintain the accreditation documentation under constant review and good configuration management. Security operating procedures (SyOPs) and incident management, reporting and response procedures must be in place and approved before entry into service and roles and responsibilities must be clearly identified. Immediately prior to the accreditation decision ensure any changes to the delivered solution have been approved and are reflected in the document.

### Review requirements for change management

Review IA requirements for change management, including adequate and timely training for all users, and ensure that these are incorporated into the business change management plan.

### Accreditation Decision

Determine whether the IS may be formally accredited for business use on the basis of the evidence presented and issue an accreditation certificate as appropriate.

### PRODUCTS:

| | |
|---|---|
| **Amendments to Business Change Management Plan**<br>**Early notification of non-compliance as appropriate** | |
| Risk Management and Accreditation Document Set (RMADS) | |
| Contents List (0-4)<br>Links and Dependencies (0-4)<br>Register of Applicable Legislation (0-4)<br>Compliance with Corporate Policies (1-4) | Section 3: Risk Management<br>Corporate Risk Environment (0-4)<br>Threat Assessment (0-4)<br>Vulnerability Assessment (1-4)<br>Risk Assessment (1-4)<br>Countermeasures List (2-4)<br>Risk Treatment Plan (1-4) |
| Section 1: Accreditation Status<br>**Accreditation Statement (4)** | |
| Section 2: Basic Information<br>Business Context of IS (0-4)<br>Description of Asset (0-4)<br>Interconnections and Interfaces (0-4)<br>Scope of Risk Management and Accreditation (1-4)<br>Responsibilities and Functions (0-4)<br>Review Process (3-4) | Section 4: Development, Acceptance and In-Service<br>Risk Management Plan (1-4)<br>**Results of IA Verification and Testing (4)**<br>**Security Operating Procedures (4)**<br>**Incident Management Reporting and Response (4)**<br>**Decommissioning and Disposal (4)** |

## Stage 5 Performance and Resource Review

### AIM:

To confirm performance and resource provision in accordance with Information Assurance (IA) requirement.

***OGC Gateway*** $^{TM}$ ***5 – Benefits Review:*** *Evaluation to whether the solution delivers benefits to the business and continues to meet the business requirement.*

### KEY ISSUES:

- Confirm that the Information System (IS) is performing effectively in accordance with its IA requirement.
- Establish any problems in practice and confirm adequate resources.

### INFORMATION REQUIRED:

- Information as available on asset performance, including any audit and inspection records, asset management and user feedback;
- Risk Management and Accreditation Document Set (RMADS) from Stage 4.

### ACTIVITIES:

#### Review effectiveness in accordance with IA requirement

After approximately 6 months, confirm that the IS is performing effectively in accordance with its IA requirement. This will require input from IS management and users as well as from IA compliance staff as appropriate.

#### Establish any problems and confirm adequate resources

Establish any problems in practice and confirm that resources are adequate to support the IA management requirements.

#### Review the IA requirement

Review and revise the IA requirement in the line with any changes in the business requirement and other aspects, including any changes to the threat. Revise the RMADS as required.

#### Make recommendations

Provide recommendations for input into IS evaluation assessments or reports as appropriate.

**PRODUCTS:**

| **Recommendations to IS evaluation assessments or reports (5)** | |
|---|---|
| Risk Management and Accreditation Document Set (RMADS) | |
| Contents List (0-5)<br>Links and Dependencies (0-5)<br>Register of Applicable Legislation (0-5)<br>Compliance with Corporate Policies (1-5) | Section 3: Risk Management<br>Corporate Risk Environment (0-5)<br>Threat Assessment (0-5)<br>Vulnerability Assessment (1-5)<br>Risk Assessment (1-5)<br>Countermeasures List (2-5)<br>Risk Treatment Plan (1-5) |
| Section 1: Accreditation Status<br>Accreditation Statement (4-5) | |
| Section 2: Basic Information<br>Business Context of IS (0-5)<br>Description of Asset (0-5)<br>Interconnections and Interfaces (0-5)<br>Scope of Risk Management and Accreditation (1-5)<br>Responsibilities and Functions (0-5)<br>Review Process (3-5) | Section 4: Development, Acceptance and In-Service<br>Risk Management Plan (1-5)<br>Results of IA Verification and Testing (4-5)<br>Security Operating Procedures (4-5)<br>Incident Management, Reporting and Response (4-5<br>Decommissioning and Disposal (4-5)) |

# Stage 6 Risk Management In-Service and Accreditation Maintenance

## AIM:

To manage security effectively throughout the in-service life of the Information System (IS), to ensure continuing compliance with its Information Assurance (IA) requirements and terms of accreditation.

***Business Process: Post Implementation Reviews:*** *Management of service, relationship with provider and changing requirements and updates to business case.*

## KEY NOTES:

- Risk management and accreditation continue through in-service life.
- Ensure the IS is used securely, in accordance with the IA requirements.
- Implement agreed processes for verification and validation.
- Provide a continuous review process throughout the life of the asset.

## INFORMATION REQUIRED:

- Additional information as appropriate on business requirements, any proposed changes and results and reports from verification and validation activities
- Asset management and user feedback;
- Risk Management and Accreditation Document Set (RMADS) from Stage 5.

## ACTIVITIES:

### Implement processes for continuing IA risk management and accreditation

Risk management and accreditation do not stop with the issue of the accreditation certificate. Ensure adequate measures and processes are in place to manage IA requirements throughout in-service life of the IS.

### Implement corporate governance processes

Maintain and revise corporate security policies as appropriate, including IA policy, business continuity, disaster recovering and forensic readiness planning and exercise as appropriate.

### Practice secure asset management

Implement procedures for configuration control, software patching and malicious software control, intruder detection and intrusion prevention, as appropriate.

### Secure Asset Use

Ensure the IS is used securely and in accordance with approved security operating procedures.

### Verification, Validation and Response

Ensure implementation of agreed processes of verification, validation and response, including as appropriate compliance checks, audits and inspections, content checking, monitoring and incident management procedures.

### Maintain the RMADS

Maintain and revise the RMADS under good configuration control.

### Carry out a continuous review process

Carry out a continuous review process throughout the life of the asset, including review of performance and resource, risk assessment and accreditation. New versions of the accreditation statement should be issued as appropriate.

**PRODUCTS:**

<table>
<tr><td colspan="2"><b>Amendments to corporate policies as appropriate (6)</b></td></tr>
<tr><td colspan="2">Risk Management and Accreditation Document Set (RMADS)</td></tr>
<tr><td>Contents List (0-6)<br>Links and Dependencies (0-6)<br>Register of Applicable Legislation (0-6)<br>Compliance with Corporate Policies (1-6)<br>Section 1: Accreditation Status<br>Accreditation Statement (4-6)<br><b>Accreditation History (6)</b></td><td>Section 3: Risk Management<br>Corporate Risk Environment (0-6)<br>Threat Assessment (0-6)<br>Vulnerability Assessment (1-6)<br><i>Risk Assessment (1-6)</i><br>Countermeasures List (2-6)<br>Risk Treatment Plan (1-6)</td></tr>
<tr><td>Section 2: Basic Information<br>Business Context of IS (0-6)<br>Description of Asset (0-6)<br>Interconnections and Interfaces (0-6)<br>Scope of Risk Management / Accreditation (1-6)<br>Responsibilities and Functions (0-6)<br>Review Process (3-6)</td><td>Section 4: Development, Acceptance and In-Service<br>Risk Management Plan (1-6)<br>Results of IA Verification and Testing (4-6)<br>Security Operating Procedures (4-6)<br>Incident Management Reporting and Response (4-6)<br>Decommissioning and Disposal (4-6)</td></tr>
</table>

# Stage 7 Secure Decommissioning and Disposal

## AIM:

To manage the secure decommissioning and disposal of an Information System (IS) in accordance with the business requirement, Information Assurance (IA) policy, legal requirements and regulatory standards.

***Business Process: Closure:*** *To end contract, decommission and dispose as appropriate.*

## KEY NOTES:

- Ensure the IS is decommissioned and disposed or transferred, in accordance with applicable policies, laws and other applicable regulations or standards.
- Address requirements for transfer or archive and future access of information.
- Cancel or transfer licences and notify interfaces/interconnections.

## INFORMATION REQUIRED:

- Corporate security policies, relevant laws, statutory regulations and other appropriate policies and standards;
- Confirmation of user requirements for information availability;
- Confirmation of notification to interfaces;
- Risk Management and Accreditation Document Set (RMADS) from Stage 6.

## ACTIVITIES:

### Ensure secure decommissioning, transfer or disposal

Ensure the IS is decommissioned and disposed or transferred, in accordance with the organisation's security policies and any other applicable laws, statutory regulations, policies and standards.

### Prepare a formal record of decommissioning

Prepare a formal record of all decommissioning activities, with each activity signed of as completed by responsible officers, supported by copies of relevant documents. This will be required by the accreditor to support the compliance certificate.

### Address requirements for information transfer, archive and access

Address any requirements for transfer or archive and future access of information, prior to system cleansing, destruction or transfer.

### Cancel or transfer licences

### Notify interfaces and interconnections

Issue notification of decommissioning to all interfaces and/or interconnections as appropriate.

### Security Decommissioning Compliance Certificate

Issue a Security Decommissioning Compliance Certificate once compliance has been verified.

## PRODUCTS:

| Risk Management and Accreditation Document Set (RMADS) | |
|---|---|
| Contents List (0-7)<br>Links and Dependencies (0-7)<br>Register of Applicable Legislation (0-7)<br>Compliance with Corporate Policies (0-7) | Section 3: Risk Management<br>Corporate Risk Environment (0-7)<br>Threat Assessment (0-7)<br>Vulnerability Assessment (1-7)<br>Risk Assessment (1-7)<br>Countermeasures List (2-7)<br>Risk Treatment Plan (1-7) |
| Section 1: Accreditation Status<br>Accreditation Statement (4-7)<br>Accreditation History (6-7)<br>**Security Decommissioning Compliance Certificate (7)** | |
| Section 2: Basic Information<br>Business Context of IS (0-7)<br>Description of Asset (0-7)<br>Interconnections and Interfaces (0-7)<br>Scope of Risk Management / Accreditation (1-7)<br>Responsibilities and Functions (0-7)<br>Review Process (3-7) | Section 4: Development, Acceptance and In-Service<br>Risk Management Plan (1-7)<br>Results of IA Verification and Testing (4-7)<br>Security Operating Procedures (4-7)<br>Incident Management Reporting and Response (4-7)<br>Decommissioning and Disposal (4-7) |

# PART 3 RISK MANAGEMENT & ACCREDITATION DOCUMENTATION

**HEALTH WARNING**

Adapt the guidance to the Information System in question and only produce documentation which is appropriate to this specific case.

186. Part 3 of this Guide provides guidance on the production of the documentation required for risk management and accreditation. It should be used in conjunction with Part 2 “The Process” and only once the user is well conversant with the principles and concepts covered in Part 1. The document or documents, henceforth referred to as the Risk Management and Accreditation Document Set (RMADS), should be appropriate to the Information System (IS) in question.

187. In order to provide linkage between the process and the documentation, the relevant process stages are shown in brackets throughout.

188. Clear, concise and appropriate documentation underpins the risk management process and the formal accreditation decision. The nature and extent of documentation will vary considerably and, in many cases, only a minimal RMADS will be required because the accreditation scope is largely within the existing corporate IA policy. Wherever it is possible to refer to existing documentation, which covers the relevant aspects of IA, this should be done.

189. Risk management and accreditation documentation should provide justification and accountability for risk management decisions, the basis for risk management, accreditation and day to day security procedures and a benchmark for compliance monitoring.

190. The documentation will be developed throughout the project and IS lifecycle and should always be held under continuous review and good configuration management. As such preparation and management of the documentation will be the responsibility of the project management staff through to IS acceptance and thereafter the responsibility of the IS management staff. The accreditor is the endorsing authority.

191. Except in the case of very limited, self-contained information systems, it is unlikely that any one document could fulfil all the aspects of accreditation. In most cases, a portfolio of related documents will be required. This accreditation documentation should be fully accountable and traceable to the business and security requirements.

192. Part 3 is also published as a Word ™ Template, should organisations wish to use or adapt this format for their documentation. Click on the following link to go to the template: NISCC Guide - Template: Risk Management and Accreditation Documentation.

# Risk Management and Accreditation Document Set

***[Title of Information System]***

The Risk Management and Accreditation Document Set (RMADS) and any separate sections or documents, which may comprise the ADS, must:

a. have a unique reference number and date;

b. identify the author and owner;

c. be subject to version control;

d. list any documents it supersedes.

**Reference:** *[RMADS Reference Number]*

**Date:** *[Document Issue Date]*

**Author:** *[Name and Position/Title]*

**Owner:** *[Name and Position/Title]*

## Contents List:

Whether or not the RMADS is a single document, it is always useful to include a contents list and, in the case of a number of separate documents, this is essential.

This should include those deliverables identified and agreed at Stage 3.

## Links and Dependencies

List with appropriate references all related policy and other documents (illustrate relationships with diagram if appropriate), e.g. Corporate IA Policy, Business Continuity Plan, Disaster Recovery Plan, Forensic Readiness Plan and the respective Asset Register.

Where there are requirements for interconnections to other systems, appropriate policies and agreements (e.g. Code of Connection (CoCo)) should be clearly referenced and, if appropriate, also appended to the RMADS.

| Document Title | Reference | Date | POC |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

## Register of Applicable Legislation

List the legal, statutory and regulatory requirements that apply to the ICT asset in question. It is important that advice on particular aspects of legal requirements should be sought from the organisation’s legal advisor. (see also Appendix B).

## Compliance with Corporate Policies

State compliance with relevant corporate policies, as applicable. In cases of non-compliance with any aspects, these should be recorded and reviewed separately and reference only made in this section.

## Section 1: Accreditation

### 1.1. Accreditation Statement

The RMADS should contain the most current version of this statement, which is a formal record of the accreditation decision. It must be signed and dated by the accreditor and include details of significant residual risks and caveats as appropriate.

### 1.2. Accreditation History

If appropriate, provide details of accreditation history – e.g. when asset was first accredited.

### 1.3. Security Decommissioning Compliance Certificate

This is the confirmation that an asset has been decommissioned in accordance with the IA requirements. It should be signed and dated by the accreditor.

## Section 2: Basic Information

This section of the RMADS sets the asset in the context of the organisation's business, describes the security-relevant aspects of the asset, outlines security requirements that need to be met, and defines the scope and management of the accreditation.

### 2.1. Business Context of the IS

This shows that the business needs of the organisation are understood and fed into the risk management process, and should cover:

- organisational ownership of the asset
- high level business aims and objectives served by the asset
- business functions supported by the asset
- information processes carried out by the asset

Organisation and/or process diagrams may be useful.

## 2.2. Description of IS

This should provide a pen picture of the asset, highlighting the most relevant aspects and providing (or referencing) details as appropriate of:

- information (description, quantity, sensitivity)
- hardware (main items, with reference to inventory)
- software (main items, with reference to inventory)
- communications (from/to, purpose, type, sensitivity)
- people (user groups, roles, organisations, personnel check / security clearances)
- locations (may be covered under above headings)

A schematic architecture diagram may be useful and, in the case of complex IS - a technical security architecture paper.

## 2.3. Interconnections and interfaces

Describe each link, grouping multiple instances of identical links. A table and/or diagram(s) may be useful. Detail may include ownership, business justification, data flows, technical details (protocols), sensitivities, etc.

## 2.4. Scope of Risk Management and Accreditation

Specify the risk management and accreditation boundaries and detail any specific exclusions. A diagram may be helpful.

## 2.5. Responsibilities and Functions

List ownership and security functions for risk management and accreditation through the full lifecycle with brief descriptions of key responsibilities and posts to which these functions are assigned. These should include ownership, policy, compliance and asset management and should be linked to appropriate Security Operating Procedures.

These will change, in particular on transfer from Project Development to In-service. Original information should be archived at such times so that the RMADS always contains the extant responsibilities and functions.

## 2.6. Review Process

State the review process and conditions for immediate review of accreditation status.

## Section 3: Risk Management Documents

### 3.1 Corporate Risk Environment

Where this is not already covered in a Corporate IA Policy, provide details as appropriate of the business risk environment, an overview of the top level business risks and the organisation’s risk appetite and constraints.

### 3.2 Threat Assessment

Summarize results of the threat assessment and highlight any major issues. Refer to full report for details as appropriate. (Note: the threat assessment may be generic for the organisation or asset specific).

### 3.3 Vulnerability Assessment

Provide results of the vulnerability assessment. If this is a detailed report and placed in annex, highlight any major issues here and refer to full report for details. (Note: the vulnerability assessment will always be asset specific).

### 3.4 Risk Assessment

State the method used. Provide results of the risk assessment. If this is a detailed report and placed in annex, highlight the most significant identified risks here and refer to full report for details. (Note: the risk assessment will always be asset specific).

### 3.5 Countermeasures List

Provide details of each countermeasure including description and business justification together with estimated costs.

### 3.6 Risk Treatment Plan

The information in the risk treatment plan will be derived from the activities detailed above. The document should include:

- Reference number
- Asset
- Threat/Vulnerability
- Business Impact
- Treatment (ie avoid, mitigate, accept, transfer)
- Specific countermeasure(s)
- Status
- Cost
- Owner
- Date Recorded

The "risk treatment plan" may support ISO17799 compliance. There are a number of possible formats for the plan. It should ensure that selected countermeasures can be traced back through prioritised risks to threats and vulnerabilities and vice versa.

Significant residual risks must be highlighted and included in the accreditation statement.

## Section 4: Development, Acceptance and In-Service

### 4.1 Risk Management Plan

During the development and acceptance stage this plan should set out clear milestones and deliverables for IA management, linked to the main project or development milestones. On entry into service, the development and acceptance plan should be archived.

Before acceptance, a new plan should be developed to set out the arrangements to meet the requirements for risk management in-service and continuing accreditation, linked to the ongoing business requirements and changes.

In the case of complex assets, a separate schedule for verification, inspection and/or testing may be produced, as a sub-set of the risk management plan.

Plans should always include: configuration control of asset, configuration control and update of the RMADS, requirements reviews, verification and validation requirements, provision of training and awareness, indication of personnel responsible for actions.

## 4.2 Results of IA Verification and Testing

Summarise the results of IA verification and testing, referring to full report for details as appropriate. Highlight any major issues and where these relate to non-compliance with the IA requirement, an exception must be raised.

Note: results may be drawn from other testing, particularly during development, e.g. Factory or System Acceptance Tests, or may be IA specific – e.g. Health Checks or Comsec Installation Inspections.

The RMADS should always include the most current results; older reports, which have been entirely superseded may be archived.

## 4.4 Security Operating Procedures

Security Operating Procedures (SyOPs) are an important part of the RMADS, but may be embedded within a number of separate documents covering the management, operation, and use of individual assets. These may include detailed technical documents (such as a Network Operations Manual), corporate standards documents (such as a Staff Handbook), and User Guides for various groups of end-users.

Even where individual documents are entirely devoted to SyOPs, in any but the simplest cases, it will be impractical to include the full text of all SyOPs in this section of the RMADS.

This section should, as a minimum:

- confirm that the required SyOPs:
    - exist for all assets;
    - have been issued to the appropriate audiences;
    - have been read and understood and where appropriate, asset management staff and users have signed to confirm acceptance of the conditions;
    - are monitored in operation and subject to regular review; and
    - are maintained under formal change control arrangements which include the requirement to consult the Accreditor about significant change proposals.
- list all documents that contain SyOPs and, for each, provide:
    - document title, reference, version, and date;
    - ownership and responsibility for management of the document;
    - distribution of the document; and
    - an outline of the SyOPs content of the document.
- highlight key accreditation issues and summarise how these are addressed by relevant SyOPs.

It should be noted that some SyOPs documents will include information about security arrangements that could be of help to a would-be attacker. The distribution of such documents should suitably limited and they should be protected accordingly.

### 4.4 Incident Management, Reporting and Response

State arrangements for incident management, reporting procedures and response requirements unless these are already covered in a corporate policy, in which case refer out to the relevant document and section.

Provide instructions for foreseeable problems, for example power outage, virus infection, loss of media items, hardware or link failure, and give details of individuals/posts/functions in the organisation who should be contacted for help.

Give clear procedures for incident reporting (both local and national) and outline response provisions.

### 4.5 Decommissioning and Disposal

State the requirements for secure decommissioning and disposal including transfer of information, cleansing and notification to managers of interconnected IS.

Formally record of all activities, with each signed off by responsible officers, and reference all supporting documents, as evidence of compliance.

# GLOSSARY

**Accreditation** Accreditation is the formal assessment of the IS against its IA requirements, resulting in the acceptance of residual risks in the context of the business requirement. It is a prerequisite to approval to operate.

**Accreditation Document Set (ADS)** An alternative to the term RMADS

**Asset** Anything that has value to the organisation, its business operations and its continuity.

**Assured Products** IT products which have been approved by government as having a recognised level of security efficiency.

**Authentication** Ensuring that the identity of a subject or resource is the one claimed.

**Availability** Ensuring that authorised users have access to information and associated assets when required.

**BCP** Business Continuity Plan: outline of the action to be taken in event of a serious disruption and priorities for recovery, in order to keep an organisation running as normally as possible at all times, even in an emergency.

**BCM** Business Continuity Management

**BS7799** BS7799-2 also known as BS7799: Part 2 is a British Standard, wholly consistent with IEC/ISO 17799 that specifies requirements for establishing, implementing and documenting Information Security Management Systems.

**CCB** Configuration Control Board

**CNI** Critical National Infrastructure: the most important elements of the nation's infrastructure involving vital systems and services, such as communications and utilities.

**Code of Connection (CoCo)** An agreement on the policy and rules for the connection of internal or external assets which are subject to different management domains.

**Comsec** Communications security

**Confidentiality** Ensuring that information is accessible only to those authorised to have access.

**Defence-in-Depth** A number of different controls used to mitigate a specific risk (or set of related risks), in order to reduce the residual risk to an acceptable level

**Disaster Recovery** The process of recovering from an emergency, including the immediate aftermath and priorities for the critical business functions which need to be resumed.

**DRP** Disaster Recovery Plan

**Forensic Readiness** Forensic readiness is the ability of an organisation to maximize its potential to use digital evidence whilst minimizing the costs of an investigation.

**FRP** Forensic Readiness Plan

**Governance** The set of policies and internal controls by which organisations are directed and managed, in order to ensure an appropriate level of responsibility and accountability.

**GSi** Government Secure Intranet.

**Impact** The result of an information security incident, caused by a threat, which affects assets.

**Information Assurance (IA)** The confidence that information assets will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

**Information Security (Infosec)** The security preservation of confidentiality, integrity and availability of information.

**Information Security Forum (ISF)** The BS7799 scope-level security management body

**Information Security Management System (ISMS)** That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (within the defined BS7799 scope).

**Information System(s) (IS)** For the purposes of this Guide, an IS will include the following: physical environment (e.g. buildings, communications facilities and links, computer hardware); information and data; software; service provision; people; intangibles (e.g. reputation, goodwill).

**Integrity** The safeguarding the accuracy and completeness of information and processing methods.

**ISO17799** ISO/IEC 17799 is the International Standard for Information Security Management. It specifies a comprehensive range of controls that can be used to establish an information security management system using a risk-based approach.

**IT Health Check** An analysis of a system to ensure correct implementation of security functions and identify vulnerabilities which may compromise the confidentiality, integrity or availability of information.

**Mitigation** Limitation of the negative consequence of a particular event.

**Non-Repudiation** The ability to prove an action or event has taken place, so that this event or action cannot be repudiated later.

**PDCA** Plan-Do-Check-Act: ISO17799 "virtuous circle" model

**Risk** The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

**Risk Acceptance** Decision to accept a risk.

**Risk Analysis** The systematic use of information to identify sources and to estimate the risk.

**Risk Appetite** Attitude taken by an organisation, which in relation to risk minimises the negative and maximises the positive business consequences and their respective probabilities.

**Risk Assessment** Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.

**Risk Avoidance** Decision not to be involved in, or action to withdraw from, a risk situation.

**Risk Identification** Process to find, list and characterize elements of risk.

**Risk Management** The process of identifying, controlling and minimising or eliminating security risks that may affect information systems, for an acceptable cost.

**Risk Management and Accreditation Document Set (RMADS)** The documentation, which specifies the IA risk management and accreditation policy, conditions and status of an IS (often referred to simply as the ADS).

**Risk Management System** Set of elements of an organisation's management system concerned with managing risk.

**Risk Mitigation** See "Mitigation"

**Risk Transfer** Sharing with another party the burden of loss or benefit of gain, for a risk.

**Risk Treatment** The process of selection and implementation of measures to modify risk (mitigate, avoid, transfer or accept).

**Risk Treatment Plan** The plan demonstrates that the risks have been properly identified, assessed and countermeasures allocated. It will also record the implementation status of each countermeasure.

**Senior Information Risk Owner (SIRO)** Member of senior management board with responsibility for IA governance and risk ownership in the organisation on behalf of the board.

**Statement of Applicability** (ISO7799) Document describing the control objectives and controls that are relevant and applicable to the organisation's ISMS, based on the results and conclusions of the risk assessment and risk treatment processes.

**Threat** A potential cause of an incident that may result in harm to a system or organisation.

**Trojan** A program designed to allow it unauthorised access to the computer systems it infects. Trojans may also be used in order to exploit a computer system to send unsolicited e-mails.

**Virus** A computer program designed to run on one computer (often with undesirable effects such as deleting files or sending unsolicited e-mails) and to send copies to as many other computers as possible.

**Vulnerability** A weakness of an asset or group of assets that can be exploited by one or more threats.

**Worm** An independent computer programme that replicates from machine to machine across network connections, often clogging information systems as it spreads.

# APPENDIX A: CROSS REFERENCE BETWEEN INFOSEC NISCC GUIDE AND ISO17799 CONTROL OBJECTIVES

## 1. Governance and Risk Management Concepts

| **IS2 Part 1 Sections**<br>**[Governance and Risk Management Concepts]** | **17799 Control Objectives** |
|---|---|
| **A - General Overview:**<br>Governance and Risk Management; Legal and Statutory Responsibilities | 4 12 |
| **B - Responsibilities and Functions:**<br>Ownership; Policy; Compliance; Delivery; IA Committees, Panels and Groups | 4 5 8 |
| **C - Corporate IA Policy** | 3 5 |
| **D - Scope of Accreditation and Interconnection Policies** | 4 8 9 |
| **E - Risk Management** | 7 8 9 10 |
| **F - Assurance and the Accreditation Decision:**<br>Verification, Validation and Evaluation | 6 7 8 9 12 |
| **G - Risk Management In-Service and Accreditation Maintenance:**<br>Secure IS Management; Verification, Validation and Response; Maintenance of RMADS | 4 5 6 8 9 10 11 12 |
| **H - Secure Decommissioning and Disposal** | 4 12 |

## 2. Risk Management and Accreditation Documentation

| BS7799 Control | Description | IS2 Part 3 |
|---|---|---|
| **1) Security Policy** | | |
| **1.1.1** | Information Security Policy Document (ISPD) | Depends on BS7799 compliance scope. If BS7799 Scope is at Corporate level, then the ISPD could be referenced under Compliance with Corporate Policies.<br>However, if it is intended that BS7799 Scope will be at IS (asset) level, then may be more logical to place under part of 2.1 – Business Context. |
| **1.1.2** | Review and evaluation of ISPD | Within ISPD itself as part of the RMADS portfolio. |
| **2) Organisational Security** | | |
| **2.1.1** | Management Information Security Forum (ISF) | As 2.5, depending upon scope either part of Business or Corporate Context. |
| **2.1.2** | Information Security coordination | Could be referenced under Compliance with Corporate Policies of include in part of 2.1 – Business Context |
| **2.1.3** | Allocation of Information Security responsibilities | Include in 2.5 – Responsibilities and Functions. Also needs a hook out at 2.1 to link into corporate security functions. |
| **2.1.4** | Authorization process for information processing facilities | Part of 4.3 – SyOPs. |
| **2.1.5** | Specialist Information Security advice | Part of 2.5 – Responsibilities and Functions. May also be a hook out at 2.1 to cover corporate security advice and guidance. |
| **2.1.6** | Co-operation between organisations | This refers to contact points in external organisations. As such probably best under 4.3 – SyOPs though there may be an argument for placing under 2.3 – Interconnections and Interfaces and reference to Corporate Policy where established communications channels may already exist. |
| **2.1.7** | Independent review of Information Security | This refers to testing to verify the implementation of the IA Requirements. It will thus come within 4.2 prior to formal accreditation and also as part in service risk management. |

| BS7799 Control | Description | IS2 Part 3 |
|---|---|---|
| **2.2.1** | Identification of risks from third-party access | The third party connections will be identified in 2.3.  The Risk Assessment in 3.4 should identify the risks from these connections.  Risk Treatment will inform how contractual arrangements should be approached (Transfer [to third party] or Mitigate [Internally]). |
| **2.2.2** | Security requirements in third-party contracts | |
| **2.3.1** | Security requirements in outsourcing contracts | |
| **3) Asset Classification and Control** | | |
| **3.1.1** | Inventory of assets | The formal register is likely to be a separate document to the portfolio but should be listed under Links and Dependencies. |
| **3.2.1** | Classification guidelines | These all fit within Compliance with Corporate Policies unless there are special requirements for the particular IS in which case they would presumably fit under 2.1 – Business Context of the IS. |
| **3.2.2** | Information labelling and handling | |
| **4) Personnel Security** | | |
| **4.1.1** | Including security in job responsibilities | These all fit within Compliance with Corporate Policies unless there are special requirements for the particular IS which case they would presumably fit under 2.1 – Business Context of the IS and 2.5 – Roles and Functions. |
| **4.1.2** | Personnel screening and policy | |
| **4.1.3** | Confidentiality agreements | |
| **4.1.4** | Terms and conditions of employment | |
| **4.2.1** | Information Security education and training | Two aspects: there is the generic material that comes under Compliance with Corporate Policies t; and the specific material that comes under 4.1 – Risk Management Plan and 4.3 - SyOPs. |
| **4.3.1** | Reporting security incidents | Section 4.4 – Incident Management, Reporting and Response and also Section 4.3 – SyOPs should include procedures for reporting these and other problems. |
| **4.3.2** | Reporting security weaknesses | |
| **4.3.3** | Reporting software malfunctions | |
| **4.3.4** | Learning from incidents | Section 4.4 – Incident Management, Reporting and Response. Dependent upon Scope, this could be under 2.1 – Business Context. There should also be an onward link into Corporate Policy. |
| **4.3.5** | Disciplinary process | Compliance with Corporate Policies. |

| BS7799 Control | Description | IS2 Part 3 |
|---|---|---|
| **5) Physical and Environmental Security** | | |
| **5.1.1** | Physical security perimeter | This will normally be part of Compliance with Corporate Policies. However, where the Business associated with the IS is isolated and distinct from the corporate entity, it could come under 2.1 – Business Context and 2.2 – Description of IS. |
| **5.1.2** | Physical entry controls | |
| **5.1.3** | Securing offices, rooms and facilities | |
| **5.1.4** | Working in secure areas | |
| **5.1.5** | Isolated delivery and loading areas | |
| **5.2.1** | Equipment siting and protection | These will generally come under 3.5 – Countermeasure List though there may be supporting procedures in 4.3 – SyOPs. |
| **5.2.2** | Power supplies | |
| **5.2.3** | Cabling security | |
| **5.2.4** | Equipment maintenance | |
| **5.2.5** | Security of equipment off-premises | |
| **5.2.6** | Secure disposal or re-use of equipment | |
| **5.3.1** | Clear desk and clear screen policy | |
| **5.3.2** | Removal of property | |
| **6) Communications and Operations Management** | | |
| **6.1.1** | Documented operating procedures | Whilst these requirements will be defined in 3.5 – Countermeasure List, the actual detail will be under 4.3 – SyOPs. |
| **6.1.2** | Operational change controls | |
| **6.1.3** | Incident management procedures | |
| **6.1.4** | Segregation of duties | |
| **6.1.5** | Separation of development and operational facilities | This should be defined under 3.5 – Countermeasures List. |
| **6.1.6** | External facilities management | As this refers to contractual terms, it really comes within OGC Gateway 3. As such it constitutes a countermeasure that should therefore appear under 3.5. |
| **6.2.1** | Capacity planning | This should be defined under 3.5 – Countermeasures List with 2.5 – Functions and Responsibilities defining who is responsible for this task and further detail under the SyOPs for relevant posts 4.3. |
| **6.2.2** | System acceptance | 4.1 – Risk Management Plan should contain the IS acceptance criteria and 4.2 – Results of IA Verification and Testing should contain the evidence to support acceptance. |

| BS7799 Control | Description | IS2 Part 3 |
|---|---|---|
| **6.3.1** | Controls against malicious software | Primarily part of 3.5 – Countermeasures List with additional information in 4.3 – SyOPs. |
| **6.4.1** | Information back-up | |
| **6.4.2** | Operator logs | |
| **6.4.3** | Fault logging | Primarily part of 4.3 – SyOPs and 4.4 – Incident Management, Reporting and Response. |
| **6.5.1** | Network controls | Primarily part of 3.5 – Countermeasures List with additional information in 4.3 – SyOPs. |
| **6.6.1** | Management of removable computer media | Whilst the requirements will be defined in 3.5 – Countermeasure List, the actual detail will be under 4.3 – SyOPs. Exchange agreements may also appear in 2.3 – Interconnections and Interfaces. |
| **6.6.2** | Disposal of media | |
| **6.6.3** | Information handling procedures | |
| **6.6.4** | Security of system documentation | |
| **6.7.1** | Security of media in transit | |
| **6.7.2** | Security of media in transit | |
| **6.7.3** | Electronic commerce security | Part of 3.5 – Countermeasures List |
| **6.7.4** | Security of electronic mail | |
| **6.7.5** | Security of electronic office systems | |
| **6.7.6** | Publicly available systems | Part of 4.3 – SyOPs. |
| **6.7.7** | Other forms of information exchange | Could be contained in 2.3 – Interconnections and Interfaces, 3.5 – Countermeasures List or 4.3 – SyOPs or in all. |
| **7) Access Control** | | |
| **7.1.1** | Access control policy | Could be covered by Compliance with Corporate Policies, otherwise part of 3.5 – Countermeasures List |
| **7.2.1** | User registration | Whilst the requirement will be defined in 3.5 Countermeasure List; the detail will be under 4.3 – SyOPs. |
| **7.2.2** | Privilege management | |
| **7.2.3** | User password management | |
| **7.2.4** | Review of user access rights | |
| **7.3.1** | Password use | |
| **7.3.2** | Unattended user equipment | |
| **7.4.1** | Policy on use of network services | Mainly under 3.5 – Countermeasures List |
| **7.4.2** | Enforced path | |
| **7.4.3** | User authentication for external connections | |
| **7.4.4** | Node authentication | |
| **7.4.5** | Remote diagnostic port protection | The requirement will be defined in 3.5 Countermeasure List; the detail will be under 4.3 – SyOPs. |

| BS7799 Control | Description | IS2 Part 3 |
|---|---|---|
| **7.4.5** | Remote diagnostic port protection | The requirement will be defined in 3.5 Countermeasure List; the detail will be under 4.3 – SyOPs. |
| **7.4.6** | Segregation in networks | Mainly under 3.5 – Countermeasures List |
| **7.4.7** | Network connection control | |
| **7.4.8** | Network routing control | |
| **7.4.9** | Security of network services | |
| **7.5.1** | Automatic terminal identification | |
| **7.5.2** | Terminal log-on procedures | |
| **7.5.3** | User identification and authentication | |
| **7.5.4** | Password management system | |
| **7.5.5** | Use of system utilities | Whilst the requirement will be defined in 3.5 - Countermeasure List; the detail will be under 4.3 – SyOPs. |
| **7.5.6** | Duress alarm to safeguard users | |
| **7.5.7** | Terminal time-out | Would expect to be under 3.5 – Countermeasures List unless covered under Compliance with Corporate Policies. |
| **7.5.8** | Limitation of connection time | |
| **7.6.1** | Information access restriction | This should appear under 3.5 – Countermeasures List |
| **7.6.2** | Sensitive system isolation | |
| **7.7.1** | Event logging | Requirement will be defined in 3.5 Countermeasure List; with supporting detail under 4.3 – SyOPs. |
| **7.7.2** | Monitoring system use | |
| **7.7.3** | Clock synchronization | |
| **7.8.1** | Mobile computing | |
| **7.8.2** | Teleworking | |
| **8) Systems Development and Maintenance** | | |
| **8.1.1** | Security requirements analysis and specification | This fits into OGC Gateway$^{TM}$ 1 where the business case is worked up. It is then defined in 2.1 – Business Context and 2.2 Description of IS. |
| **8.2.1** | Input data validation | Requirement will be defined in 3.5 - Countermeasure List; with supporting detail under 4.3 – SyOPs. |
| **8.2.2** | Control of internal processing | |
| **8.2.3** | Message authentication | Requirement will be defined in 3.5 - Countermeasure List. |
| **8.2.4** | Output data validation | Requirement will be defined in 3.5 - Countermeasure List; possibly with supporting detail under 4.3 – SyOPs. |
| **8.3.1** | Policy on the use of cryptographic controls | Will probably come from Compliance with Corporate Policies though for sensitive systems could be under 2.1 – Business Context and 2.2 – Description of IS. |
| **8.3.2** | Encryption | Requirement will be defined in 3.5 - Countermeasure List. |
| **8.3.3** | Digital signatures | |
| **8.3.4** | Non-repudiation services | |

| BS7799 Control | Description | IS2 Part 3 |
|---|---|---|
| **8.3.5** | Key management | Part of 4.3 – SyOPs. |
| **8.4.1** | Control of operational software | |
| **8.4.2** | Protection of system test data | |
| **8.4.3** | Access control to program source library | |
| **8.5.1** | Change control procedures | |
| **8.5.2** | Technical review of operating system changes | |
| **8.5.3** | Restrictions on changes to software packages | Requirement will be defined in 3.5 - Countermeasure List; with supporting detail under 4.3 – SyOPs. |
| **8.5.4** | Covert channels and Trojan code | Part of 4.3 – SyOPs. |
| **8.5.5** | Outsourced software development | This should be covered in part by the outsourcing contract and therefore will come within 2.1 – Business Context and in part by 4.3 – SyOPs; in particular those SyOPs supporting development work and its implementation into “live”. |
| **9) Business Continuity Management (BCM)** | | |
| **9.1.1** | Business continuity management process | This is in part dependent upon the approach to BCM. This would most usually be wholly covered in Compliance with Corporate Policies, especially where the IS asset is tightly coupled to the existing Corporate Infrastructure (physical and technical). However, where there is sufficient segregation, then significant parts of this will need to be covered in 4.3 – SyOPs. |
| **9.1.2** | Business continuity and impact analysis | |
| **9.1.3** | Writing and implementing continuity plans | |
| **9.1.4** | Business continuity planning framework | |
| **9.1.5** | Testing, maintaining and re-assessing business continuity plans | |
| **10) Compliance** | | |
| **10.1.1** | Identification of applicable legislation | The results of this will create the Register of Applicable Legislation. |
| **10.1.2** | Intellectual property rights (IPR) | Comes under 4.3 – SyOPs, in particular rules covering authorization and introduction of new software etc. |

| BS7799 Control | Description | IS2 Part 3 |
|---|---|---|
| **10.1.3** | Safeguarding of organisational records | Comes under 3.5 – Countermeasure List and 4.3 – SyOPs covering archive with a further reference under 4.5 – Decommissioning and Disposal. Note that the legal requirements for archive will fall out of the Register of Applicable Legislation. These requirements should be translated into the business need in 2.1– Business Context, where not already covered under Compliance with Corporate Policies. |
| **10.1.4** | Data protection and privacy of personal information | Where appropriate, this too will be under both 3.5 – Countermeasure List and 4.3 – SyOPs. Clearly DPA will be mentioned in the Register of Applicable Legislation and should form part of Compliance with Corporate Policies. |
| **10.1.5** | Prevention of misuse of information processing facilities | This too will be under both 3.5 – Countermeasure List and 4.3 – SyOPs. |
| **10.1.6** | Regulation of cryptographic controls | Primarily under 4.3 – SyOPs although relevant legislation should be referenced in the Register of Applicable Legislation. Corporate Policies should also cover such aspects and be referenced under Compliance with Corporate Policies. |
| **10.1.7** | Collection of evidence | Primarily under 4.1 – Risk Management Plan, 4.2 – Results of IA Verification and Testing and 4.3 - SyOPs although the Register of Applicable Legislation should include reference to laws on admissibility of evidence and further detail should be contained in the Forensic Readiness Plan (FRP). Compliance with the FRP should be covered under Compliance with Corporate Policies. |
| **10.2.1** | Compliance with security policy | This really fits under 4.1 – Risk Management Plan and 4.2 – Results of IA Verification and Testing during in-service life with a hook to cover 4.5 – Decommissioning and Disposal. It may also be addressed in part under Compliance with Corporate Policies. |

| BS7799 Control | Description | IS2 Part 3 |
|---|---|---|
| **10.2.2** | Technical compliance checking | This is a mix of 4.1 – Risk Management Plan, 4.2 – Results of IA Verification and Testing and 4.3 – SyOPs and will also be addressed in 4.5 – Decommissioning and Disposal. |
| **10.3.1** | System audit controls | This needs to be covered under 3.5 – Countermeasures List and 4.3 – SyOPs but could also be housed under 4.1 – Risk Management Plan together with 4.2 – Results of IA Verification and Testing. It should also be included in any FRP. |
| **10.3.2** | Protection of system audit tools | This needs to be covered under both 3.5 – Countermeasure List, 4.3 – SyOPs and in any FRP. |

THIS PAGE IS INTENTIONALLY LEFT BLANK

# APPENDIX B: RELEVANT LAWS AND REGULATIONS

This appendix outlines the main legal requirements relevant to Information Assurance (IA) and is only intended as a basic guide. It is important that advice on particular aspects of legal requirements should be sought from the organisation's legal advisor.

## Unauthorised Disclosure of Official Information

### Official Secrets Act 1989

Under the Official Secrets Act 1989, it is an offence for a Crown servant or government contractor to disclose official information in any of the protected categories if the disclosure is made without lawful authority and is damaging to the national interest. It is an offence if a member of the public, or any other person who is not a Crown servant or government contractor under the Act, has in his or her possession, official information in one of the protected categories, and the information has been disclosed without lawful authority, or entrusted by a Crown servant or government contractor on terms requiring it to be held in confidence.

## Official Disclosure

### Public Records Acts 1958 and 1967

The law on public records is set out in the Public Records Acts of 1958 and 1967. Public records are defined as "administrative and departmental records belonging to Her Majesty's Government, whether in the United Kingdom or elsewhere". The Public Records Act of 1958 places a responsibility on all government departments to review the records which are produced within the department, to choose those which are worthy of permanent preservation and transfer them to the Public Records Office (PRO), and to destroy all records which are not selected. The 1967 Act stipulates that all surviving public records should normally be released to the public 30 years after their creation.

### Data Protection Act 1998

This Act provides a right of access by living individuals to personal data held about them by any person, subject to any exemption which may apply. It also imposes responsibilities on those who process personal data. The Act requires compliance with eight data protection principles, one of which is ensuring that adequate security is employed when processing personal data.

The Act also requires those persons who hold personal data to register that fact with the Information Commissioner together with a description of the purpose of the processing, the data class (the information processed), its sources and the recipients (persons to whom it may be disclosed).

### Freedom of Information Act 2000

The Freedom of Information Act 2000 relates to the publication and disclosure of information held by public authorities. It gives a statutory right of access to information, which entitles any person to be told on request, subject to certain exemptions, whether the Department holds particular information (the duty to confirm or deny) and, assuming that it does, to have that information communicated to them within 20 working days. The Act also requires all public authorities to maintain a Publication Scheme and to release information proactively and keep the scheme under review.

### Human Rights Act 1998

This Act, which brings the European Convention on Human Rights (ECHR) in UK domestic law, provides every person in the UK certain human rights and fundamental freedoms including the right to privacy and freedom of expression, subject to a number of exceptions. The extent of these rights, including an individual's right to privacy and freedom of expression, has been tested in the European Court of Human Rights and in the domestic courts by a number of cases.

## Communications and Information Systems

### Computer Misuse Act 1990

This deals with the rights of computer owners against the unauthorised use of a computer by any party, making offences of attempted or actual penetration or subversion of computer systems. Under the terms of Section 3 of the Computer Misuse Act it is a criminal offence to introduce unauthorised software into a computer system with the intention of impairing the operation of the computer system or the integrity of any data or program stored within the computer system.

### Copyright (Computer Programs) Regulations

Infringement and copying of Computer Software is governed by the Copyright Designs and Patents Act 1988. Individuals and users should be aware that copyright infringements are not exclusively a matter of civil actions for damages by a copyright owner. The criminal penalties for infringing computer software copyright may include heavy fines, imprisonment (for up to 2 years) and the forfeiture of infringing copies and articles for making them. The Director or CEO of an organisation may also be subject to prosecution for permitting the illegal copying of software or its use within the area of their responsibility.

### Civil Evidence Act 1968 and the Police and Criminal Evidence Act

These acts define conditions under which computer based evidence may be obtained and used.

### Wireless Telegraphy Act 1949

This prohibits the unauthorised use of wireless telegraphy apparatus for the transmission or reception and subsequent disclosure of communications.

### The Communications Act 2003

This Act largely repeals the provisions of earlier communications Acts, e.g. Telecommunications Act 1984, and confers functions on the Office of Communications (OFCOM) and makes provision about the regulation of the provision of electronic communications network and services and the use of the electronic spectrum.

### Regulation of Investigatory Powers Act 2000 (RIPA)

This is a piece of permissive legislation allowing for the interception of communications, the carrying out of surveillance, and the running of covert human intelligence sources in certain limited circumstances. In relation to the interception of communications, authorisation can only be given by the Secretary of State, and in relation to surveillance and source handling activities authorisation must be given senior official level. The Act also confers on the Secretary of State the power to make orders, regulations or rules under various provisions of the Act. RIPA does not prohibit the interception of communications where all parties have consented to the interception (see also below).

### The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

These Regulations authorise certain interceptions of telecommunication communications which would otherwise be prohibited by section 1 of the Regulation of Investigatory Powers Act 2000. The interception has to be by or with the consent of a person carrying on a business for purposes relevant to that person's business and using that business's own telecommunication system.

Interceptions are authorised only if the controller of the telecommunications system on which they are affected has made all reasonable efforts to inform potential users that interceptions may be made.