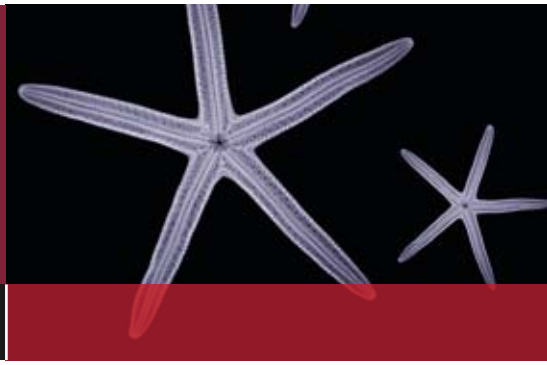
Best Management Practice
For Portfolio, Programme, Project, Risk and Service Management



CLINCH CONSULTING

OGC

ITIL V3 and Information Security

by Jim Clinch

White Paper
May 2009

Synopsis

This paper discusses the role and importance to the business of effective Information Security Management (ISM), how it is supported by an extensive family of global standards and the way these harmonize with ITIL.

The intended readership is business and IT managers familiar with or interested in ITIL. The paper discusses the contents and purposes of, and relationships between global standards, best practice guidance and organizational policies and procedures in the creation of effective ISM.

There is no longer a separate ITIL publication on Security Management, so the paper explores the role of ISM within ITIL and how ITIL and the available ISM standards and guidance are aligned and can work together. ISM content in ITIL is mapped to the ISO/IEC standards.

In Appendix D, the paper summarizes the key findings of the committees set up to examine recent serious security failings in the public sector. Their recommendations are valuable and as applicable to commercial business as they are to Government departments.

Contents

'The formation of right habits is essential to your permanent security. They diminish your chance of falling when assaulted, and they augment your chance of recovery when overthrown.'

John Tyndall
(1820–1893)
English physicist

1 Introduction

News headlines in recent years have demonstrated the importance to the business of an effective approach to Information Security Management (ISM) by illustrating what can happen in its absence. In the widely publicized case of the loss in transit of Her Majesty's Revenue and Customs (HMRC) child benefit records, it appears they were sent to another public sector body by inappropriate means. Although documented procedures were in place, and would have prevented the incident, staff were not aware of them. Apart from the risk of fraud if the data fell into the wrong hands, and any possible legal infractions that occurred, this episode caused great public and parliamentary concern. It also led to loss of confidence in HMRC and the resignation of the then Chairman, Paul Gray.

In more recent news, data has been lost because it was held on mislaid or stolen laptops or USB memory keys. In some of these cases, the data should never have been transferred to a mobile device. In others, critical data on a mobile device had not been backed up. Some of the lessons learned from these recent public sector security failures will be examined later. The occurence of such incidents points to the need for an integrated approach to ISM, aligned with business risks and needs and involving of course, technical measures, but also policies, procedures and education to ensure that data is treated in an appropriately secure way at all times. There has been a tendency to concentrate on technical approaches such as firewalls, whereas statistics show that human error is at the root of more than half of all security breaches, and technical failures cause less than a tenth.[1] Technical measures are important, but a wider view is needed.

This paper is high-level and discussive rather than deeply technical, although there is some detail in the appendices. The intended audience is business managers and IT Service Providers. The paper describes the need for an appropriate, business-based approach to ISM, and how that relates to standards, certification and best practices, particularly ITIL. It will explore the alignment of ITIL with the wider ISM best practice captured in the ISO ISM standards, indicating ISM areas that are and are not addressed by the published ITIL guidance. ITIL guidance at Version 3 (V3) is relatively stable whilst the ISO ISM standards are proliferating rapidly at the moment, so the paper will also review the standards, taking stock of those published already, and those in the pipeline.

In ITIL today (V3), OGC no longer publishes a separate publication on Security Management as was the case in V2. Because of the existence and growing content of the international standards on Information Security and related guidance, OGC does not consider that the provision of a separate updated ITIL publication on ISM would add value to the wide range of support and guidance material already available. Instead, ISM topics are discussed as they arise in the description of the IT Service Lifecycle throughout the five ITIL core publications, and an ISM process is described in the ITIL *Service Design publication*. This paper seeks to address any alignment issues between ITIL and other specialized guidance on Information Security.

Some scene-setting would be helpful, so Section 2 will contextualize ITIL by describing the functions and roles of standards, best practices and organizational structures and procedures, and the relationships between them.

1 Computing Industry Association Inc (CompTIA) Survey.
Ref. http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=79485

2 Best practices and standards

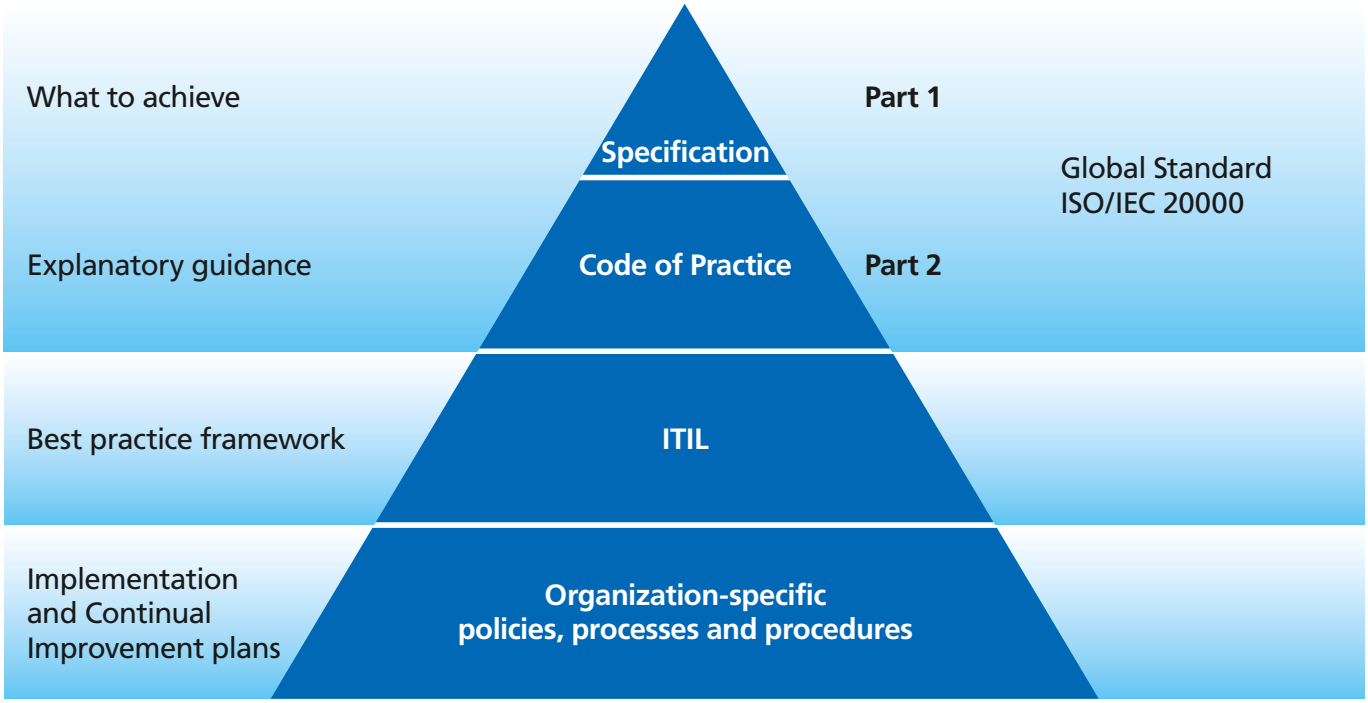


Figure 1 The ITSM standards pyramid

ITIL is a collection of best practice guidance on the management of IT services. It is offered as a comprehensive framework from which organizations, or their agents, can derive a structure within which to design and implement their own procedures. Standards, best practices and implementations have different roles but are related as in the pyramid shown in Figure 1, of which ITIL forms the middle layer.

Standards

At the top, global standards for Information Technology Service Management (ITSM) specify the things we should seek to achieve. Such specifications are often rather terse, but are amplified and clarified by codes of practice and other additional parts of the standard, and together they tell you what you have to do to achieve the targets in the specification.

Organizations can be certificated to show their compliance with the standard.

ITSM Standards

The global IT Service Management standard is ISO/IEC 20000:2005 and this is presently well aligned with ITIL. Two parts have been published: Part 1 (*Specification*) and Part 2 (*Code of Practice*), both of which are currently being revised. Also in development are several new parts, including Part 3 (*Guidance on Compliance: Scoping and Applicability*), Part 4 (*Process Reference Model*), to be followed by Part 5 (*Incremental Conformity Based on ISO/IEC 20000*) and ISO 15504 Part 8 (*An Exemplar Process Assessment Model for IT Service Management*), which will be aligned.

ISM Standards

There is an ever-growing list of global standards in ISM (the ISO/IEC 27000 family). The specification, ISO/IEC 27002, is a renumbering of ISO/IEC 17799, which was based on BS 7799. The detail of the published ISM standards will be discussed in Section 7, and those on development in Appendix C.

For an integrated approach to ITSM as specified by ISO/IEC 20000 and using ITIL, and ISM as specified in ISO/IEC 27000, we are interested in achieving a set of organizational policies, practices and procedures that are compatible with both, as well as with other guidance in other disciplines, such as governance.

Best practices

Best practice products such as ITIL occupy the middle position, and tell you how to do it. ITIL provides a framework of approaches, processes, functions and organizational structures that enable the specification to be met. The ITIL framework has been distilled from the knowledge and experience of IT Service Management professionals globally, and the cyclical updating of ITIL ensures that the guidance describes the best way the authors could discover of accomplishing any particular aspect of ITSM. This is why best practices are so compelling; anybody working alone could not duplicate this effort, and will not discover the best way to approach every aspect of Service Management without reference to best practice.

Individuals can be certified to show their knowledge of ITIL.

Organizational practices

The lowest level of the pyramid is the implementation of IT Service Management best practices, which involves customization and adaptation of the framework to suit the local situation and business needs. This can be done by an internal group, but this role is often supported by outside contractors with experience of implementing IT Service Management best practices in a variety of business contexts. ITIL is written at the most detailed level possible for a generic framework and it is not appropriate to implement without tuning for particular requirements. That is the reason expressions such as 'ITIL-compliant' make little sense, because they suggest there is a formal prescribed implementation.

At the implementation level, *organizations* are encouraged to have their own policies, procedures and structures, and internal training and certification schemes can be created or adopted for individuals to support these internal standards.

Organizational management system

As mentioned earlier, none of these disciplines exist in isolation once they are implemented. In reality, an organization wishes to implement practices and processes from multiple sources in multiple disciplines and soon discovers inconsistencies and clashes between various standards and supporting best practices that they had hoped were complementary. Each major discipline, such as ITSM and ISM, comes with a framework for a management system, with ISO 9000, which provides an overarching approach to the implementation of a quality management system, also in widespread use. Whilst there is much commonality between management systems, there are also differences. In order to overcome the conflicts, avoid duplication and nugatory effort, and ensure focus on business needs, the organization needs a single, consistent management system, necessitating careful selection of elements and processes from various sources to be integrated into it, covering all the areas necessary to support the organization's business interests.

For example, the organization needs to have a single, unified approach to Configuration Management, Change Management, Availability Management, IT Service Continuity Management and Risk Management that meets the needs of both ISM and ITSM (and possibly other areas such as Quality Management). This is a challenge that they will have to meet by creating organizational policy and designing processes to meet their goals. All of these also need to link to business processes. For example, IT Service Continuity Management needs to work with Business Continuity Management, and the same applies to business and IT Change Management, Risk Management, etc.

BSI offers some assistance in PAS 99:2006 *Specification of common management system requirements as a framework for integration*. It is intended for use by organizations who are implementing the requirements of two or more management system standards such as ISO 9001 (Quality), ISO 14001 (Environment), ISO/IEC 27001 (Information Security), ISO/IEC 20000 (IT Service Management) and OHSAS 18001 (Occupational Health and Safety). Like most of the standards it supports, PAS 99 uses the Deming Cycle of Plan-Do-Check-Act. It unifies different standards through six common requirements: Policy, Planning, Implementation and Operation, Performance Assessment, Improvement and Management Review. These elements should be present in recognizable form in any standards or best practice-derived management system and can be regarded as a bedrock for building an organizational management system to integrate elements of management system standards.

3 ISM in business today

Beyond IT

As the communications infrastructure and everyday activities of business have become increasingly dependent on information technology, the security of information in many organizations has been perceived as an IT responsibility. This is perhaps because the growth of IT has provided many new ways for critical business information to be compromised and business managers expect the IT department to manage the new vulnerabilities created. But there is a limit to the protection the IT department can offer without a whole-business approach – the best firewall in the world will not prevent an ignorant employee sending critical data out of the organization. Resources and capabilities outside of IT need to be harnessed in an enterprise-wide ISM structure based on documented procedures and training, as well as technical measures. Information security is everyone's responsibility. Just as IT infrastructure and services enable business activities, effective ISM can also be thought of as an enabler, and it needs to be approached at the business level.

Recommendations

- Security policy, organization and implementation are wider issues than just IT, and should be considered and decided at CEO and Board level, with a Board member having permanent responsibility for all security matters. Authority and support can then flow down to the working level, allowing priorities and funding to be set across the organization based on perceived risk and exposure.
- A best practice-based approach should be taken to ISM implementation, built around people, processes and technology, and aiming to meet the specifications of ISO/IEC 27002.

Drivers for improvement

Other pressures today, many of which concern good governance, indicate that Information Security is a business-wide issue. In the area of compliance with legislation, organizations have responsibilities to meet many different legal requirements, including auditably sound financial practices, data protection and protection of national security. Failure to do so may have serious consequences for Board members, apart from loss of confidence of customers, partners and shareholders. Customers are likely to be less immediately aware of bad ISM practices, but although they may not have a name for it, both customers and investors will be discouraged by evidently poor ISM, brought to their attention by negative publicity. Customers will not be tolerant of an organization that demonstrates poor custody of its information assets, for example, by losing their personal data or permitting fraud or identity theft, and neither will investors seek to invest in an organization with visibly bad ISM. Repeated incidents will result in a boardroom coup, if not the demise of the organization.

Be positive

There is a danger that all these negative messages about dire consequences of the absence of effective ISM reinforce the view that money spent on it is just an overhead that prevents things going wrong in the IT department which could affect the business. If we take to heart ITIL's message that a service is something that delivers business value by improving customer outcomes[2], we should be seeking to position ISM as a business activity that directly contributes towards the delivery of enhanced business value to customers.

The way forward

The Information Security Manager should appreciate the broader business aspects of the organization, and understand its structure, its culture and its business propositions. Then the manager can concentrate and prioritize ISM activities in the way that is most supportive of the organization's business activities. Such a business analysis will support the Information Security risk analysis by, for example, bringing an understanding of the role played by suppliers and partners. and will provide a suitable context in which to consider the measures that must be in place to protect the organization's information assets whilst permitting effective communication in support of business – i.e. reducing the risk. A sound knowledge of the business and the organization is vital to support the customization of the best practice guidance in an appropriate and effective implementation that will 'take' in that particular environment, culture, business and organizational structure. Information Security Managers need to be aware of the lifecycle of organizational information assets and future plans

2 A 'Service' is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. *Service Strategy*, London: TSO 2007.

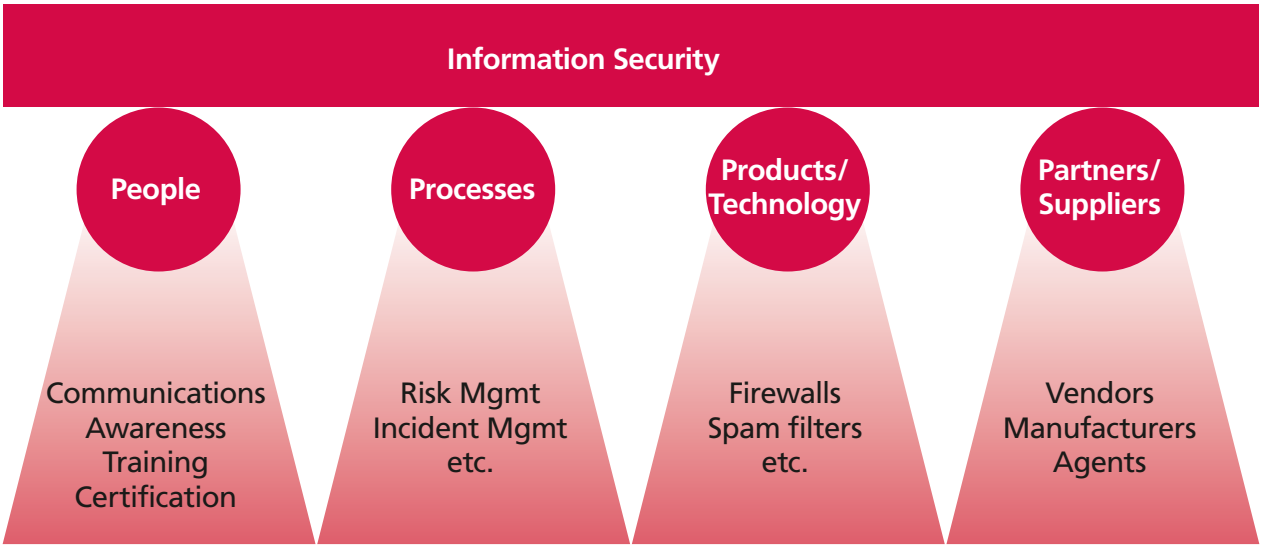


Figure 2 Achieving effective Information Security Management through the four Ps

and business ventures being considered, in order to ensure the risks are assessed and appropriately mitigated at every stage of that lifecycle. The other business functions in an organization will expect this to be done effectively, seamlessly and invisibly, and without being subjected to arcane technical jargon. The more successfully this is done, the more likely it is that the ISM function will be accepted as a valid partner in delivering value for the business.

An ISM policy and an Information Security Management System (ISMS) should be developed to ensure that information is protected at all stages of all business processes. A useful perspective that divides up the scope might be the ITIL 'four Ps of Service Design' shown in Figure 2.

Whilst all the internal Information Security risks may come readily to mind, it is possible to underestimate the security risks arising from organizational or personal information held, used or conveyed by partners. Here, a 'partner' is any other entity in the value network, including the customer. Similarly, information accessed by partners on the organization's premises or IT systems needs to be safeguarded. There will also be a need to safeguard partners' and individuals' data whilst in the organization's custody.

To arrive at a coherent and effective set of ISM practices, an organization should follow these steps:

- Produce, maintain, distribute and enforce an Information Security Policy, supported by specific policies
- Understand the current business security policy and plans
- Understand and agree current and future business security requirements
- Implement security controls that support the Information Security Policy and manage risks associated with access to services, information and systems
- Document all security controls and their operation, maintenance and associated risks
- Manage suppliers and contracts in respect of access to systems and services, in conjunction with the Supplier Management function
- Manage all security breaches and incidents
- Proactively improve security controls and security risk management
- Ensure security aspects are integrated into all other ITSM processes.

The creation of an effective ISMS follows the Plan-Do-Check-Act cycle. In this case, ITIL describes a cycle with the following steps: Control, Plan, Implement, Evaluate and Maintain (see Figure 3).

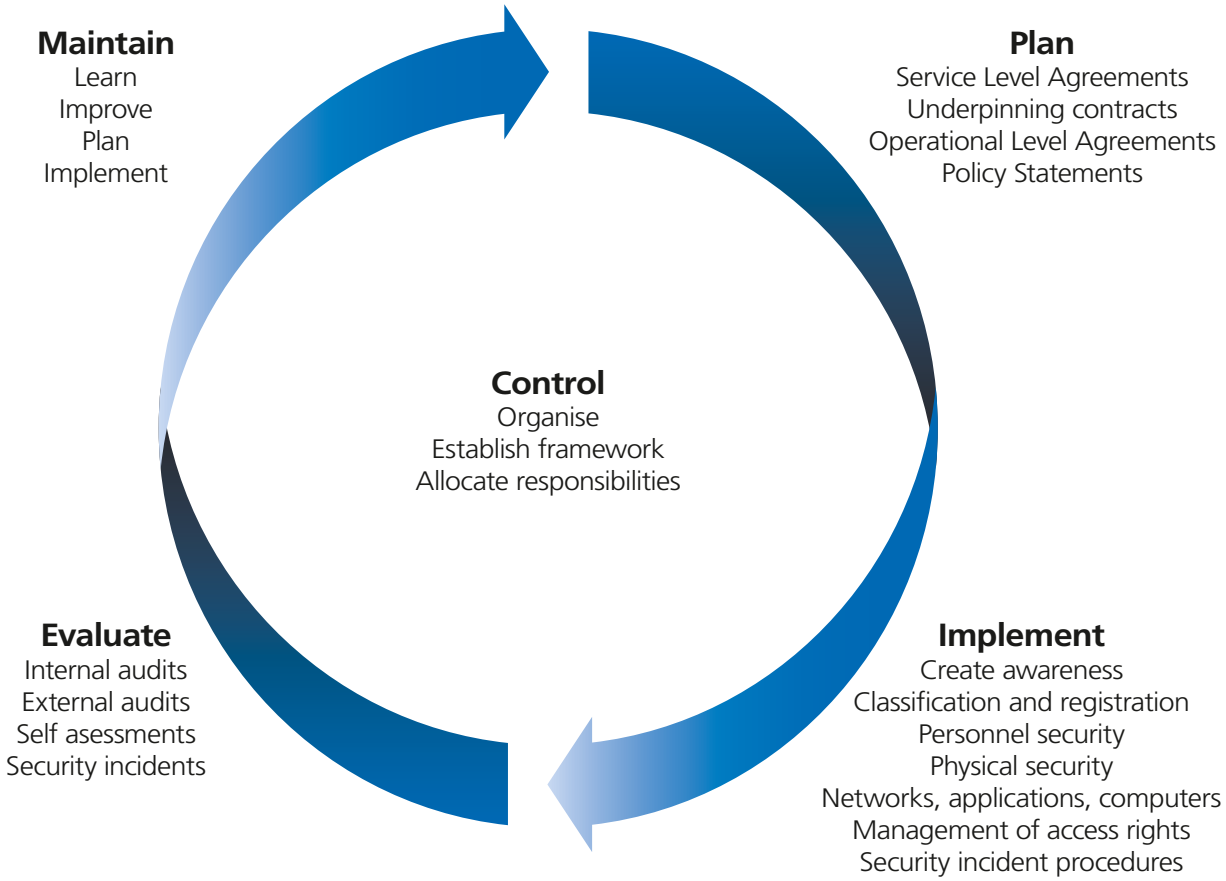


Figure 3 Framework for an Information Security Management System

4 The wider security context

With all this discussion, it is possible to forget that information is a single class of organizational asset and Information Security is one aspect of an overall security strategy. However, the response to all security threats should be proportionate, and it is likely that Information Security will be one of the larger security concerns in an organization today.

Security

But what is generic 'security'? Generally it refers to protection against loss or danger or any outside threat that would have a detrimental effect on people, infrastructure, goods, activities or goals. Setting aside national security (threats to your country, its critical national infrastructure or citizens from terrorism, weapons of mass destruction, etc.), the security concerns of an organization might include the following:

- **Financial:** e.g. fraud or theft, but also good governance, compliance, accountability and audit
- **Industrial:** e.g. protection of assets (including paper records and electronic assets) from espionage, theft, sabotage; security of supply (materials, energy), second sourcing; secure transport of assets, staff or customers
- **Premises:** e.g. access controls, secure stores, surveillance, intruder detection;outsourced facilities management
- **Individual:** e.g. protection of customers, staff, partners and suppliers from hazardous substances or environments; safety and welfare in the workplace (see below); freedom from discrimination, intimidation and bullying; immunity from legal action when acting on behalf of the company, etc.
- **Educational:** e.g. awareness programmes, regular communications, training, drills.

Business Continuity

Threats to Business Continuity that are considered as part of a Business Impact Analysis (BIA) usually include storm, fire and flood, and perhaps today, terrorism. Such a scope is a legacy of the days when Business Continuity went little further than disaster planning. However, planning for Business Continuity3 should cover every foreseen occurrence that might affect future business, and many of these are not disaster-related. Examples might be poor financial management, failures of legislative compliance, loss of expert staff, single-sourcing of raw materials, product safety issues, reputational risks and failures of investor confidence.

Equally important are loss of data or voice networks or servers. ISM, ITSCM and IT Security Management have key roles to play in support of business continuity by assuring the continuing availability of the IT and telecoms infrastructure, safeguarding of critical information and continuing provision of business-critical IT services.

Safety

There are some boundary issues between an organization's security officer and its safety officer. Being safe is a legitimate part of being secure, but often safety officers will be observing compliance with safety legislation such as the Health and Safety at Work Act 1974, which regulates health, safety and welfare in the workplace, and has a wide scope. They may also undertake safety risk assessments, safety procedure rehearsals (e.g. fire drills) and safety incident investigations.

3 See BS 25999.

5 Key ISM concepts

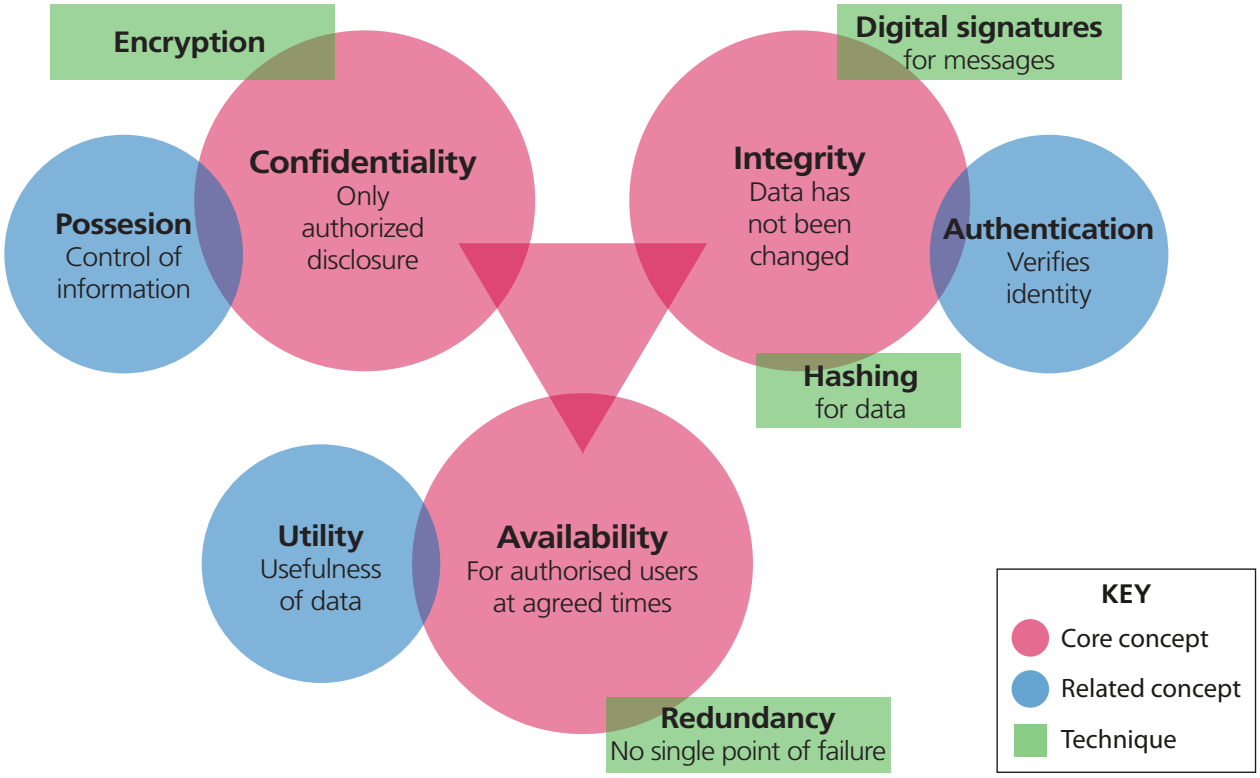


Figure 4 Core and secondary Information Security concepts

Readers will have noticed that earlier ITIL guidance talked about IT security whereas today we focus on Information Security Management, which seeks to protect information in whatever form. Of course, the security of IT systems and procedures plays a huge role in ISM. There are a few terms that should be clarified (see also Figure 4):

Information assurance is the management of all risks concerning information. This involves identifying and taking protective measures to address the basic 'CIA' triad of concerns in respect of information and information-handling systems: Confidentiality, Integrity and Availability, although in practice there are other related concerns. It also includes planning and setting up of measures to monitor, detect and react to Information Security breaches, and to restore information and information systems when required.

Information Security is the active protection of information, however stored or conveyed, to ensure it is available only to authorized users at the time they require it, with appropriate levels of integrity. This is normally achieved through an Information Security Management system (ISMS).

IT security or **computer security** is the management of the security of information held or conveyed by computers and networks. Organizational policy will define the exact measures and structures necessary to meet organizational business needs, and the security policy will result from the risk analyses conducted as part of the information assurance activities.

Confidentiality is the assurance that only intended and authorized recipients or systems have access to information. Examples of breaches of confidentiality include reading someone else's mail, examining rubbish for information content and writing down a password. A very public example of unauthorized disclosure occurred in May 2008 when in an embarrassing incident for the Government, the then Housing Minister Caroline Flint was photographed holding a briefing document on the UK housing market. The photograph was detailed enough for the text to be read, revealing Government concerns that would not otherwise have been made public. See http://www.timesonline.co.uk/tol/news/politics/article3923351.ece.

Integrity is the assurance that information has not been changed or modified in storage or transmission except by authorized persons or processes. It covers any form of unauthorized change, deliberate or otherwise. An example might be modification of data stored on a computer by the action of a computer virus.

Availability is the assurance that information is available to authorized users or systems at the times they are authorized to access it. An example of a security failure concerning availability might be the prevention of authorized persons accessing corporate data because of an internet-based denial of service (DOS) attack. Another might be the inability to run a payroll program because of accidental deletion of a staff data file.

Authenticity means assuring that transactions and contracts, information and communications are genuine and that the identities of persons or systems accessing the information, or taking part in communications or transactions are known and verified. An example is identity theft where one individual misrepresents himself as another, usually for fraudulent financial gain.

Non-repudiation in the wider world means that legal contracts, once agreed, cannot be undone by the parties to the contract or anyone else. In an Information Security context, it means that the parties to any form of agreement, or any third parties, cannot change it or deny having entered into it later. In the conveyance of data, it means that the recipient has proof of the identity of the sender and the sender has proof of delivery to the recipient. For example, non-repudiation of the sending of emails can be supported by messaging systems that timestamp the message and sign it with the sender's unique digital signature. This makes it extremely difficult for the sender to later deny sending the email, or claim it was sent at a different time.

Risk Management is a coordinated set of activities to identify and assess security vulnerabilities and put in place countermeasures (controls) to reduce the residual risk to the level agreed in the security policy which has been designed to meet the organization's business needs.

Some security experts have identified additional concepts[4] such as possession and utility. An example of possession might be the theft of a laptop containing encrypted data. The data has not been compromised and no unauthorized disclosure has taken place, but it possibly could be in future, and the organization no longer has sole possession of the data. If the stolen laptop held the only copy of the data, this could be a serious incident.

If all copies of an encrypted database remain in the possession of authorized users, but for any reason the database cannot be decrypted for authorized use, then the data is available, but not in an immediately usable form. Another example is the receipt of a file in a proprietary format not recognized by any of the recipient's computer applications. No unauthorized disclosure has taken place, but this is a failure of utility as the data is available, but not usable.

Example

To show that these concepts are primarily related to information itself rather than IT systems, let us consider the example of a medieval king who sends a messenger with new battle plans to a commander elsewhere in the field of battle. He will have written a message on a scroll of paper rolled and sealed with wax and impressed with his seal. If the commander receives the scroll and the seal has not been disturbed, he can be reasonably assured about the *confidentiality* and the integrity of the information. *Confidentiality* would be further enhanced by the use of a cipher, or code. *Availability* depends on the messenger getting the scroll to the commander at the appropriate time for the information to be useful. *Authenticity* implies the recipient can be assured that the messenger is genuine and has a genuine message from the king. Again, here the seal helps. The messenger also needs to be sure he is delivering to the correct person, and one fears the messenger might have difficulty insisting the commander prove his identity.

4 *Fighting Computer Crime: A New Framework for Protecting Information*, Donn B. Parker, Wiley, 1998.

6 ITIL and the ITSM and ISM standards

The scope, functionality and interaction of ITIL and the ISM standards are explored in this section. Their areas of overlap are explored after a brief description of each.

ITIL

ITIL is a framework of best practice guidance in Information Technology Service Management (ITSM). It describes processes, functions and structures that support most areas of IT Service Management, mostly from the viewpoint of the Service Provider. One of the many processes it describes is Information Security Management (ISM). ITIL can be adapted and applied to suit the circumstances of a particular provider, customer or implementation, depending on various factors such as size, culture, existing management systems, organizational structure and the nature of the business. ITIL is not prescriptive and because of the necessary implementation tuning, there is no rigidity of application that would indicate that tests of compliance are appropriate.

ITSM standards

The international standard for ITSM is ISO/IEC 20000, which has a number of parts. Part 1 provides a specification against which Service Providers may be certified.

Although the standard and ITIL have some differences in coverage in the field of ITSM, ITIL does generally provide the how? to the what? given in the certifiable specifications provided in ISO/IEC 20000 part 1. Of course, Service Providers using ITIL are not obliged to seek ISO certification, and the ITIL framework is sufficient to permit the design of a structure with policies and processes to manage IT services effectively. However, Service Providers should consider certification, as this will give customers confidence in the provider's competence, and increasingly, customers are mandating in their procurements that their IT Service Providers should have certification to demonstrate their compliance to ISO/IEC 20000.

ISM standards

There are four published Information Security Management standards in the ISO/IEC 27000 family:

- 27001:2005 *Information Security Management Systems – Requirements*
- 27002:2005 *Code of Practice for Information Security Management*
- 27005:2008 *Information Security Risk Management*
- 27006:2007 *Requirements for Bodies Providing Audit and Certification of Information Security Management Systems*
- Plus ISO/IEC 27799:2008 *Health Informatics – Information Security Management in Health Using ISO/IEC 27002*, which is particularly aimed at one industry sector.

There are many more in preparation:

- 27000 Introduction with principles, concepts and vocabulary
- 27003 Implementation guidance for 27001 and 2
- 27004 Measurement and metrics for ISM
- 27007 Guidance to auditors of Information Security Management Systems against the specification in ISO/IEC 27001
- 27008 (Technical report) Guidance for auditors on ISMS controls
- 27010 ISM issues in interorganizational and international communications
- 27011 ISMS implementation guide for the telecommunications industry
- 27031 ICT readiness for Business Continuity (role of IT and telecoms)
- 27032 Cybersecurity. Expected to be guidance to ISPs and other internet users
- 27033 Network security. Seven parts currently planned (updates 18028 part 1)
- 27034 Information security for IT applications.

27001 and 27002 are the key documents here, but evidently, the new standards will cover more aspects and perspectives than just a specification and code of practice. The coverage of the published standards is described in Section 7, and the unpublished ones in Appendix C.

The relationship between these standards and ITIL is visualized in Figure 5. Parts of ISO/IEC 20000 (IT Service Management) are also shown for completeness.

Appendix B provides a table showing mapping of ISM topics between ITIL and ISO/IEC 27001 and 27002.

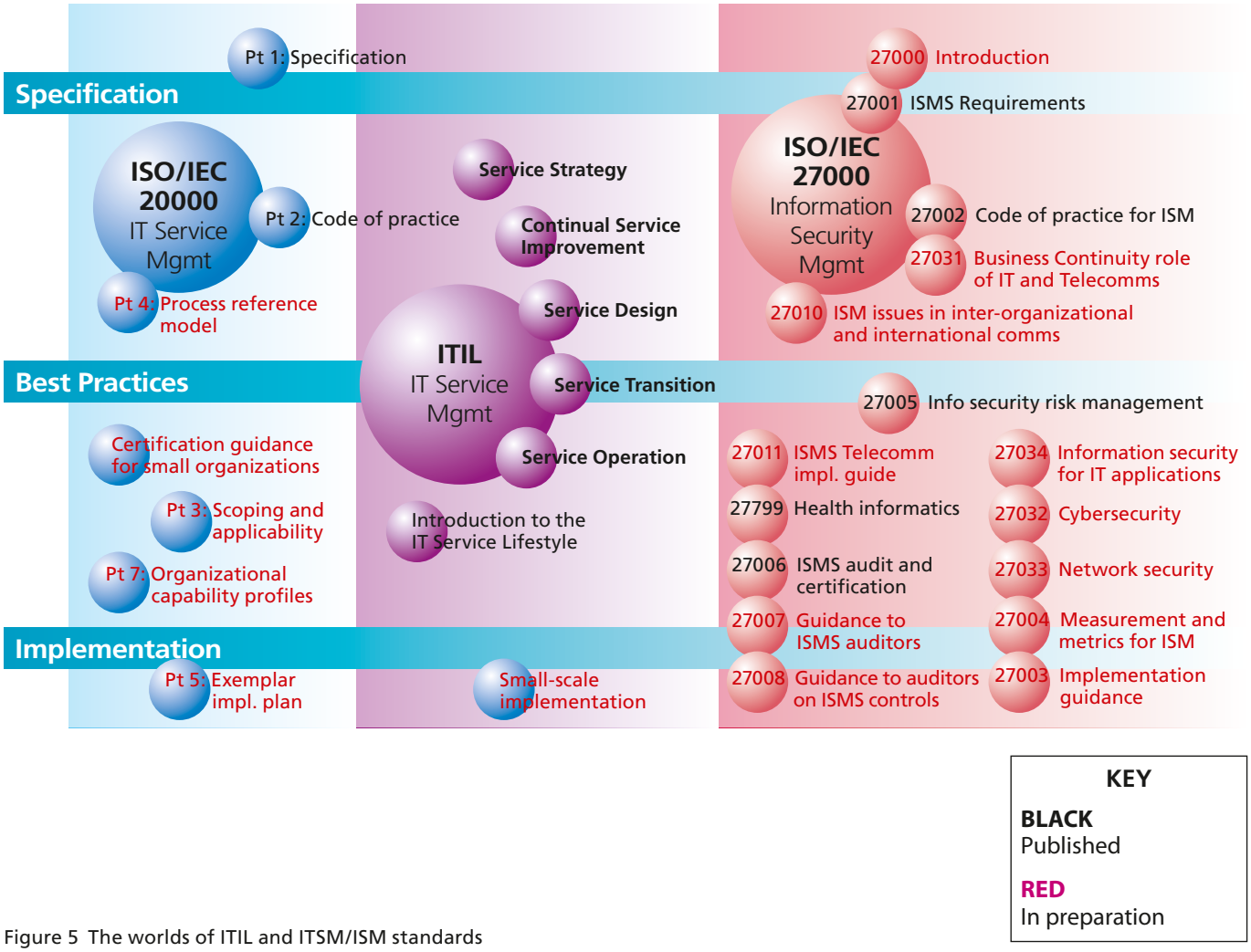


Figure 5 The worlds of ITIL and ITSM/ISM standards

7 ISM according to ITIL

in ITIL, ISM is defined in a pleasingly positive way as...

> *... the Process that ensures the Confidentiality, Integrity and Availability of an organization's Assets, information, data and IT Services. Information Security Management usually forms part of an organizational approach to Security Management that has a wider scope than the IT Service Provider, and includes handling of paper, building access, phone calls, etc., for the entire organization.*

ITIL Glossary[5]

The main reference for ISM in ITIL is in the *Service Design* publication, Section 4.6, but it is also mentioned in context throughout the Service Lifecycle. Here is a reference list of the location of the ISM topics within the ITIL core publications:

Service Strategy
(only mentions ISM in passing)

Service Design

- 4.4.5.2 The proactive activities of Availability Management
- 4.5.5 ITSCM Process activities, methods and techniques (ITSCM initiation and risk analysis)
- 4.5.6 Triggers, inputs, outputs and interfaces (interfaces and integration with ITSCM)

- 4.6 Information Security Management (main reference)
  - 4.6.1 Purpose/goal/objective
  - 4.6.2 Scope
  - 4.6.3 Value to the business
  - 4.6.4 Policies/principles/basic concepts
    - 4.6.4.1 Security framework
    - 4.6.4.2 The Information Security Policy
    - 4.6.4.3 The Information Security Management System (ISMS)
  - 4.6.5 Process activities, methods and techniques
    - 4.6.5.1 Security controls
    - 4.6.5.2 Management of security breaches and incidents
  - 4.6.6 Triggers, inputs, outputs and interfaces
    - 4.6.6.1 Inputs
    - 4.6.6.2 Outputs
  - 4.6.7 Key Performance Indicators
  - 4.6.8 Information Management
  - 4.6.9 Challenges, Critical Success Factors and risks
- 4.7 ISM issues in Supplier Management

Service Transition

- 4.4.9 Release and Deployment risks
- 5.3.2 Stakeholder Management

Service Operation

- 4.2.4.2 Incident Models

- 4.5 Access Management
  - 4.5.1 Purpose/goal/objective
  - 4.5.2 Scope
  - 4.5.3 Value to business
  - 4.5.4 Policies/principles/basic concepts
  - 4.5.5 Process activities, methods and techniques
    - 4.5.5.1 Requesting access
    - 4.5.5.2 Verification
    - 4.5.5.3 Providing rights
    - 4.5.5.4 Monitoring identify status
    - 4.5.5.5 Logging and tracking access
    - 4.5.5.6 Removing or restricting rights
  - 4.656 Triggers, inputs, outputs and interfaces

5 ITIL Glossaries/Acronyms © Crown Copyright Office of Government Commerce. Reproduced with the permission of the Controller of HMSO and the Office of Government Commerce.

  - 4.5.7 Information Management
    - 4.5.7.1 Identity
    - 4.5.7.2 Users, groups, roles and service groups
  - 4.5.8 Metrics
  - 4.5.9 Challenges, Critical Success Factors and risks
- 5.5 Network Management
  - 5.11 Internet/Web Management responsibilities
  - 5.13 Information Security Management and Service Operation (role of Service Operation)
- 6.1 Service Operation functions
  - 6.6.9 Access Management roles
- Appendix F: Physical Access Control

Continual Service Improvement

  - 3.11.3 Standards

8 The 27000 series family of standards

At the time the previous version of ITIL was written (V2, in 1999) the only ISM standard was BS 7799:1999 and thus CCTA (now OGC) thought it useful to produce an ITIL publication to describe best practices for ISM. Since then, BS 7799 part 1 has become ISO/IEC 17799:2000 (Code of practice for Information Security Management) and was revised in 2005. After it became clear that a whole family of ISM standards would be produced, a new numbering system was chosen, and ISO/IEC 17799:2005 was renamed ISO/IEC 27002:2005. BS7799 part 2 (2002) became ISO/IEC 27001.

Commonly known as the 27k family, the new range of standards is intended to provide all the information necessary to plan, implement and operate a certifiable Information Security Management System (ISMS). Parts of the family were inherited from earlier standards, as mentioned above. Other parts will align with, consolidate or draw from further existing standards.

Ownership of 27k standards development lies with ISO/IEC JTC1/SC27. JTC1 is the ISO/IEC Joint Technical Committee on Information Technology, established in 1987. Sub-committee (SC) 27 works on IT Security techniques. It has five working groups looking at various aspects of ISM. More detail can be found at http://www.iso.org.

This section provides details of the published standards in the 27k family and Appendix C describes those in preparation.

ISO/IEC 27001:2005 *Information Security Management* Systems – Requirements

This is the top-level specification and certification standard for effective ISM for all types of organizations.

It covers:

- Definitions of terms
- General requirements
- Establishing and managing
- Implementing and operating
- Monitoring and reviewing
- Maintaining and improving
- Documentation requirements
- Document and record controls
- Management responsibility and commitment
- Resource provision and management
- Training awareness and competence
- Internal audits
- Management reviews
- Continual improvement.

There are also mappings to OECD principles, ISO 9001 and ISO 14001 for organizations that already have management systems based on these standards.

ISO/IEC 27002:2005 *Code of Practice for Information Security Management*

This is the code of practice that outlines what it is necessary to do in order to meet the specification.

It was created in 2007 by renumbering ISO/IEC 17799:2005 to bring it into the 27k family. Note that this version is a considerable revision of the first version of ISO/IEC 17799 in 2000, which had been based on BS 7799. The 2005 revisions included improved guidance on risk and incident management and a clearer structure.

The standard outlines a set of controls in each area of ISM and then gives implementation guidance on the way the control objectives can be met. The intention is that these controls are applied against risks identified through a risk assessment.

The areas covered include:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operational management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance.

ISO/IEC 27005:2008 *Information Security Risk Management*

This standard provides guidance on Information Security Risk Management in all types of organizations.

It builds on the concepts in ISO/IEC 27001 and 27002, involving the design of an Information Security Management System based on an Information Security risk assessment.

It replaces ISO/IEC TR 13335-3:1998 and TR 13335-4:2000, which have been withdrawn.

ISO/IEC 27006:2007 *Requirements for Bodies Providing Audit and Certification of Information Security Management Systems*

Part 6 of the 27k family offers guidelines for accreditation of those organizations that offer ISMS certification against ISO/IEC 27001.

The requirements of this standard apply in addition to those of ISO/IEC 17021:2006 (Conformity assessment – Requirements for bodies providing audit and certification of management systems). Part 6 describes the additional accreditation requirements that apply to bodies offering Information Security Management certification.

Part 6 incorporates and effectively replaces guidance from the EA (European Cooperation for Accreditation) in EA 7/03 (http://www.european-accreditation.org/n1/doc/EA-7-03.pdf).

ISO/IEC 27799:2008 *Health Informatics – Information Security Management in Health Using ISO/IEC 27002*

This standard details controls for managing health Information Security and provides best practice guidelines.

Compliance with this standard will ensure a minimum requisite level of security appropriate to an organization's circumstances that will maintain the confidentiality, integrity and availability of personal health information.

ISO 27799 applies to health information in all its aspects on any media (words and numbers, sound recordings, drawings, video and medical images), whatever the means of storage (printed or written paper or electronic storage) and whatever the means of transmission (by hand, fax, computer network or post), ensuring the information is always appropriately protected and the lifecycle of the information is fully auditable.

ISO 27799 has been developed by a different group than the other 27k standards (TC215 Health Informatics in this case) and defines guidelines to support the interpretation and implementation of ISO/IEC 27002 in the field of health informatics, which is regarded as a special environment with special requirements, for example, to protect patient privacy and safety.

9 ITIL, ISM and standards working together

ISM is a process and a function in ITIL. Awareness and consideration of security risks and issues are background obligations for every step of successful IT Service Management under ITIL. The ISO/IEC ISM standards and the great volume of supporting guidance provide a much deeper consideration of all the elements, including policies, processes, measurements, improvements, necessary for the creation of an effective ISMS and a successful ISM implementation. Many ISM issues are not explored in depth in ITIL, but please refer to Appendix B, which shows the links between topics in the ITIL publications and in the ISO/IEC standards.

Appendix A: Abbreviation list and glossary

Abbreviation list

BS	British Standard
CEO	Chief Executive Officer
CSI	*Continual Service Improvement* (ITIL publication)
HMRC	Her Majesty's Revenue and Customs (UK Government department)
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
ISM	Information Security Management
ISMS	Information Security Management System
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
ITIL	Best practice guidance on IT Service Management from OGC (formerly IT Infrastructure Library). Originally published 1989 – 1998 (informally called Version 1) Revised 2000 – 2004, (Version 2) Revised 2007 (Version 3)
ITSCM	IT Service Continuity Management
ITSM	IT Service Management
ITU	International Telecommunications Union (United Nations)
OECD	Organization for Economic Cooperation and Development
OGC	(UK) Office of Government Commerce
OLA	Operational Level Agreement
SD	*Service Design* (ITIL publication)
SLA	Service Level Agreement
SO	*Service Operation* (ITIL publication)
SS	*Service Strategy* (ITIL publication)
ST	*Service Transition* (ITIL publication)
TR	Technical Report
USB	Universal Serial Bus (connection standard for computers)

Glossary of key terms in ISM[6]

TERM	INFORMAL DEFINITION	ITIL DEFINITION
Asset	Anything of value to an organization.	(*Service Strategy*) Any Resource or Capability. Assets of a Service Provider include anything that could contribute to the delivery of a Service. (abbreviated)
Authenticity	The assurance that transactions and contracts, information and communications are genuine and that the identities of persons or systems accessing the information, or taking part in communications or transactions are known and verified.	
Availability	The assurance that information is available to authorized users or systems at the times they are authorized to access it.	(*Service Design*) Ability of a Configuration Item or IT Service to perform its agreed Function when required. Availability is determined by Reliability, Maintainability, Serviceability, Performance, and Security. Availability is usually calculated as a percentage.
Confident-iality	The assurance that only intended and authorized recipients or systems have access to information.	(*Service Design*) A security principle that requires that data should only be accessed by authorized people.
Control	(Or Countermeasure). A means of managing a risk.	A means of managing a Risk, ensuring that a Business Objective is achieved, or ensuring that a Process is followed. Example Controls include Policies, Procedures, Roles, RAID, door-locks etc. A control is sometimes called a Countermeasure or safeguard. Control also means to manage the utilization or behaviour of a Configuration Item, System or IT Service.
Guideline	Practical advice on achieving policy objectives.	A document describing best practice, that recommends what should be done. Compliance to a guideline is not normally enforced. See Standard.
Information Security	Preservation of Confidentiality, Integrity and Availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation and Reliability can also be involved.	
Information Security Event	Any observed state of information, storage or processing systems or information conveyance means, that might indicate that a breach of Information Security may have occurred.	
Information Security Incident	One or more Information Security Events that threaten Information Security and Business Operations.	

6 ITIL Glossaries/Acronyms © Crown Copyright Office of Government Commerce. Reproduced with the permission of the Controller of HMSO and the Office of Government Commerce.

TERM	INFORMAL DEFINITION	ITIL DEFINITION
Information Security Management (ISM)	An organization-wide process to reduce Information Security risks to an acceptable level.	(*Service Design*) The Process that ensures the Confidentiality, Integrity and Availability of an organization's Assets, information, data and IT Services. Information Security Management usually forms part of an organizational approach to Security Management which has a wider scope than the IT Service Provider, and includes handling of paper, building access, phone calls etc., for the entire organization.
Information Security Management System (ISMS)	The processes, functions and structure that form part of the Management System, that ensures that that organizational Information Security Risks are managed in accordance with agreed policies.	(*Service Design*) The framework of Policy, Processes, Standards, Guidelines and tools that ensures an organization can achieve its Information Security Management Objectives.
Information Security Policy	The policy that enables an organization to meet its agreed goals for Information Security Management by defining the agreed scope and approach.	(*Service Design*) The Policy that governs the organization's approach to Information Security Management.
Integrity	The assurance that information has not been changed or modified in storage or transmission except by authorized persons or processes.	(Service Design) A security principle that ensures data and Configuration Items are only modified by authorized personnel and Activities. Integrity considers all possible causes of modification, including software and hardware Failure, environmental Events, and human intervention.
Non-repudiation	The assurance that the parties to any form of agreement, or any third parties, cannot maliciously change it later. In the conveyance of data, it means that the recipient has proof of the identity of the sender and the sender has proof of delivery to the recipient.	
Policy	A formal statement of intent and direction.	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of Processes, Standards, Roles, Activities, IT Infrastructure, etc.
Residual Risk	The Risk remaining after Risk Management measures have been taken.	
Risk	Uncertainty in an event that might affect the achievement of objectives. A Risk may be a Threat or an opportunity. The magnitude of a Threat depends on the probability of its occurrence, the Vulnerability of the organization to the threat and the impact if it were to happen.	A possible Event that could cause harm or loss, or affect the ability to achieve Objectives. A Risk is measured by the probability of a Threat, the Vulnerability of the Asset to that Threat, and the Impact it would have if it occurred.
Risk Assessment	Risk analysis and evaluation.	The initial steps of Risk Management. Analysing the value of Assets to the business, identifying Threats to those Assets, and evaluating how Vulnerable each Asset is to those Threats. Risk Assessment can be quantitative (based on numerical data) or qualitative.
Risk evaluation	Estimation of the significance of a risk.	

TERM	INFORMAL DEFINITION	ITIL DEFINITION
Risk Management	A coordinated set of activities to identify and assess security Vulnerabilities and put in place Countermeasures (controls) to reduce the residual Risk to the level agreed in the Security Policy.	The Process responsible for identifying, assessing and controlling Risks. See Risk Assessment.
Risk treatment	Application of measures to control Risk.	
Third party	A person or organization that is outside of an agreement between two parties, but may have an interest.	A person, group, or Business who is not part of the Service Level Agreement for an IT Service, but is required to ensure successful delivery of that IT Service. (abbreviated)
Threat	A type of Risk that if a Vulnerability exists, may cause an Incident that prevents organizational objectives from being met.	Anything that might exploit a Vulnerability. Any potential cause of an Incident can be considered to be a Threat. For example, a fire is a Threat that could exploit the Vulnerability of flammable floor coverings. (abbreviated)
Vulnerability	A weakness that may be exploited by a Threat.	A weakness that could be exploited by a Threat. For example, an open firewall port, a password that is never changed, or a flammable carpet. A missing Control is also considered to be a Vulnerability.

Appendix B: Mapping ITIL to ISO/IEC ISM primary standards

The following tables show a cross-reference between ISM topics in the two primary standards (ISO/IEC 27001 and 27002) and ITIL.

Note: The ITIL publication titles are abbreviated as in the list of acronyms above.

ISO/IEC 27001	ITIL	
4.1 [ISMS] General requirements	SD	4.6.4.1 Security framework
4.2 Establishing and managing the ISMS 4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS 4.2.3 Monitor and review the ISMS 4.2.4 Maintain and improve the ISMS	SD	4.6.4.3 The Information Security Management System (ISMS)
4.3 Documentation requirements 4.3.1 General 4.3.2 Control of documents 4.3.3 Control of records	SD	4.6.6.2 [ISM] Outputs 4.6.8 [ISM] Information Management
5 Management responsibility 5.1 Management commitment 5.2 Resource management 5.2.1 Provision of resources 5.2.2 Training, awareness and competence		
6 Internal ISMS audits		
7 Management review of the ISMS 7.1 General 7.2 Review input 7.3 Review output		
8 ISMS improvement 8.1 Continual improvement 8.2 Corrective action 8.3 Preventive action		

ISO/IEC 27002	ITIL	
0.1 WHAT IS INFORMATION SECURITY?	SD	4.6.1 Purpose/goal/objective
0.2 WHY IS INFORMATION SECURITY NEEDED?	SD	4.6.3 Value to the business
0.3 HOW TO ESTABLISH SECURITY REQUIREMENTS	SD	4.6.6.1 Inputs
0.4 ASSESSING SECURITY RISKS	SD	4.6.4.3 The Information Security Management System (ISMS)
0.5 SELECTING CONTROLS	SD	4.6.5.1 Security controls
0.6 INFORMATION SECURITY STARTING POINT	SD	4.6.5 Process activities, methods and techniques
0.7 CRITICAL SUCCESS FACTORS	SD	4.6.9 Challenges, Critical Success Factors and risks
0.8 DEVELOPING YOUR OWN GUIDELINES		
1 SCOPE	SD	4.6.2 Scope
2 TERMS AND DEFINITIONS		ITIL Glossary
4 RISK ASSESSMENT AND TREATMENT 4.1 ASSESSING SECURITY RISKS	SD	4.5.5 ITSCM Process activities, methods and techniques (ITSCM initiation and risk analysis)
4.2 TREATING SECURITY RISKS	SO	8.3 ASSESSING AND MANAGING RISK IN SERVICE OPERATION
5 SECURITY POLICY	SD	3.5 Design activities
5.1 INFORMATION SECURITY POLICY	SD	4.6.4.2 The Information Security Policy
6.1 INTERNAL ORGANIZATION [OF INFORMATION SECURITY]	SD	4.6.4.1 Security framework
6.1.1 Management commitment to Information Security	SD	4.6.9 Challenges, Critical Success Factors and risks
6.1.2 Information security coordination 6.1.3 Allocation of Information Security responsibilities 6.1.4 Authorization process for information processing facilities 6.1.5 Confidentiality agreements 6.1.6 Contact with authorities 6.1.7 Contact with special interest groups 6.1.8 Independent review of Information Security	SD	4.6.4.3 The Information Security Management System (ISMS)
6.2 EXTERNAL PARTIES	SD	4.7.5.1 ISM issues in Supplier Management
6.2.1 Identification of risks related to external parties	SD	4.6.6.2 Outputs
6.2.2 Addressing security when dealing with customers		
6.2.3 Addressing security in third-party agreements	SD	Appendix F: Sample SLA and OLA
7 ASSET MANAGEMENT	ST	4.3 Service Asset and Configuration Management
7.1 RESPONSIBILITY FOR ASSETS	ST	4.3 Service Asset and Configuration Management
7.1.1 Inventory of assets	ST	4.3.4.3 Configuration Management System
	ST	Appendix A: Description of asset types
7.1.2 Ownership of assets	ST	4.3.5.3 Configuration identification
7.1.3 Acceptable use of assets	ST	4.3.4.1 Service Asset and Configuration Management policies
7.2 INFORMATION CLASSIFICATION	SD	4.6.4.3 The Information Security Management System (ISMS)

ISO/IEC 27002	ITIL	
8 HUMAN RESOURCES SECURITY		
8.1 PRIOR TO EMPLOYMENT 8.1.1 Roles and responsibilities 8.1.2 Screening 8.1.3 Terms and conditions of employment	SO	5.13.4 Screening and vetting
8.2 DURING EMPLOYMENT 8.2.1 Management responsibilities 8.2.2 Information security awareness, education, and training 8.2.3 Disciplinary process	SO	5.13.5 Training and awareness
8.3 TERMINATION OR CHANGE OF EMPLOYMENT		
8.3.1 Termination responsibilities		
8.3.2 Return of assets		
8.3.3 Removal of access rights		
9 PHYSICAL AND ENVIRONMENTAL SECURITY		
9.1 SECURE AREAS		
9.1.1 Physical security perimeter		
9.1.2 Physical entry controls 9.1.3 Securing offices, rooms, and facilities	SO	Appendix F: Physical Access Control
9.1.4 Protecting against external and environmental threats		
9.1.5 Working in secure areas	SO	5.13.3 Operational security control
9.1.6 Public access, delivery, and loading areas	SO	5.13.3 Operational security control E7 Shipping and receiving
9.2 EQUIPMENT SECURITY		
9.2.1 Equipment siting and protection	SO	5.12 FACILITIES AND DATA CENTRE
9.2.2 Supporting utilities		
9.2.3 Cabling security		
9.2.4 Equipment maintenance		
9.2.5 Security of equipment off-premises	SD	4.6.4.3 The Information Security Management System (ISMS)
9.2.6 Secure disposal or reuse of equipment	SD	4.6.4.3 The Information Security Management System (ISMS)
9.2.7 Removal of property	SO	5.12 FACILITIES AND DATA CENTRE
10 COMMUNICATIONS AND OPERATIONS MANAGEMENT		
10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES	SO	5.13 INFORMATION SECURITY MANAGEMENT AND SERVICE OPERATION 5.2.1 Console Management/Operations Bridge
10.1.1 Documented operating procedures	SO	3.7 Documentation

ISO/IEC 27002	ITIL	
10.1.2 Change management	ST	(4.2 Change Management)
10.1.3 Segregation of duties	SO	5.13 INFORMATION SECURITY MANAGEMENT AND SERVICE OPERATION
10.1.4 Separation of development, test, and operational facilities	ST	4.5.4.9 [Service Validation and Testing] Design considerations
10.2 THIRD-PARTY SERVICE DELIVERY MANAGEMENT 10.2.1 Service delivery 10.2.2 Monitoring and review of third-party services 10.2.3 Managing changes to third-party services	SD	4.6.6.2 Outputs
10.3 SYSTEM PLANNING AND ACCEPTANCE		
10.3.1 Capacity management	SD	4.3 Capacity Management
10.3.2 System acceptance	ST	4.4.6 (Deployment) Triggers, input and output, and inter-process interfaces
	SD	Appendix B: Service Acceptance Criteria (example)
10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE 10.4.1 Controls against malicious code 10.4.2 Controls against mobile code	SD	4.6.4.3 The Information Security Management System (ISMS)
10.5 BACK-UP	SO	5.2.3 Backup and restore
10.5.1 Information back-up	SD	Appendix K: The typical contents of a recovery plan
10.6 NETWORK SECURITY MANAGEMENT 10.6.1 Network controls 10.6.2 Security of network services	SO	5.5 Network Management
10.7 MEDIA HANDLING 10.7.1 Management of removable media 10.7.2 Disposal of media 10.7.3 Information handling procedures 10.7.4 Security of system documentation	ST	4.3 Service Asset and Configuration Management
10.8 EXCHANGE OF INFORMATION 10.8.1 Information exchange policies and procedures 10.8.2 Exchange agreements 10.8.3 Physical media in transit 10.8.4 Electronic messaging 10.8.5 Business information systems		
10.9 ELECTRONIC COMMERCE SERVICES 10.9.1 Electronic commerce 10.9.2 Online transactions 10.9.3 Publicly available information	SO	5.11 Internet/Web Management responsibilities

ISO/IEC 27002	ITIL	
10.10 MONITORING 10.10.1 Audit logging 10.10.2 Monitoring system use 10.10.3 Protection of log information 10.10.4 Administrator and operator logs 10.10.5 Fault logging 10.10.6 Clock synchronization	SO	5.13 Information Security Management and Service Operation (role of Service Operation)
11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL 11.1.1 Access control policy	SO	4.5.4 [Access Management] Policies/principles/basic concepts
11.2 USER ACCESS MANAGEMENT	SO	4.5 Access Management 6.6.9 Access Management roles Appendix F: Physical Access Control
11.2.1 User registration	SO	4.5.5.1 Requesting access 4.5.7.1 [User] identity
11.2.2 Privilege management	SO	4.5.5.3 Providing rights
11.2.3 User password management	SO	4.5.5.5 Logging and tracking access 4.5.5.6 Removing or restricting rights
11.2.4 Review of user access rights	SO	4.5.5.4 Monitoring identity status
11.3 USER RESPONSIBILITIES 11.3.1 Password use 11.3.2 Unattended user equipment 11.3.3 Clear desk and clear screen policy		
11.4 NETWORK ACCESS CONTROL 11.4.1 Policy on use of network services 11.4.2 User authentication for external connections 11.4.3 Equipment identification in networks 11.4.4 Remote diagnostic and configuration port protection 11.4.5 Segregation in networks 11.4.6 Network connection control 11.4.7 Network routing control	SO	5.5 Network Management 5.8 Directory Services Management

ISO/IEC 27002	ITIL	
11.5 OPERATING SYSTEM ACCESS CONTROL 11.5.1 Secure log-on procedures 11.5.2 User identification and authentication 11.5.3 Password management system 11.5.4 Use of system utilities 11.5.5 Session time-out 11.5.6 Limitation of connection time	SO	7.6 Access Management
11.6 APPLICATION AND INFORMATION ACCESS CONTROL 11.6.1 Information access restriction 11.6.2 Sensitive system isolation	SO	6.5 APPLICATION MANAGEMENT
11.7 MOBILE COMPUTING AND TELEWORKING 11.7.1 Mobile computing and communications 11.7.2 Teleworking	SO	5.9 DESKTOP SUPPORT
12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE	ST	4.4.5.3 [Release and deployment management] Build and test
12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS	ST	4.4.5.3 [Release and deployment management] Build and test
12.1.1 Security requirements analysis and specification	SD	4.4.5.2 The proactive activities of Availability Management Appendix F: Sample SLA and OLA
12.2 CORRECT PROCESSING IN APPLICATIONS 12.2.1 Input data validation 12.2.2 Control of internal processing 12.2.3 Message integrity 12.2.4 Output data validation	SO	5.2.2 Job Scheduling 5.10 MIDDLEWARE MANAGEMENT
12.3 CRYPTOGRAPHIC CONTROLS 12.3.1 Policy on the use of cryptographic controls 12.3.2 Key management		
12.4 SECURITY OF SYSTEM FILES 12.4.1 Control of operational software 12.4.2 Protection of system test data 12.4.3 Access control to program source code	ST	4.3.4.3 Configuration Management System (Definitive media library) 4.5.4.9 [Service Validation and Testing] Design considerations

ISO/IEC 27002	ITIL	
12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES 12.5.1 Change control procedures 12.5.2 Technical review of applications after operating system changes 12.5.3 Restrictions on changes to software packages 12.5.4 Information leakage 12.5.5 Outsourced software development		
12.6 TECHNICAL VULNERABILITY MANAGEMENT 12.6.1 Control of technical vulnerabilities		
13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES 13.1.1 Reporting Information Security events 13.1.2 Reporting security weaknesses	SO	4.2.4.2 Incident Models
13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS 13.2.1 Responsibilities and procedures 13.2.2 Learning from Information Security incidents 13.2.3 Collection of evidence	SO	4.5.5.5 Logging and tracking access 5.13 INFORMATION SECURITY MANAGEMENT AND SERVICE OPERATION (Service Operation's role)
14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT 14.1.1 Including Information Security in the business continuity management process 14.1.2 Business continuity and risk assessment 14.1.3 Developing and implementing continuity plans including Information Security 14.1.4 Business continuity planning framework 14.1.5 Testing, maintaining and reassessing business continuity plans	SD	4.5 IT SERVICE CONTINUITY MANAGEMENT
	SO	4.6.8 IT Service Continuity Management
15.1 COMPLIANCE WITH LEGAL REQUIREMENTS		
15.1.1 Identification of applicable legislation		
15.1.2 Intellectual property rights (IPR)		
15.1.3 Protection of organizational records	SO	5.6 STORAGE AND ARCHIVE
15.1.4 Data protection and privacy of personal information	SO	5.6 STORAGE AND ARCHIVE
15.1.5 Prevention of misuse of information processing facilities		
15.1.6 Regulation of cryptographic controls		

ISO/IEC 27002	ITIL	
15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE 15.2.1 Compliance with security policies and standards 15.2.2 Technical compliance checking	SO	5.1 MONITORING AND CONTROL
15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS 15.3.1 Information systems audit controls 15.3.2 Protection of information systems audit tools	SO	5.1.2.9 Service Operation audits

Appendix C: ISO/IEC 27k ISM standards in preparation or planning

ISO/IEC 27000

This standard introduces the 27k family of standards, giving an overview and outlining fundamental principles, concepts and vocabulary used throughout.

ISO/IEC 27003 (2009/2010 publication)

This standard will give implementation guidance for the specification in ISO/IEC 27001 and the code of practice in ISO/IEC 27002. It is expected to outline Critical Success Factors and an approach to planning, designing, operating maintaining and improving processes, working through each phase of the Plan-Do-Check-Act cycle, finishing with guidance on inter-organization cooperation.

ISO/IEC 27004

This standard concentrates on the development and use of measurement and metrics for Information Security Management. It details methods of collecting and analysing measurements to derive meaningful information to support management decisions, which will be used to assure the continuing effectiveness of an implementation.

Coverage includes policy, objectives and security controls, as prescribed in ISO/IEC 27001. The standard is intended to apply to the widest range of organizations with differing Information Security Management requirements.

ISO/IEC 27007 (2009/2010 publication)

This standard provides guidance to auditors of Information Security Management Systems against the specification in ISO/IEC 27001 and to some extent 27002. ISO/IEC 27007 builds on material in ISO 19011 with the addition of guidance specific to Information Security Management Systems information.

(ISO 19011:2002 provides guidance on the principles of auditing, managing audit programmes, conducting quality management system audits and environmental management system audits, as well as guidance on the competence of quality and environmental management system auditors.)

ISO/IEC TR 27008 (late 2011 publication)

This technical report will provide more specific guidance to auditors than ISO/IEC 27007 on ISMS controls in a risk-based approach to Information Security Management. It is expected to cover verification of the implementation level of the necessary controls.

ISO/IEC 27010

Part 10 is a new work item which began in 2008 and is expected to comprise many parts, dealing with Information Security Management issues arising from inter-organizational (and international) communications between industries in the same or different sectors, and with Governments. It will contain guidance on measures to protect critical infrastructure and to help all parties meet their legal, contractual and compliance responsibilities whilst allowing secure exchange of information.

ISO/IEC 27011 (late 2008 publication)

Part 11 is the first industry-specific ISMS implementation guide. It is for the Telecommunications Industry and will be published both as ISO/IEC 27011 and ITU-T Recommendation X.1051. X.1051(2004) already exists but will be updated by this joint development between ITU-T and ISO/IEC JTC1/SC27.

ISO/IEC 27031 (2010/2011 publication)

Part 31 is a specification for ICT Readiness for Business Continuity (title subject to change), and will look at the concepts and principles behind the role of information and communications technology in ensuring business continuity. It was initially envisaged as a multi-part standard (Overview/ Management framework/Threat monitoring and detection/ Vulnerability management/ Incident management/Services/ Testing and measurement/Assurance). In April 2008 this was changed to a single part (a guideline). The development team is liaising with ISO Technical Committee 233 to align with current work on business continuity.

Other relevant standards:

- ISO/IEC 18043 *Selection, Deployment and Operations of Intrusion Detection Systems*
- ISO/IEC TR 18044 *Information Security Incident Management*
- ISO/IEC 24762 *Guidelines for ICT Disaster Recovery Services*.

ISO/IEC 27032 (2010 publication)

ISO/IEC 27032 will offer guidelines for cybersecurity. Final scope of this standard is not yet fixed. It is expected to provide guidance to internet Service Providers and other internet users on their security responsibilities as part of the online community, to assist in (for example) the reduction of spam, virus and Trojan attacks.

ISO/IEC 27033

ISO/IEC 27033 is a multi-part (seven or more) standard that is both a renumbering and an updating of ISO/IEC 18028, published in 2006.

The standard will provide 'detailed guidance on the security aspects of the management, operation and use of information system networks, and their inter-connections. Those individuals within an organization that are responsible for Information Security in general, and network security in particular, should be able to adapt the material in this standard to meet their specific requirements' (from first Control Draft of 27033-1).

The many parts will cover risks, design techniques and control issues on additional aspects such as LANs and WANs; wireless, radio, broadband and voice networks; IP convergence (data, voice, video) networks; web host architectures; Internet email architectures (including issues arising from internet access for incoming and outgoing traffic) and routed access to third-party organizations.

Current model is as follows:

- Part 1: Guidelines for network security – a revision of ISO/IEC 18028 part 1
- Part 2: Guidelines for the design and implementation of network security – a revision of ISO/IEC 18028 part 2
- Part 3: Reference networking scenarios – Risks, design techniques and control issues in typical network scenarios
- Part 4: Securing communications between networks using security gateways – Risks, design techniques and control issues – a revision of ISO/IEC 18028 part 3
- Part 5: Securing remote access – Risks, design techniques and control issues – a revision of ISO/IEC 18028 part 4
- Part 6: Securing communications across networks using Virtual Private Networks (VPNs) – Risks, design techniques and control issues
- Part 7: Guidelines for securing risks, design techniques and control issues (specific networking technology topic heading(s) to be decided).

ISO/IEC 27034 (2009/2010 publication)

ISO/IEC 27034 is at an early stage. It is expected to develop guidance on Information Security for all activities concerned with IT application systems. These would include specification, design, programming, procurement and implementing.

Use of the standard will not be dependent on any particular application design method; its approach will be generic, and based on the establishment of relevant Information Security controls. This standard is likely to have a wide scope, and therefore to have multiple parts. The first part is at the working draft stage, but further parts are being planned.

Appendix D: Lessons from public sector security incidents

UK readers will be familiar with headlines like these:

Public sector incidents are more visible than those in the private sector, but it would be wrong to think that the Government is any worse in its ISM than other organizations. Indeed, in many of these examples, the fault lay with a contractor. However, Government databases are typically bigger, and incidents may potentially affect everyone in the country. The loss of the HMRC data in the UK in 2007 was taken very seriously by the UK Government and many enquiries and reviews have taken place following that and subsequent data loss incidents, with hundreds of pages of recommendations. This appendix looks at key recommendations that emerged from these studies. On 25 June 2008, several reports were published, the most important of which was the Coleman Report:

Independent Review of Government Information Assurance (The Coleman Report) (25 June 2008)

Nick Coleman is former Head of Security Services at IBM. This report discusses principles of information assurance as applied to UK Government and reviews the extent to which they have been applied. Topics include the changing business environment, operational risks, principles for successful assurance and how well the Government is doing. There is a list of recommendations concerned with vision, a unified Government approach to Information Assurance, a central facility for sharing risk information and other cross-Government capabilities. Information risks should be owned and reported on at Board level with the following in place: common supplier metrics to understand the capabilities of Government contractors; regular reports to the Prime Minister; common mandatory policy rules across Government; professionalism; measurement through auditing and monitoring and retention by Government of an independent oversight capability.

On the same day, the Government also published *Cross Government Actions: Mandatory Minimum Measures* that are to be applied across Government. The first section covers process measures to ensure that departments identify and manage their information risks. The second section outlines specific minimum measures that departments must take to protect personal information, although departments are expected to go further. The guidance is derived from the ISO/IEC 27000 series of standards. Progress in implementing the new measures and actions will be overseen by the Cabinet Sub-Committee on Personal Data Security. Departments will report each year and the Cabinet Office will report annually to Parliament on progress across Government as a whole.

Also that day, *Data Handling Procedures in Government: Final Report* was published. This is a Cabinet Office report commissioned after the HMRC Child Benefit CDs data loss. It summarizes work conducted in Departments to improve data handling and describes the steps the Government is taking to improve Information Security.

Key recommendations from these and other Government reports on ISM

- **Clarity in corporate governance arrangements** where ownership and accountability lie. Information handling should meet all compliance requirements and be audited, with responsibility at senior executive level
- **ISM needs to be, and be seen to be, a corporate objective with a senior owner**, implemented from Board level downwards with line of business objectives
- **ISM procedures should be formalized and integrated at all levels**
- **Stronger accountability** mechanisms within departments
- **Stronger scrutiny** of performance
- **Core measures to protect** personal data and other information across Government
- Create a **culture** that properly values, protects and uses information
- **Standardize and enhance processes** to understand and manage information risk
- **Identify the key individuals** responsible for information assets and setting out their responsibilities
- **Mandatory risk assessment** of the confidentiality, integrity and availability of information
- **Mandatory training** for all staff involved in handling personal data, reinforced on an annual basis
- **Staff awareness and education programmes**, embedding ISM into working life and behaviours
- **Use of Privacy Impact Assessments** when introducing new policy or processes involving personal data
- **Statements on Internal Controls** to include information risk, for scrutiny by the National Audit Office and spot checks by the Information Commissioner
- Further enhancing **transparency** of arrangements, through annual reporting to Parliament on progress and the use of Information Charters which provide clarity to citizens about the use and handling of personal data
- A range of **other measures** to improve Information Security across Government
- **Prioritization** of specific areas for attention, such as accountability for data and mail handling in business units.

Further information and links to sources

1 *Poynter Review into the HMRC Loss* (25 June 2008)

http://www.hm-treasury.gov.uk/poynter_review_index.htm

There were 45 recommendations in this report, most of which are being actively implemented by HMRC.

2 *Burton Review into the Loss of a Ministry of Defence Laptop* April 2008 – published 25 June 2008)

http://www.mod.uk/DefenceInternet/AboutDefence/CorporatePublications/PolicyStrategyandPlanning/ReportIntoTheLossOfModPersonalData.htm

This report particularly questioned the need for a personnel database to be kept on mobile devices and recommended that personal data should be available in future via secure links to central servers.

3 *Walport/Thomas Review of Data Sharing* (commissioned before the losses, published 11 July 2008)

http://www.justice.gov.uk/reviews/datasharing-intro.htm

The report gives key recommendations for organizations handling and sharing personal information. The Government's response was to give the Information Commissioner increased powers under proposals announced by Justice Secretary Jack Straw on 24 November 2008.

4 *Data Handling Procedures in Government: Final Report* (25 June 2008)

http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

This Cabinet Office report was commissioned after the HMRC Child Benefit CDs data loss. It summarizes work conducted in departments to improve data handling and describes the steps the Government is taking to improve Information Security through new minimum mandatory measures.

5 *Independent Review of Government Information Assurance (The Coleman Report)* (25 June 2008)

http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/ia_coleman080626.pdf

6 *Cross-Government Actions: Mandatory Minimum Measures* (25 June 2008)

http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/cross_gov080625.pdf

7 *National Information Assurance Strategy* (2007)

http://www.cabinetoffice.gov.uk/csia/national_ia_strategy.aspx

This strategy on cross-Government planning and approaches to Information Security Risk Management was published by the Central Sponsor for Information Assurance (CSIA), Cabinet Office in 2007. Its guidance is aligned with the other reports mentioned here. The objectives of the strategy will be developed into various actions and activities supporting a unified approach to information assurance, initially in Government, although after consultation the CSIA expects to generalize the approach for other industry sectors.

8 *Local Government Data Handling Guidelines* (SOCITM)

http://www.socitm.gov.uk/socitm/Library/Local+Government+Data+Handling+Guidelines.htm

Appendix E: Further information

Publications

ITIL

http://www.best-management-practice.com/Portfolio-Library/IT-Service-Management-ITIL/ITIL-Version-3/?trackid=002094&DI=582733

ISM Standards

http://www.iso.org/iso/store.htm

http://www.bsi-global.com/upload/Standards%20&%20Publications/shop.html

Publications from BSI to support the ISM standards:

BIP 2008:2003 *IMS and Information Security.* June 2003. Examines the benefits of an ISMS based on BS ISO/IEC 17799 as part of an integrated management system.

BIP 0064:2007 *Information Security Incident Management. A Methodology.* August 2007. Provides guidance on standard policy, requirements and methodology for Information Security incident response and management across many organizations, both commercial and Government.

BIP 0105:2008 Information Security Based on ISO 27001/ISO 17799: A Management Guide June 2006. Introduction and overview to both standards; links to other standards, such as ISO 9001, PAS 56 and ISO 20000; and links to frameworks such as CobiT and ITIL. Above all, guides organizations in the development of a best practice ISMS.

BIP 0106:2008 *Implementing Information Security Based on ISO 27001/ISO 17799: A Management Guide* June 2006. Covers the implementation issues of the Information Security standards up to and including audits; covers the installation of an ISMS.

BIP 0072:2005 *Are You Ready for a BS ISO/IEC 27001 Information Security Management Systems (ISMS) Audit?* September 2005. Intended primarily for organizations preparing for certification. System developers may also find it a useful reference document when considering the security aspects of new systems.

See these publications at the BSI online shop at

http://www.bsigroup.com/en/Shop/Shop-Product-List-Page/?d=N)0&q=information+security&f=&ps=10&pg=2&no=10&c=10

PAS 99:2006 Specification of Common Management System Requirements as a Framework for Integration.

http://www.bsi-global.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/PAS-99/

http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=0000000000030144033&recid=1876

BS 25999 Business Continuity

http://www.bsi-global.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999/

http://www.bs25999.com/

Qualifications

ITIL

http://www.itil-officialsite.com/Qualifications/ITILV3QualificationScheme.asp

Infosec Training Paths and Competencies (ITPC) qualifications offer recognized formal training and development for IT security professionals working for the UK Government and related organizations.

http://www.cabinetoffice.gov.uk/infosec.aspx

Professional bodies

The Institute of IT Service Management (UK)
http://www.iosm.com/

Institute of Certified Service Managers (USA)
http://www.icsmusa.org/

Institute of Information Security Professionals (UK)
http://www.instisp.org/

Websites

Central Sponsor for Information Assurance (CSIA)
This is a unit within the UK Government's Cabinet Office providing a central focus for information assurance activity across the UK.

http://www.cabinetoffice.gov.uk/csia.aspx

CPNI Centre for the Protection of National Infrastructure
Top ten guidelines for creating, reviewing, or updating your security plans.

http://www.cpni.gov.uk/About/topTen.aspx

CESG The National Technical Authority for Information Assurance
http://www.cesg.gov.uk/

The UK Department for Business, Enterprise & Regulatory Reform (BERR)
Has a website on Information Security at

http://www.berr.gov.uk/sectors/infosec/

It has a good summary page, 'ISO/IEC 27002 Explained' at

http://www.berr.gov.uk/sectors/infosec/infosecadvice/legislationpolicystandards/securitystandards/isoiec27002/page33370.html

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html

Author

Jim Clinch, B Tech (Elec Eng), MIET.
CLINCH Consulting

Jim has 34 years of experience of IT in the public sector, working for CCTA and OGC. Before joining the OGC Best Practice Group he spent 15 years as a senior consultant, researcher and speaker in Advanced Technology. During his last three years at OGC he was Project Manager and Chief Editor of the most recent revision of ITIL, which was published as five core books in 2007. Since leaving OGC, Jim has continued to work in IT Service Management best practice and contributes to the maintenance and enhancement of the official ITIL offerings.

Email cc@sukiya.plus.com

Reviewers

Stuart Rance, HP

Stuart is a senior Service Management and security consultant working for Hewlett Packard. He delivers a wide range of services, including Service Management strategy workshops, Service Management assessment, designing and managing improvement programmes, developing and implementing processes, and delivering security assessments and security improvement planning. Stuart has worked at senior levels within HP's largest customers, helping to improve their IT Services. Stuart also develops and teaches Service Management training courses and regularly presents at major Service Management events.

Stuart works as an examiner for the APM Group and for BCS ISEB. He is a member of the OGC/TSO Change Review Board for ITIL, a Chartered Fellow of the British Computer Society (FBCS CITP), a Fellow of the Institute of Service Management (FISM), and a Certified Information Systems Security Professional (CISSP).

Colin Rudd, Items Ltd

With 35 years experience, Colin is internationally recognised as a leading authority on Service Management. Lead author in the development of V1, 2 and 3 Colin was responsible for the design of the ITIL V2 framework. He now works for his own company using his extensive practical knowledge of Service Management to assist a number of major clients with the improvement of their Service Management processes and solutions.

Former President of the Institute of IT Service Management he is now a Director of itSMF International and Chair of the itSMF Standards Management Board. Colin's enormous contribution to the Service Management industry was recognised in 2002, with the presentation of the itSMF's "Paul Rappaport" Lifetime Achievement Award.

www.itemsltd.co.uk

Sourced by TSO and published on www.best-management-practice.com