ISM
Information security management

# GUIDE TO ACHIEVING ISO 27001 CERTIFICATION

## 1. Introduction

The management of information security is one of the most important issues facing business today, particularly for organisations who store or process information owned by their customers (e.g. suppliers of outsourced services, SaaS vendors, financial services, local and central government). How do organisations satisfy themselves, and their clients and stakeholders, that their security procedures are adequate?

The international standard ISO 27001 is generally acknowledged as the definition of best practice for information security management. But how should it be applied? Where do you start?

The purpose of this guide is to show you a straightforward way of building an ISO 27001 conformant Information Security Management System. It is designed to enable organisations achieve ISO 27001 compliance (and certification if required), giving their customers and stakeholders independent confirmation that they manage security effectively.

The guide contains:

- an introduction to ISO 27001, what it is and why it is important
- detailed instructions on how to develop an ISO 27001 conformant information security management system (ISMS).

The guide identifies the key components of an ISMS and the suggested contents. Microsoft Word templates and other tools are available (from www.pondergrove.co.uk/ism) so that you can use parts of this guide to build standard components quickly.

Details of the ISO 27001 standard are available from www.iso.org or http://shop.bsigroup.com/.

## 2. ISO 27001 - the worldwide standard for information security management

### 2.1 What is ISO 27001?

ISO 27001 was originally introduced in 1995, as BS 7799, the British Standard for information security management. It was adopted as an international standard, ISO 27001, in 2005, and revised in 2013.

Organisations (companies, government departments, local authorities etc) can apply to have their security management systems assessed against the Standard by independent third parties. These 'certification bodies' are appointed via the Department for Business, Energy & Industrial Strategy (formally BIS) and authorised to issue ISO 27001 certificates. The certificate is normally valid for three years and is dependent on periodic visits by the certification body.

ISO 27001 therefore enables customers to satisfy themselves that an organisation manages security effectively.

The Standard is in two parts. Part 1 (originally BS 7799-1, subsequently adopted as ISO 17799 and later renumbered ISO 27002) is entitled 'Code of Practice' and contains a comprehensive set of guidelines on protecting information. Part 2 (originally BS 7799-2, now ISO 27001) specifies the mandatory components required in an ISO 27001 compliant management system and is the standard against which certification assessments are conducted.

## 2.2 Why is ISO 27001 important?

ISO 27001 is an international yardstick by which customers, stakeholders and other parties can measure the effectiveness of an organisation's management of information security.

Rather than having to rely solely on their own judgement, ISO 27001 allows customers (at no cost to themselves) to use a qualified third party to verify whether the organisation's security is well managed.

It is tempting to make a comparison with ISO 9000 and quality management, and to conclude that holding an ISO 27001 certificate does not equate to good security management. There are however several important differences between the applications of ISO 9000 and ISO 27001. For example:

- ISO 27001 is a larger, more comprehensive standard than ISO 9000. It delivers a far more objective, and reliable, assessment of security than can be made of quality using ISO 9000.
- Because so many organisations hold an ISO 9000 certificate, it can no longer be used by customers to differentiate one supplier from another. In contrast, comparatively few organisations are ISO 27001 registered, making ISO 27001 a real differentiator.
- There are other ways to assess a prospective supplier's management of quality, such as sampling the product or service or taking up references. This approach doesn't work with security. The most effective security attacks are not detected. Customers don't know about them until it is too late.

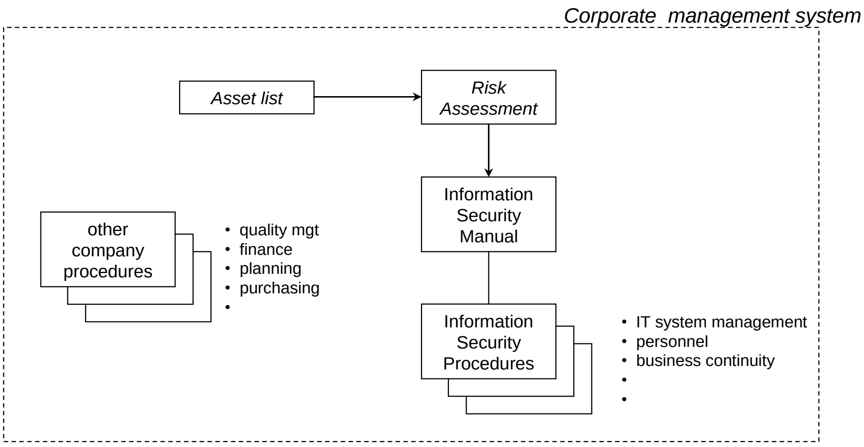
In summary, the fact that you have security policies, procedures, firewalls, encryption, backups etc tells people that you have a security management system. Showing them an ISO 27001 certificate tells them whether it is any good.

# 3. Developing an Information Security Management System

## 3.1 Principles

To develop an effective security management system quickly, we recommend that you follow two principles (illustrated in the diagram below):

- **Integrate it with your existing management system**. In other words if you have existing procedures (covering quality, personnel, finance etc) write the security procedures in the same style and include cross-references where necessary. There are two reasons for this:
  1. Some of your existing procedures may already address requirements of ISO 27001. Internal auditing, management review, IT acceptable use, supplier evaluation and purchasing are examples. Also, if your information processing depends on in-house developed software, your procedures for software development and version control need to be part of the ISMS.
  2. Like quality, security needs to be part of people's everyday thinking in order to be effective. Including security procedures within your existing management system helps to achieve this.
- **The ISMS should be based on a risk assessment**. As a general rule, a management system should be based on the organisation's business operation rather than the applicable standard. (Please see our Principles of Management Systems). Starting with the operational security requirements (i.e. what needs to be protected and why?) will result in a system that helps rather than constrains the business. The start point should therefore be a risk assessment, which is also a mandatory component of an ISO 27001 ISMS.
  The controls that you need to manage security depend on the information-related assets you hold (data, IT, people, buildings) and the risks to those assets. The sequence should be:
  - List the assets (see paragraph 3.2)
  - Assess the risks (see paragraph 3.3)
  - Develop the procedures which contain the necessary controls identified by the Risk Assessment



***the ISMS needs to be part of the organisation's overall management system and based on a Risk Assessment***

The main ISMS procedures are likely to comprise:

- The Information Security Manual, which should define the organisation's approach to information security, the organisation and structure of the security management system and the general security procedures which apply to all staff. The Security Manual should also show the certification body's assessor how the ISMS complies with each clause of ISO 27001.
- IT System Management procedure, which should define the controls which need to be applied by those who manage the organisation's IT and telecommunications infrastructure.
- Human Resources / Personnel procedure, which should define the personnel management controls such as recruitment of new staff, employment contracts, confidentiality agreements.
- Business Continuity procedure, which defines the controls which enable the business operation to continue in the event of a disaster such as destruction of the building or loss of the IT infrastructure.

The appendix contains suggested contents of these procedures. The remainder of this section explains how to create the Asset List and Risk Assessment.

### 3.2 The Asset List

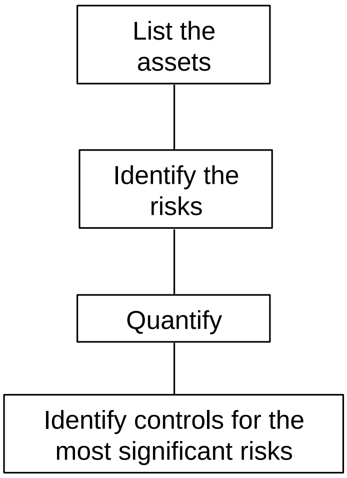
The purpose of the Asset List is to identify those assets of the organisation which have any impact on information security. This enables a Risk Assessment to be conducted and the necessary control mechanisms put in place to implement effective information security.

The list is simply a table listing the assets (e.g. building and infrastructure, IT, data, paper based information, human resources) together with their 'owners' i.e. the person responsible for their management and protection.

### 3.3 The Risk Assessment

The Risk Assessment is the foundation of the Information Security Management System. Its purpose is to identify the significant risks to the security of the organisation's information assets, in order to ensure that the security management system incorporates adequate controls to manage those risks.

We recommend a sequential approach to conducting the Risk Assessment as shown overleaf.



The controls are then defined in the security management procedures (see later paragraphs).

The Risk Assessment needs to:

- identify each risk
- assess each risk, in measurable terms, to ensure that the security management system is addressing all significant risks
- identify or cross-refer to the control which addresses the risk.

This is most easily presented in two tables. The first table should list the assets (brought forward from the asset list) and against each asset:

- identify the risks to:
    - Confidentiality (making sure that information is available only to those who have a legitimate need or right to access it)
    - Integrity (safeguarding the accuracy and completeness of information, so that a recipient can be sure that information received has not been altered during delivery)
    - Availability (ensuring that legitimate users of information have access to it when required)
- quantify the risks, by:
    - assessing the probability of the threat (T) as high (3), medium (2) or low (1)
    - making a similar assessment (V) of how vulnerable the asset is to the threat
    - making a similar assessment (I) of the impact to the organisation's business operation, should the threat materialise
    - multiplying T by V by I to quantify the risk on a scale from 1-27.

For those significant risks (where the measurement is > or = 6, say) a second table should be used to analyse them further and identify the controls. The controls may be physical (e.g. door locks) as well as management (who issues the keys?). The table should also give a cross-reference to where the applicable control is defined (e.g. Security Manual).

Click here for a Microsoft Word template to help you prepare your Risk Assessment; or go to our website to see how you can use our Risk Assessment software to make the task even easier.

## 4. What to do next

This guide has shown you how to build an ISO 27001 compliant security management system quickly, based on a risk assessment. The appendices list the suggested contents of the main procedures. You will also need other mandatory procedures whose scope goes beyond security management (e.g. internal audit, corrective action, document control, management review). Their content is largely defined by the Standard and the requirements are similar to those of other ISO standards (e.g. ISO 9001, ISO 14001). Templates are available from ISM.

Having built the system you are then ready to apply for assessment and to join the exclusive list of ISO 27001 registered organisations who can demonstrate that they have effective security management in place. A list of certification bodies, authorised to assess your security management system and issue an ISO 27001 certificate, is available from the UK Accreditation Service website.

Certification bodies normally make two visits, 1-2 months apart: the first to review the documented procedures and check they comply with the standard, and a second to verify that the procedures are being applied.

Building an ISMS can take anything from a few weeks to several months depending on what security controls are already in place. The Risk Assessment will confirm the scope of what you need. You could therefore achieve certification within three months from now.

Further help is available from our website, including:

- a risk assessment toolkit
- a comprehensive set of training courses
- a risk assessment service
- sample procedures.

# APPENDIX - CONTENTS OF THE ISMS COMPONENTS

## A.1 Introduction

This appendix lists the suggested contents and purpose of the main ISMS components, which are:

- Information Security Manual
- IT System Management Procedure
- Personnel Procedure
- Business Continuity Procedure.

## A.2 Information Security Manual

**Purpose:** to define the organisation's approach to information security, the organisation and structure of the security management system and the generic procedures which apply to all staff.

### Suggested contents:

| Heading | Content |
|---|---|
| Security Policy | |
| • Policy statement | Overall company statement on security. It should include:<br>• A statement of the purpose of information security i.e. why security is important to the organisation<br>• A management commitment to security<br>• Responsibilities for information security<br>• A statement on how information security is managed (i.e. by applying the ISMS)<br>The policy should drive much of the rest of the security management system |
| • Review arrangements | Who reviews the policy and when? |
| Organisation and responsibilities | Role of the Information Security Manager: who owns the security management system? |
| Scope and structure of the security management system | List of procedures, how they fit together, how they integrate with the company's overall management system (see 3.1) |
| General access and management controls | |
| • Building security | • Presence of locks, alarms etc; control of keys<br>• Links to external security agencies |
| • Secure areas | Control of areas in the building (e.g. comms/server room) to which access is restricted |
| • Control of visitors | Issue of passes, responsibility for supervision of visitors |
| • Information asset classification and control | • How are assets classified (e.g. company confidential, client confidential)? how are they identified? how are they controlled (storage and transmission e.g. by email or exchangeable media)?<br>• Clear/tidy desk policy |
| • Use of IT | General instructions to staff on use of IT facilities<br>• Control of passwords<br>• Use of the internet; precautions for incoming and outgoing email<br>• Use of local disk drives (e.g. C:, D:, E:)<br>• Locking screens when away from desk |

| Heading | Content |
|---|---|
| • Mobile computing and teleworking | Control of laptops, tablets and smartphones, including remote access to company networks; use of non-corporate IT e.g. public internet facilities |
| • Information exchange | Precautions for:<br>• Loading of external data<br>• Discussions off site (e.g. in public places) + use of mobile phones<br>• Avoidance of 'shoulder-surfing' |
| • Use of licensed software | Control of software installation on devices (PCs, phones etc) |
| • Corporate telecommunications | Control of information stored in telephone system (e.g. voicemail messages) |
| • Reporting security incidents and malfunctions | Procedure for staff to report incidents (e.g. suspected security breaches, observed or potential weaknesses in the security management system, software malfunctions) |
| Other controls | |
| • Staff training | What security training is provided (e.g. briefing for new staff), and how? |
| • Maintenance of records | What happens to security records? How long are they kept for? (e.g. visitors' book) |
| • Maintenance of data protection and privacy | How are the requirements of data protection legislation (e.g. Data Protection Act) met? |
| • Other applicable legislation | How is other applicable legislation applied (e.g. the Computer Misuse Act 1990, the Criminal Justice and Public Order Act 1994, the Copyright, Designs and Patents Act 1988, the laws relating to theft with regard to 'pirate' software)? |
| Statement of ISO 27001 Applicability | A table listing all clauses of ISO 27001 Annex A and for each:<br>• Stating whether it applies to the business<br>• If so, where the applicable control is defined (i.e. which procedure and paragraph)<br>Click here for a Word template (you will need your username and password; contact us if you would like us to resend these details to you) |
| ISO 27001 compliance matrix | A table showing how the ISMS complies with the mandatory clauses (4-10) of ISO 27001. Click here for a Word template (you will need your username and password; contact us if you would like us to resend these details to you) |

## A.3 IT System Management Procedure

**Purpose:** to define the controls within the organisation's IT and telecommunications infrastructure which enable the information security policy to be applied.

Notes on scope:

- This procedure should address those security controls which are the responsibility of the IT manager and staff. Procedures and controls which apply to all staff should be in the Security Manual.
- There is no need to duplicate what is defined in product manuals. The procedure should define the IT management policies which the IT staff are required to implement. For example, the procedure should define what is to be backed up and how frequently. How this is implemented technically (e.g. what software to run, parameters to be set) will be defined in the product documentation.

## Suggested contents:

| Section heading | Content |
|---|---|
| Technical infrastructure | Diagram (or cross-ref to diagram) illustrating the organisations IT infrastructure (e.g. servers, workstations, printers, LAN, internet links, firewalls) |
| • General policies | • Hardware redundancy to provide capacity and resilience<br>• Configuration of PCs: build standard; use of encrypted drives (e.g. for laptops)<br>• Use of UPS<br>• Use of trunking to secure cabling<br>• Use of wireless network(s);<br>• VPN for remote access<br>• IT maintenance arrangements (covered by service agreements which address confidentiality) |
| • Virus/malware/intrusion protection arrangements | • End point (workstation) protection<br>• Daily scans<br>• Web/email filtering; email filtering<br>• Firewall |
| • Authorisation for changes | • E.g. no changes without IT Manager approval<br>• All new hardware and software to be subject to the corporate purchasing policy<br>• Maintenance of records<br>• Procedure for removal of assets from site |
| • Internet links | • Control and standby arrangements |
| • Corporate telephone system | • Description; back up lines; setup of voice mailboxes + passwords; maintenance arrangements |
| IT asset management | • Maintenance of the asset list (PCs + software loaded on each)<br>• Removal of assets from site (e.g. laptops) |
| Access controls | • Segregation of data e.g. on specific directories/folders/drives (S:, H: etc) for protection ; mechanism for deciding who has access to which directories/folders/drives<br>• User ID and password issue and control; internal (staff) and external (customer)<br>• Use of standard email banner to advise the recipient of any restrictions on the use of the information<br>• Time-outs and automatic log-offs<br>• Control of web-based applications: e.g. use an encrypted log-in screen (https://) |
| Management procedures | |
| • Password management | • Password policy: e.g. minimum length, mixture of alpha and numeric, life<br>• Arrangements for renewing expiring passwords |
| • Change/configuration management for software patches | Arrangements for automatic application (installation on release); maintenance of application software |
| • Back up | What is backed up, when, how; is media stored offsite? Where/how? |
| • Archiving | Process for removing old data from online access; where is it stored? |
| • Operator and fault logging | Process for logging of housekeeping activities (e.g. backup) and noting any incidents |
| • Monitoring system access and use | Process for checking system logs for abnormal or unexpected events such as failed log-in attempts; policy for disabling terminals after successive failures to log-in |
| • Clock synchronisation | Process for checking that all system clocks are synchronised with each other and standard time (e.g. GMT) |

| Section heading | Content |
|---|---|
| - Disposal / reuse of equipment | How is surplus used equipment (e.g. redundant PCs, servers etc which may contain sensitive data) disposed of? |
| - Technical compliance checking | Use of tools (e.g. network analysers, password crackers) to verify that security policies are being adhered to; and the control of those tools to prevent misuse; penetration testing |

## A.4 Personnel Procedure

**Purpose:** to define the personnel management controls which enable the information security policy to be applied.

**Suggested contents:**

| Section heading | Content |
|---|---|
| Staff recruitment process | • Process for checking whether a new recruit might pose a threat to security (e.g. use of CV, interview, references)<br>• How do new staff know what their security responsibilities are and what is expected of them (e.g. use of a confidentiality agreement, employee handbook, contract of employment, briefing by Security Mgr)? |
| Termination | What steps are taken to protect company information when a member of staff leaves (e.g. user ID disabled to prevent access to IT systems, recovery of keys)? |
| Disciplinary process for breaches of security procedures | What is it? |

## A.5 Business Continuity Procedure

**Purpose:** to define the processes which make up the organisation's arrangements for continuing business operation in the event of a disaster.

It is assumed there is a separate disaster recovery (D/R) plan which defines the steps needed to recover the critical facilities (based on the risk assessment); or the plan can be included below.

**Suggested contents:**

| Section heading | Content |
|---|---|
| Planning | • Scope of the disaster recovery plan<br>• Responsibility for invoking the disaster recovery plan and appointing a Business Recovery manager |
| Disaster recovery arrangements | • Management of disaster recovery e.g. establishment of a command centre |
| Implementation | • Actions required for continuing business whilst recovery is in operation |
| Resumption of normal operations | • Basis of decision for resuming normal operations |
| Rehearsal | • Arrangements for rehearsing disaster recovery and business continuity, and frequency |
| Appendix: Corporate Business Continuity Requirements | • Table listing the critical IT systems and maximum outage times for each (as an input to the IT D/R plan) |