INFORMATION SECURITY – AN ESSENTIAL TODAY

A guide to ISO/IEC 27001 and ISO/IEC 27002 for business managers
INFORMATION SECURITY – AN ESSENTIAL TODAY

A guide to ISO/IEC 27001 and ISO/IEC 27002 for business managers

by W. List, D. F. C. Brewer, and G. R. Price
CONTENTS

Executive Summary 4
1 Preliminaries 5
  1.1 Information security – what is it? 5
  1.2 Management system standards – what are they? 5
  1.3 Other management system standards 6
2 What are ISO/IEC 27001 and ISO/IEC 27002? 8
  2.1 Why the standards exist and the development of 27001/27002 8
  2.2 Structure of ISO/IEC 27001 9
  2.3 Structure of ISO/IEC 27002 10
3 How to Use the Standards 12
  3.1 Initial decisions 12
  3.2 Plan 15
  3.3 Do 19
  3.4 Check 20
  3.5 Act 22
4 Conformance and Certification 24
  4.1 Conformance and certification 24
  4.2 What is certification? 24
  4.3 Who performs certification? 24
  4.4 The certification process 24
  4.5 Auditor findings 25
  4.6 Preparation for certification 25
  4.7 Benefits of certification 26
5 Case Studies 27
Appendix A Definitions 30
Appendix B Accreditation of CBs and Auditor Qualifications 31
Appendix C Sources of Further Information 32
EXECUTIVE SUMMARY

Information security is the term for those procedures and processes which control the integrity, availability and confidentiality of all information used by the organisation.

The technology changes how business tasks are performed, changes the effect of extant control procedures, and introduces new sources of error and management concern. Organisations wish to take advantage of the new technology, yet many members of management feel much less at home with IT than with the normal business functions of sales, production, finance and marketing. Therefore they rely on technical staff or third parties to advise them appropriately.

The objective of the ISO/IEC 27001 standard is to provide a method by which management can identify the information security requirements in their organisation, can police the implementation of cost effective controls and manage the changes to those controls, over time, to take account of business and technological change.

This will enable management to have greater confidence that the automated procedures are supporting their organisation effectively, providing a proper service to customers and stakeholders, and also reliable internal information. In addition, management will also be able to demonstrate that the wider aspects of information security are being addressed in a cohesive manner.

The standard and its accompanying code of practice, ISO/IEC 27002, are formidable documents to those unfamiliar with standards. Management should not be put off: used as a guide to marshal the current control procedures into a manageable structure, they are very powerful. It has been regularly found that organisations often have a large proportion of relevant controls actually in place, but that they have not been formalised.

Clearly the formality of the procedures in organisations varies with their structure and size. Even the smallest SME can use the standard to advantage provided they do not allow themselves to get overwhelmed. At least one ‘two-person’ business is certified to the standard.

This guide will help management set out on the road of improving their information security.
1.1 Information security – what is it?
Today the vast majority of organisations use computer technology as part of their daily routine. All organisations have an internal control system; in large organisations it is formal and highly documented, in small organisations it is usually informal and only essential parts are documented. Where computers and other electronic devices are used they perform specific tasks, which used to be done manually, and also perform control functions. They, therefore, have ‘taken over’ part of the previous internal control system and as a consequence the activities of computers must form part of the consideration of modern internal control systems.

Information security entails the maintenance of the integrity, availability and confidentiality of all information used in the organisation, however it is held. To be effective, the technical, clerical and managerial controls need to be integrated into one co-ordinated management approach; the ISO/IEC 27001 standard explains how to achieve this.

In a world where most computers, mobile phones, portable computing devices etc are designed to communicate with one another, it is obvious that organisations need measures to protect themselves from the ill-intentioned deliberately attacking them, people obtaining information that they should not have or they misuse, as well as the accidental errors which are inherent in all human activity.

Many of the internal controls we, as businessmen and women, are familiar with are, in modern parlance, information security controls because their purpose is to prevent or detect and correct errors in the financial and other records.

The need to be able to demonstrate to trading partners and/or regulators that an organisation has effective information security management both to protect itself and to ensure it does not damage others is becoming far more important, and, in some cases, a pre-requisite for doing business.

1.2 Management system standards – what are they?
ISO has published a series of management system standards, of which ISO/IEC 27001 is one. All of these management systems are based on the Deming cycle – Plan; Do; Check; Act (PDCA). This cycle is the basis of all effective management systems and was used in the Audit Practice Board briefing paper – ‘Providing Assurance on the effectiveness of Internal Control’.

In ISO-speak, a ‘management system’ is the engine that drives the PDCA cycle. Thus ISO/IEC 27001, for example, sets out how to:

- Identify an organisation’s security needs, using a risk based approach, and choose what information security controls are needed to reduce the information security risks to a level that is acceptable to the organisation (Plan);
- Operate those controls, giving them a fair chance of working by increasing staff awareness of information security issues and having processes in place to deal with incidents (Do);
- Check that the controls are working as intended, and indeed that the most effective controls have been chosen for the situations now being faced (Check);

1 Briefing paper published in July 2001 available from www.apb.frcpublications.com
Take appropriate action to remedy any defect in the controls that has occurred, or which may occur in the future, or would otherwise improve matters (Act).

The resulting system of management processes is called an Information Security Management System, or ISMS for short. It is not a document or a piece of technology, although there is a requirement to document the ISMS; and technology such as hypertext and intranets can help to meet the requirements for document control. It is, as we have mentioned, a set of management processes, so the standard is very much an instruction for what people, and in particular the directors and senior managers, should do to ensure that their organisation’s information security needs are at all times adequately addressed.

What the standard does not specify is what security the organisation needs, but it does help by providing a catalogue of likely information security controls, covering a broad spectrum of needs, to help to ensure that nothing important has inadvertently been missed out at the Plan stage – Annex A to ISO/IEC 27001. This is another important feature of a management system standard and is what some people call an AIL, or alternative ideas list.

The AIL therefore helps to ensure that the controls are in the right ballpark. The ISMS, through the operation of the PDCA cycle, then helps to fine tune the controls and keep pace with any changes to those needs; for example changes in business processes, changes in technology and changes in the organisation’s view of acceptable risk.

1.3 Other management system standards

Other management system standards include:

- ISO 9001 (quality);
- ISO 14001 (environmental protection);
- ISO/IEC 20000 (IT service provision);
- ISO 22000 (food safety);
- OHSAS 18001 (occupational Health and Safety);
- ISO PAS28000 (supply chain).

They all operate in the same way and their requirements can all be described in terms of being part of a ‘common PDCA cycle’ and an ‘AIL’ appropriate to the particular focus of that standard. For example, in ISO 9001, the AIL is section 7 of ISO 9001, called ‘Product Realisation’, which lists all the controls that may be applicable in ensuring that the products (which in ISO-speak includes services) that an organisation sells to its customers actually meet its customers’ requirements.

Like information security, quality management and the others are just other parts of internal control. Thus, we may think of:

- An ‘integrated management system’ as being the engine that drives the PDCA cycle for the whole system of internal control;
- Management system standards, such as ISO/IEC 27001, ISO 9001 etc, as being a cross-sectional view of that engine from a particular perspective, such as information security or quality.
Indeed, ISO/IEC 27001 was created with this concept firmly in mind and allows organisations to construct an integrated management system, covering any number of management system standards. Those organisations that have taken advantage of this possibility, not only enjoy just one set of certification audits covering all standards at the same time, but also the benefit of a single cohesive approach to internal control.

There are also (and will be) other standards in the ISO/IEC 27000 series:

- 27000 describes the fundamentals and vocabulary for information security;
- 27002 is a ‘Code of Practice’ that gives guidance on how the information security controls listed in Annex A to ISO/IEC 27001 may be implemented;
- 27003 will give guidance on implementing and operating an ISMS;
- 27004 will give guidance on metrics and measuring ISMS effectiveness;
- 27005 gives guidance on risk management;
- 27006 gives guidance on the certification process.
WHAT ARE ISO/IEC 27001 AND ISO/IEC 27002?

2.1 Why the standards exist and the development of 27001/27002

With the inexorable rise of computing in latter part of the twentieth century, from mainframes, through PCs and end-user computing to highly specialised and personalised interconnected technology, there arose a need for different sorts of controls from the traditional internal controls. In many cases the need was not met adequately, resulting in system and project failures over the years.

In the early 1990s it was appreciated that as interconnection between organisations grew, organisations which were well controlled internally would be at risk if others to whom they connected did not have as effective control mechanisms in their organisations. In addition, with the coming of the Internet, people were exploiting vulnerabilities in the software to create viruses and other ‘malware’ which could spread easily across the world.

A group of influential IT security managers and auditors from retail, banking, technical services, pharmaceuticals and the professions got together and produced a Code of Practice under the auspices of the Department of Trade and Industry (DTI). The objective of this code was to enable a ‘baseline’ to be established, which all organisations could reach, and also to enable clear communication to be established between trading partners on the subject of security.

The Code of Practice identified some 100 controls that could be applicable to information security systems of which ten key controls were regarded as essential for any organisation using IT. Subsequently, the Code of Practice was published as a British Standards guidance document PD0003, entitled ‘A Code of Practice for Information Security Management’.

The Code’s further development is set out in Figure 1 and paragraphs 2.1.1 et seq.

![Figure 1: Derivation of ISO/IEC 27001 and 27002](image-url)
2.1.1 BS 7799 Parts 1 and 2
Following a period of further public consultation, PD0003 was recast as a British Standard in its own right – BS 7799:1995 ‘A Code of Practice for Information Security’.

In February 1998, a second part, BS 7799-2:1998 was added to provide guidance on how to manage information security. This standard set out a process by which management could identify the security risks in the organisation and select from the controls in Part 1 those that were applicable, and add additional controls if appropriate.

2.1.2 BS 7799 Part 1 becomes ISO/IEC 17799
The Code of Practice (BS7799-1) became an international standard ISO 17799:2000. This standard was revised to take into account changes in technology, technical upgrades, compatibility issues and modern day security techniques. Existing controls were being enhanced and revised, and new controls added and this resulted in ISO/IEC 17799:2005 ‘Information Technology – Security Techniques – Code of Practice for Information Security Management’. ISO/IEC 17799:2005 became ISO 27002 in 2007.

2.1.3 BS 7799 Part 2 becomes ISO 27001

2.2 Structure of ISO/IEC 27001
The introduction to this standard reflects on the importance of the process approach adopted for ‘establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation’s Information Security Management System (ISMS)’. It explains that the Deming model (Plan, Do, Check, Act), adopted to structure the ISMS processes, is an effective approach to OECD Guideline2 principles governing risk assessment, security design and implementation, security management and reassessment. (See para 1.2 for a more detailed explanation of the Deming cycle.)

The introduction also explains the compatibility with two other management systems, ISO 9001:2000 and ISO 14001:2004, and the fact that it is designed to enable the integration of an ISMS with other management systems.

The standard is intended to be applicable to all organisations, regardless of type, size and nature. Certified organisations range in size from a two-person operation to multinationals.

Paragraphs follow concerning the scope of the standard, its application, other essential documentation to assist implementation, together with the normal terms and definitions.

The key part of the specification is contained in clauses 4-8. These requirements can be summarised as follows:

- Establish, implement, operate, monitor, review, maintain and improve the ISMS, using a risk based approach;

---

• Maintain document control over the ISMS;
• Formalise management’s commitment to making the ISMS work, and to providing the necessary resources to operate the ISMS and the controls that are implemented. Training, competence and awareness of staff must also be implemented;
• Carry out regular internal ISMS audits;
• Review of the ISMS on a regular basis by management;
• Continually improve the ISMS by ensuring that any non-conformities with the requirements are identified and corrected, and appropriate changes are made to reflect changes in business circumstances and use of technology.

Annex A of ISO/IEC 27001 comprises a summary of all the control objectives and related controls that are detailed in the Code of Practice (ISO 27002). It is the AIL as described in section 1.2. It is used to complete the Statement of Applicability, a mandatory requirement of the ISMS.

There are two additional annexes, ‘OECD principles and this International Standard’ and ‘Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard’, both of which help to set the context concerning respectively, OECD Guidelines for the Security of Information Systems and Networks, and other international management standards, i.e. quality and environmental issues.

Finally, there is a supporting bibliography.

2.3 Structure of ISO/IEC 27002
This is a Code of Practice and effectively provides a textbook or reference book detailing a wide variety of control objectives (11) and individual controls (133). There is no intention in the standard to expect organisations to have every suggested control in place, although the control objectives and controls have been put together based on the practical experiences of a number of technical and professional contributors.

The introduction contains useful background information about the concept of information security, why it is needed and how an organisation’s security requirements can be established. There is an emphasis on risk assessment being the starting point for selection of controls.

It highlights the three areas of control that are considered to be essential from a legislative point of view:
• Data protection and privacy of personal information;
• Protection of organisational records;
• Intellectual property rights.

It then goes on to identify seven controls that are considered common practice for information security:
1 Information security policy document.
2 Allocation of information security responsibilities.
3 Information security awareness, education and training.
4 Correct processing in applications.
5 Technical vulnerability management.
6 Business continuity management.
7 Management of information security incidents and improvements.

A quick glance at the above list shows that this is not by any means just a technological standard and is well within the compass of chartered accountants without technological expertise to assimilate, use and promulgate.

The main body of ISO/IEC 27002:2005 contains 11 security clauses which collectively contain 39 main security categories, and one introductory clause which introduces risk assessment and treatment. Within each of the 39 main security categories there is a control objective and one or more controls that can be used to achieve the objective.

Each control description comprises:

• A clear definition of the control;
• More detailed information to help in implementing the control, if required;
• Other information such as legal considerations and references.

The 11 control categories, or sections, apart from the introductory clause on risk assessment and treatment, are entitled:

1 Security policy.
2 Organisation of information security.
3 Asset management.
4 Human resources security.
5 Physical and environmental security.
6 Communications and operations management.
7 Access control.
8 Information systems acquisition, development and maintenance.
9 Information security incident management.
10 Business continuity management.
11 Compliance.

Again, a quick glance at the above list highlights the fact that this is not just a technical IT standard.
### 3.1 Initial decisions

- Scope
- Policy
- Risk Assessment (RA)
- Risk Treatment Plan (RTP)
- Statement of Applicability (SOA)
- ISMS Improvements
- Preventive Action
- Corrective Action
- Operate Controls
- Awareness Training
- Manage Results
- Prompt Detection and Response to Incidents
- Management Review
- Internal ISMS Audit

![Figure 2: Features of an ISMS](image)

Figure 2 shows the salient features of an ISMS. Paragraphs 3.2 to 3.5 work their way around the PDCA cycle in a moment, but before that there are some general requirements that should be looked at first.

#### 3.1.1 Management structure

Since an ISMS is a set of management processes, a management structure must exist in which to operate them. It is best to set this up, or certainly have it in mind, at the outset with the following considerations:

- In particular, who will own the ISMS? The owners have two principal duties:
  - The first is to decide on the acceptability of residual risk;
  - The second is to own the management review process, which checks to ensure that the controls are maintaining the required level of acceptable risk in practice;

- One or more people should be designated to carry out the internal ISMS audits (a mandatory requirement in ISO/IEC27001);

- It is often appropriate to put someone in charge of ISMS documents and record keeping;

- There may be other roles that people may play depending on the structure of the organisation.
3.1.2 Metrics and effectiveness

There is an old adage that says that something cannot be managed unless it can be measured. ISO/IEC 27001 embraces this with a requirement for metrics and the measurement of the effectiveness of the information security controls. The requirement, which was not included in the original British Standard, appears in a variety of places (which is why we have not included it in Figure 2) and it is best to treat it as a general requirement.

The idea is to identify and use an appropriate set of metrics to measure the effectiveness of the ISMS and, in particular, the information security controls. Guidance will be forthcoming in ISO/IEC 27004, but suffice for the moment to understand that broadly speaking there are two types of measurements: performance against a plan and performance against an objective. Once again it is best to think about this requirement at the start as it will assist in the design of the ISMS and the controls that are required.

Measurements of performance against a plan do not question whether the plan was the right plan in the first place. Only measurements of performance against an objective will answer that question, and in this case the pertinent objective is to reduce risks to the level accepted by management.

Some measurements may have temporary utility. For example, a set of metrics may be introduced to assist in gauging the commitment of managers to ISO/IEC 27001. Once the goal of ‘100%’ commitment has been achieved, there may be little point in continuing that form of measurement because the evidence of commitment will actually show in other ways. In this case the original measurements should then be abandoned.

Some measurements have near universal utility. Examples are measurements to determine the effectiveness of controls.

Controls act to:

- Prevent the events that may lead to some adverse impact (preventive controls);
- Detect the event, ideally in sufficient time for some other control, which may be technical or human, to correct the problem before the impact occurs (detective controls);
- React to the incident that results when the event is allowed to run its course, and all attempts to avert the impact fail (reactive controls).

Their effectiveness can be measured using the metrics of time and money as shown in Figures 3 and 4 (overleaf). This approach is referred to in the literature as the ‘Time Theory’. By factoring in the cost of controls, such measurements facilitate decisions to be made concerning the types of control, for example whether it is best to prevent the events, or merely react to the occurrence of impacts with a well thought out disaster recovery plan. These decisions have an important role to play when selecting controls.
For the purposes of designing controls, an effective control is able to prevent events or detect them in sufficient time to prevent the onset of a disaster, or failing that the ISMS has plans and processes in place to mitigate the impact. Figure 3 shows reduction of profit from P1 to P2 if the event (E) is detected not by the controls (because they are ineffective) but by management (M), after the impact has occurred (W). Figure 4 shows the effect if the same event is prevented by the controls or detected (D) and corrected (F) before the impact occurs (W). In this case the reduction in profit is significantly less.

Further details of this principle can be found at www.gammassl.co.uk/topics/time/index.html

### 3.1.3 Documentation requirements

ISO/IEC 27001 requires the organisation to have and maintain a documented ISMS. This means that the management processes that comprise the ISMS must be documented. There is no requirement to document anything else, unless there is a good reason to want to. For example, if for reasons of business efficiency it is necessary for a lot of people to do something in exactly the same way, it may be appropriate to document what they must do in the form of detailed work instructions.

Likewise the standard requires a number of records to be kept. These will inevitably include the document control records pertaining to the ISMS itself, internal ISMS audit reports, management review meeting minutes and data concerning ISMS effectiveness. However, above all, it is important to remember that the records are there to assist the owners of the ISMS to use the ISMS to manage information security. If the records do not do that, and there is no statutory reason to have them, then there is little point in having them.

Documentation and records do not have to be paper-based, and indeed they may be entirely electronic using hypertext technology. In this case the ISMS documentation and records are accessed using a web browser and using the ISMS becomes very much like using the Internet.
3.1.4 The 'To-Do-List'

There are a whole host of requirements that can be met by providing evidence of management performance. The standard also recognises that information security is a journey and not a destination. Thus, it is possible that, at any particular time, the existing controls may prove unsuitable for management’s needs and require to be changed. Some changes, for example those affecting a large and complex IT network, may take several months or even years to implement. The ISMS should demonstrate that management has control over the change process and, in particular, that it is managing the risks throughout the transition.

A convenient way of doing this is to include a simple ‘To-Do-List’ in the ISMS. It would:

- Record all the required changes;
- Include target and actual completion dates;
- Provide an appropriate level of detail (the record can always refer to further detail held elsewhere);
- Act as a summary of what has happened and is going on.

An interesting question is ‘does an organisation need all the information security controls that it requires in place before compliance with the standard can be demonstrated?’ The answer has to be ‘no’, as any corrective/preventive action or ISMS improvement (as required to conform with the standard) would render the ISMS non-conformant, and that would be nonsense. It therefore makes sense to build an initial ISMS that reflects the current state (as all ISMSs will require change once they have become operational); that is:

- They will have all the management processes, required by the standard, in place and fully operational, with plenty of ISMS records to demonstrate that fact;
- They will have a To-Do-List showing a history of corrective/preventive actions and ISMS improvements, some of which will be outstanding, but showing clear evidence of progress and that any attendant risks are being managed.

The process described in paragraphs 3.2.3 to 3.2.5 below could be considered as a review of the current position and/or the performance of a gap analysis of the current position against the required position. Clearly if major problems existed in the information security controls, the organisation might delay certification until these were rectified.

An important consideration which underpins this approach is that the ISMS should clearly distinguish between the current state of affairs and any plans for future improvements.

Many failings of ISO 9001 in the 1990s were attributed to managers documenting what they felt the assessors would like to read rather than what actually happened. Of course, when the assessors discovered that reality did not correspond in any way to the documentation, they had no alternative but to argue that the documentation was right and hold the organisation non-conformant in failing to adhere to its own policies and procedures.
3.2 Plan

3.2.1 Scope

Having dealt with the preliminaries, we are now in a position to take each of the major PDCA requirements in turn and give advice on their implementation.

The first step is to define the scope of the ISMS. The organisation chooses what this scope is. For example, it could be the whole of the organisation, some particular site, a department or a particular business service.

It is usual to define the scope in two ways: first, as short paragraph of one or two sentences. This will appear on the organisation's certificate if it opts for certification. Secondly, it is a requirement to have a more elaborate description, which will also serve the purpose of defining the context in which the risk assessment will be performed. Make sure that the owners of the ISMS have management responsibility for everything in scope of the ISMS and that there is a clear boundary (physical or logical, or both) between what is in scope and what is not (then there can be no argument as to what is in scope and what is not).

In practice, if the scope of the ISMS is the whole of an organisation, the ISMS should be owned by the executive directors and it may be appropriate, in this case, for the ISMS to be a board committee with wider powers, such as internal control in general. It may also be appropriate to have a hierarchy of ISMSs; with an overarching ISMS at executive board level and subordinate ISMSs at the department/business unit level. It would be appropriate for the overarching ISMS to establish common policies and procedures across the whole of the organisation.

If the scope is part of the organisation (e.g. just the IT department) then care needs to be taken in drawing up the risk treatment plans (see paragraph 3.2.4) to ensure that the controls within scope of the ISMS do not trespass into the areas of responsibility of those parts that are outside scope (e.g. the user departments). There may also be a complication if the ISMS is itself dependent upon controls which are the responsibility of other parts of the organisation that are outside the scope of the ISMS, for example HR. In this case, it is appropriate to reference the existence of the controls (e.g. a staff handbook) but say that they are not within scope of the ISMS.

3.2.2 Policy

ISO/IEC 27001 requires the organisation to have an ISMS policy. This is far more embracing than just having an information security policy and concerns ISMS governance as a whole. It should, for example, define the responsibilities of the ISMS owners, identify the organisation's approach to risk assessment and define the criteria that are used for accepting risk. In this sense the standard identifies a number of topics that must be covered by the ISMS policy, but organisations are free to add others. For example, it would be appropriate to refer to policies that originate outside of the ISMS, but with which the ISMS must comply – for an ISMS that has the IT department as its scope, such policies would undoubtedly include those set by the HR department concerning the hiring/firing of staff and their welfare. As a counter example, an ISMS for the HR department would include in its ISMS policy the IT policies that had been defined by the IT department.

Although an information security policy is not a requirement, in practice it is a very good idea to have one, as it documents the organisation's definition
of what it means by information security. No doubt it would address the three principal tenets of information security (confidentiality, integrity and availability) but it could also extend the scope of the policy to other tenets such as accountability and non-repudiation. In addressing these issues, it would present a high level statement of what the organisation seeks to achieve.

### 3.2.3 Risk assessment

The requirement for risk assessment originates from the overriding objective to ensure that information security controls must be proportionate to the degree of risk that they are designed to combat. Risk assessment is the first step in the process to achieve proportionality in the selection of controls, as illustrated in Figure 5.

ISO/IEC 27001 does not mandate or even recommend an approach to risk assessment, but it does describe the process in terms of threats, vulnerabilities, assets and impacts. As shown in the diagram, a threat exploits a vulnerability to violate an asset to cause an adverse impact. For example, a hacker may exploit the naivety of an Internet user to steal that user’s bank account details and passwords and thereby steal their victim’s money.

The objective of the risk assessment is to gauge the extent of the risk, and in this sense the output of the assessment could simply be a list of risks, some of which (in keeping with the Audit Practices Board guidance on internal control) are deemed to be non-applicable and no further action is taken.

The requirement for considering threats, vulnerabilities, assets and impacts is to help to ensure that nothing of importance is overlooked. If there is, then as explained in paragraph 1.2, there is an AIL that will come to our rescue, but that will only work if the controls that we need are included in Annex A to ISO/IEC 27001. Unfortunately, the Annex A controls are not exhaustive and are particularly weak in the context of business applications. If these are in scope of the ISMS, then it should be these applications that form the focus of the risk assessment and reference should be made to other documents to assist in checking that all appropriate controls are included (e.g. the ICAEW criteria for assessment of packages). Indeed, the standard continuously reminds us of this focus with its numerous references to the organisation’s ‘overall business risks’.

---

**Figure 5: Risk assessment, risk treatment and the selection of controls**
3.2.4 Risk treatment

Having identified what risks merit further consideration, as illustrated in Figure 5, the standard asks the organisation first to decide how to treat them. It suggests that the organisation might avoid the risk, accept it, transfer it or mitigate it. If it is decided that the risk of electronic commerce was too great for the organisation, then the risk could be avoided by not having an e-commerce website, or the risk might be transferred by outsourcing the e-commerce website to a professional service provider. Alternatively, the organisation might mitigate the majority of the risks associated with e-commerce and accept those judged to be unlikely and of inconsequential value.

In choosing to mitigate the risk, the final step in the process described in Figure 5 is to select the controls. A convenient way of doing this, which incidentally rolls the risk assessment, risk treatment and control selection all into one single process, is to consider events and corresponding impacts.

The events and impacts listed in Figure 6 have proven to be most comprehensive in the application of ISo/IEC 27001 and therefore provide a useful starting point. Indeed for many organisations these are all that are required. The method generates a Risk Treatment Plan (RTP) for each event. The method is intended to be performed by the owners of the ISMS who will:

- Firstly consider what, if anything, is done to prevent the event;
- What is done to detect the event, should for example the preventive measures fail;
- What is done to recover from the impact if all else fails.

The analysis is recorded in the form of a story, making it easy to read and understand. There may be different story lines (sometimes called threads) each dealing with different threats, vulnerabilities, assets and impacts, and ending with a statement that the residual risk is acceptable. Each time the authors document what is done, they are identifying the applicable control(s).

Of course, during this process it is possible that improvements will be identified. If they are, they can be noted in the RTP, but most importantly added to the To-Do-List with a target completion date that reflects the severity of the risk that is being taken in the absence of the control.

<table>
<thead>
<tr>
<th>EVENTS</th>
<th>IMPACTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft</td>
<td>Adverse press coverage</td>
</tr>
<tr>
<td>Acts of God, vandals and terrorists</td>
<td>Organisation ceases trading</td>
</tr>
<tr>
<td>Fraud</td>
<td>Inability to carry out all or some of its business</td>
</tr>
<tr>
<td>IT failure</td>
<td>Loss of customer confidence</td>
</tr>
<tr>
<td>Hacking</td>
<td>Loss of revenue</td>
</tr>
<tr>
<td>Denial of service</td>
<td>Increased costs</td>
</tr>
<tr>
<td>Disclosure</td>
<td>Prosecution</td>
</tr>
<tr>
<td>Breach of the law</td>
<td></td>
</tr>
</tbody>
</table>

Figure 6: Example events and impacts
3.2.5 Statement of Applicability

Annex A to ISO/IEC 27001 is a list of the 133 controls described in ISO/IEC 27002. The requirement is to go through all 133 controls and decide whether or not the control is applicable to the ISMS. The record of the decisions as to applicability of each of the 133 controls is called the Statement of Applicability (SOA).

As mentioned in paragraph 1.2, Annex A acts as a safety net to ensure that important information security controls are not inadvertently omitted. We have also mentioned that the list of controls is not exhaustive, particularly from the perspective of business applications. However, in terms of IT platforms and the physical/personal security measures on which they rely, the controls in Annex A are pretty robust.

If a control in Annex A is deemed not applicable, an explanation is required. For example, the controls concerning outsourced software development may not apply because the organisation does not outsource software development. In general, the organisation should find that the explanations for non-applicable controls are as simple as in this example.

If a control in Annex A is applicable, justification is required by reference to the risk assessment. In practice, a control can be justified by reference to an ISMS policy statement (which is effectively a reference to the implicit risk of failing to meet ISMS policy). If the risk assessment/treatment uses the ‘tell it like a story’ approach described in the previous section on risk treatment, then justification can also be made simply by reference to at least one RTP that invokes the control. Note that it is unnecessary to reference all the RTDs as the SOA is just a cross-check to ensure that controls have not been inadvertently omitted.

The standard requires the organisation to indicate whether the control exists or not. If the organisation uses the To-Do-List approach, then if the control does not yet exist, it should be identified on the To-Do-List.

Although not required by the standard, in practice it is convenient to describe how the applicable controls are implemented in the SOA. Either write down a short description of how the control is implemented, or reference a documented procedure. The standard states that the SOA provides a summary of controls, and writing the SOA in this way provides a convenient way of doing that.

3.3 Do

3.3.1 Operate controls and manage resources

It should almost go without saying that the controls, once they exist, should be operated in accordance with the organisation’s intentions, for example as recorded in its RTDs and the SOA. To facilitate this, there is also a requirement for management to ensure that there are adequate resources to operate them. Of course, anything on the To-Do-List should be progressed. ISO/IEC 27001 makes a special reference to this in clauses 4.2.2 (a) and (b), and although it does not call it a To-Do-List, this is what it means.

3.3.2 Awareness training

In common with all management system standards, ISO/IEC 27001 has a requirement for awareness, training and competence. There will be some people in an organisation that will be responsible for maintaining the security
controls, for example IT people to maintain the firewalls and security guards to lock the buildings. The standard requires these people to be competent in the discharge of their respective duties and to receive appropriate training. The standard asks for records to be kept to help the organisation keep abreast of how well it can rely on them to do their duty. Remember: if the firewalls are wrongly configured they will not work as intended, just as an unlocked door will not deter a burglar. The same is true of all other information security controls, whether they are technical in nature or not.

Whilst some people in the organisation may have specific information security responsibilities, everyone has a general responsibility for maintaining security, and this is where the requirement for awareness comes in:

• Teach the staff what the policies are and what the organisation expects of them;
• Raise their awareness of information security issues such as viruses, phishing, eavesdropping, denial-of-service and hacking;
• Point out to them how these threats can damage the business and even affect the staff in their personal lives;
• Instruct the staff on what they should do when they spot something wrong or even suspect that something is wrong.

Staff may be able to prevent the occurrence of a security event, or detect it soon after it has happened and bring it to attention with sufficient time for management to take action to avoid the impact. (Remember the Time Theory we discussed in paragraph 3.1.2.) Staff should thus be regarded as information security controls in their own right. They form an integral part of the system of internal control, as they always have done. They are not victims of it!

3.3.3 Prompt detection and incident response

The standard recognises, quite rightly, that security cannot be 100%, and that there will be incidents. The standard is cognisant of the Time Theory, which is why it insists on having controls for the prompt detection of errors and other events.

When there is an incident, the management and staff need to know what to do, and the actions to be taken will run a lot smoother if management has worked them out in advance, and in some cases has practised them as well. What happens if someone smells burning? They may be instructed to raise an alarm, under some circumstances to tackle the problem themselves and in others to escalate the problem for more experienced people to deal with. Ultimately, this will be the fire brigade. Staff will be able to be evacuated, quickly and safely, because they know what to do and have practised it many times before. Management knows what to do with them after the evacuation, how to deal with the media, how to deal with the emergency services, how to deal with the anxieties of their staff's friends and relatives, how to deal with the loss adjusters and how to recover their organisation's business. They have a plan and it starts with the process of prompt detection and incident response.

Fire is, of course, a threat to information security as indeed is theft, which is why these start the list of typical information security relevant events (see Figure 6). The treatment of other information security relevant events follows exactly the same process. If someone opens an e-mail attachment and infects
their computer, what are they supposed to do? What action is taken to prevent the virus from affecting the whole network? What does the organisation do if it does? The answer is to have a plan for prompt detection and incident response.

3.4 Check

3.4.1 Internal ISMS audit

If there is an effective set of information security controls, they will work when they are required to work; they will work as intended and reduce the risk to the level previously judged by the ISMS owners, when they chose the controls, to be acceptable. But what if they are wrong? If there are no events, the controls do not have anything to do. How does anyone know that they will work when an event occurs? The answer to this question lies in the requirement for internal ISMS audit.

Internal ISMS audit is the primary means by which the owners of the ISMS can determine whether the controls and indeed the management system processes themselves are working as intended. A requirement of the standard is that the auditors do not audit their own work; therefore this task can be carried out by any independent member of staff whether or not they are called internal audit. The auditors should operate in accordance with a schedule that aims to look at the whole of the management system and all of the applicable controls at least once per year.

Internal ISMS audit is so named to distinguish it from any other function of internal audit, which for many organisations traditionally has a financial connotation. Where an internal audit unit exists in an organisation the works of ISMS internal audit may conveniently be integrated with their existing work.

The auditors should be looking for evidence of performance. For example, evidence that the internal audits are being performed is provided by the audit reports and the prosecution of the audit schedule. Evidence that an access control policy is being implemented is provided by looking at what is inside the computer access control tables. Better still, find out if the managers look at these tables and take action if their staff do not have the access rights, or indeed have more access rights than they need to do their jobs.

Auditing is about checking, which is why it is one of the mainstays in the 'check' activity of the PCDA cycle. But in addition to checking that the various processes and controls are being operated as intended, the auditor may also be requested by management to consider whether the processes and controls are indeed the right ones, or if the controls could be implemented in a better way. In information security, one way of doing this is to look for evidence that the controls are working as a whole in accordance with the risk treatment plans to reduce the actual risks to the levels deemed acceptable by management. Another objective would be to check compliance with the standard (and indeed any relevant legislation and/or regulation).

3.4.2 Management review

Management review requires the owners of the ISMS to take stock of the ISMS and take action to ensure its continued effectiveness. In particular they are charged with ensuring that the information security controls as actually practised, will continue to reduce their risks to an acceptable level, and indeed that the risk level is still acceptable. In addition, the review should consider if the controls in place are the right controls – could they be replaced by a better
control now the technology has evolved? Could they be implemented in a
different way to be more efficient or effective?

The standard requires this review to take place at least annually. It does not
have to be a special meeting. It could be an agenda item at some regular
meeting of the ISMS owners. The standard does, however, stipulate what the
inputs to the meeting must be, what must be discussed and what the outputs
must be (see Figure 7). The inputs include the results of audits, feedback
from interested parties, results from the measurements of effectiveness and
recommendations for improvements. The outputs make adjustments to the
ISMS and are discussed in our next and final section on the PDCA cycle, which
considers the ‘act’ phase.

3.5 Act

3.5.1 Corrective action

Corrective action is required when there is something that is required to
maintain security, or indeed maintain conformity of the ISMS with ISO/IEC
27001, which manifestly the organisation is not doing. The action is simply
to put matters right. The ‘something’ that is not being done is called a non-
conformity.

In taking action, do not forget, of course, that the cause of the failing might
be because the staff are not aware, or perhaps lack training, or that the
instructions given to them might be defective in some way or plain simply
wrong. In this case, the action might be to improve awareness or change the
instructions.

A requirement of the management reviews is to determine the effectiveness of
corrective actions. One way to do this is to look for trends. Analysis of many
corrective actions might indicate that they are symptomatic of some underlying cause that was not immediately apparent when the corrective actions were considered individually. Another requirement is to take action to ensure that non-conformities do not reoccur.

3.5.2 Preventive action
Preventive action is action taken to prevent or otherwise avert some future problem. An example would concern the introduction of some new security technology in anticipation of a future threat. The threat might be a function of the quantity of business that an organisation does. The current controls are adequate, but business is booming and at some time in the future the risk will be deemed unacceptable by the ISMS owners. Currently there is not a problem, but it is anticipated that there will be and therefore the action taken to install the new technology is a preventive action.

A related example would be the failure to prosecute the project to introduce this new technology. If the project is delayed, or business grows at a faster rate, some other preventive action needs to be taken. If it is not, there is a good chance that the information security risk will become unacceptable. This would need to be treated as a non-conformity if it were allowed to happen. The moral here is the diligent use of the To-Do-List to manage the corrective and preventive actions.

3.5.3 Improvement
An improvement is something that makes the ISMS and/or the information security controls better than they currently are. An example would be improving the effectiveness of controls:

- Using the ‘auto-protect’ feature of an anti-virus product will increase the effectiveness of the anti-virus measures as the time taken to detect the presence of a virus will be decreased;
- Using a ‘live-update’ facility, rather than relying on users to manually update their virus libraries, will render it more effective as it will be able to detect new strains of virus as soon the updates are released by the anti-virus vendor.

Another example would be improving efficiency by removing redundant controls and bureaucracy. Good candidates for this type of treatment are IT systems that merely emulate the original non-IT systems. Often in these cases, IT controls duplicate and run in parallel with the original non-IT controls leading to business inefficiency.
4.1 Conformance and certification
Historically, several organisations seized upon the original Code of Practice, BS 7799:1995, and claimed conformance to it (often described as compliance to it) as a way of demonstrating that their information security controls conformed to best practice. Whilst this was well intended, it was difficult for outsiders to ascertain exactly what the organisation was conformant to. For example, had they implemented all the controls or only those applicable to their organisation? Did they have an ISMS? Third party assessment of conformance (or as it is better known – certification) has always been to the ISMS standard, presently ISO/IEC 27001.

Creating an ISMS, as has been explained previously (paragraphs 1.2 and 3.2) includes a requirement to create a risk treatment plan for identified risks to the organisation and to identify all controls described in ISO/IEC 27002 that are applicable. Therefore, by implication, the organisation has implemented ‘best practice’ applicable controls.

Whilst an organisation can always claim compliance, there is a world-wide certification scheme that facilitates independent third party assessment of conformance. This is considered to be the best way to demonstrate compliance.

4.2 What is certification?
Certification is the process by which the ISMS is independently audited as conformant with the ISO/IEC 27001 standard. Following a satisfactory completion of the audit, a certificate is issued to the organisation stating that their ISMS is conformant with ISO/IEC 27001.

Conformance with ISO/IEC 27002 is not capable of being certified, the technical argument being that it is a code of practice and not a specification.

4.3 Who performs certification?
The independent audit is conducted by a Certification Body (CB). This is an organisation whose purpose is to certify conformance with any type of standard; be it a management system (e.g. ISO/IEC 27001), food safety, equipment calibration, etc. In order to conduct the audits the CB needs to be accredited for each standard for which it will perform the work. See Appendix B for further details on the accreditation process for CBs.

CBs may employ certified auditors and, where required, technical experts, to perform the audits for conformance to ISO/IEC 27001.

4.4 The certification process
The organisation wishing to be certified contracts with a CB to perform the audit. The CB then conducts the audit and, subject to satisfactory performance by the organisation, awards a certificate. It is usual for the scope of the ISMS to be recorded on the certificate. Subsequent to the award of the certificate the CB will perform surveillance visits (usually six monthly or annually) to ensure that the ISMS and the controls in place continue to be satisfactory from an audit point of view.

The certification audit is conducted in two stages:

---

3 The term ‘certification body’ is used in the UK. However in other countries it may variously be described as ‘registration bodies’, ‘registrars’, ‘assessment and registration bodies’ and ‘certification/registration bodies’. In this document all these organisations will be referred to as certification bodies.
• Stage 1 is an examination of the ISMS documentation to determine if it conforms to the requirements of the standard. These requirements are in clauses 4 to 8 of the ISO/IEC 27001;

• Stage 2 is testing that the procedures and controls specified in the ISMS are operational in practice. This part of the audit is very similar to a compliance audit conducted by financial auditors.

Surveillance visits are planned so that the full scope of the ISMS is tested over a three year period.

4.5 Auditor findings
During the conduct of the audit and the surveillance visits the auditors may discover matters which cause them concern and areas where improvements may be made. The auditor will prepare and agree their report with the representatives of the organisation being certified prior to the conclusion of the audit. As part of this report the auditor will recommend certification (or otherwise). This discussion affords the organisation the opportunity to debate and resolve with the auditor any areas of controversy, and is similar in objective to a traditional external audit management letter.

4.5.1 Non-conformities
A non-conformity usually occurs where the organisation is either failing to meet the mandatory requirements of the standard (e.g. there are no internal ISMS audits organised or no management reviews) or where the actual activities of the people/equipment are not as stated in the ISMS or procedures used in the organisation (i.e., the organisation is not doing what it said it was supposed to do). Where a non-conformity exists, the auditor will agree with the organisation a corrective action plan (CAP) to rectify the situation, the time allowed being consistent with the severity of the non-conformity. However, it is usually the case that a non-conformity must be resolved before a certificate can be issued or, if it comes to light on a surveillance visit, very promptly after the visit.

4.5.2 Observations
An observation (sometimes called a minor non-conformity) is a gentle hint that there is something amiss, which, if allowed to continue or get out of hand, would constitute a non-conformity.

4.5.3 Recommendations for improvement
Sometimes during the audit, suggestions will emerge for the improvement of the ISMS. Some of these may well have been previously identified by the organisations and the auditee may simply be telling the auditor what these are. In either case it is usual practice for the auditor to make a record of them in the audit report.

4.6 Preparation for certification
Organisations wishing to be certified must have in place the mandatory documentation and records specified in the standard, otherwise they will fail either Stage 1 or Stage 2 of the certification audit.

Areas where often the preparation has been inadequate are the failure to:
• Record adequate justification for the selection of controls from Annex A (Stage 1);
• Plan a series of ISMS internal audits to cover the whole ISMS in a year (Stage 1) and/or not to have followed this plan (Stage 2);
• Hold and/or record management meetings and ensure that actions decided upon at such meetings are followed up (Stage 2);
• Follow the procedures as laid down (Stage 2).

4.7 Benefits of certification
Given that an organisation has in place an ISMS conformant to the standard and that the organisation’s management is not unhappy with the quality of information security in place, then for the marginal cost of certification the organisation could reap the following benefits:
• It demonstrates a commitment to information security as part of good corporate citizenship in this ever increasingly regulated world. This may have a market advantage and be useful in discussions with regulators;
• Reduction in insurance premiums – some insurers give reductions;
• Easier discussions with trading partners, particularly if both are certified. Whilst some detailed specific connectivity issues will need to be agreed, the general security framework and quality can be assumed, as can the structure within which the detailed requirements are to be implemented. At the very least they will have a common language and common understanding of information security;
• If the organisation provides outsourcing arrangements to others, then being certified will assist and may well increase its customers’ or stakeholders’ confidence in the security measures that are in place and the ability of the organisation to manage security, particularly when new ways of attacking IT systems are discovered. Experience has shown that this may lead to a dramatic reduction in the number of customers or interested parties who want to carry out their own technical security audits prior to buying or whilst using the service.
The text of this booklet has been drawn from the authors’ many and varied experiences in developing and applying ISO/IEC 27001, and observing it being applied by others. This chapter presents five studies which summarise why each particular organisation embarked upon ISO/IEC 27001 conformance, how it went about the task, the benefits it gained and the resources it consumed in the process. The organisations cited range from the very small to the very large, and include private companies, utilities and governments.

5.1 Case 1
A company providing payroll services, with approximately 120 staff, was asked by one of its clients to obtain certification within twelve months, otherwise the client would take its work elsewhere. The contract was worth £3m per annum.

The company used consultants to undertake most of the work setting up the ISMS which entailed agreeing scope, identifying relevant assets and undertaking a risk analysis. At this point serious involvement was needed from senior management.

During the process the company found significant improvements in their working practices, including the fact that training and awareness presentations at induction were helping to reduce the turnover of staff. In addition, the company has been able to tender for other clients where ISO 27001 certification has been a pre-requisite.

The process needed 25-30 consultancy days, and time spent internally of about two days per week, prior to certification. Had the company undertaken most of the work itself, consultancy time would have been more than halved. On-going maintenance of the mature ISMS requires approximately six days a year.

5.2 Case 2
A company, with approximately 10 staff, providing network security audits and penetration tests decided that as their work involved access to sensitive areas on clients’ systems, it would be a good demonstration of their commitment to information security to obtain certification.

During the preparation process the company found that the formalising of procedures that had previously been informal and ad hoc improved the overall knowledge of essential activities amongst key people. With an increase in staff levels, formal procedures have been essential to bring new staff up to speed.

An additional benefit is that the company can respond to government, health service and major company tenders without having to give a detailed description of how it manages information security. Demonstration of formal certification is enough.

The process took about 20 days of senior management involvement, with about five days of consultancy to guide the process.

5.3 Case 3
As part of its commitment to sound corporate governance, a two man business decided to extend the scope of its existing ISO 9001 certified management system, designed using hypertext, to encompass ISO/IEC 27001.

In addition to ISO 9001, the company had already structured its management system in accordance with the recommendations of the UK Audit Practices Board for sound internal control. Thus, the internal controls addressed all
aspects of the company’s business and had been selected on the basis of a risk assessment.

The company performed the changes necessary to comply with ISO/IEC 27001 without any external assistance. It took a mere six days to complete. Certification was carried out soon after the company now enjoys a combined audit covering both ISO 9001 and ISO/IEC 27001. Since the records are hyperlinked into the management system, everything that the certification auditor wants to see, and indeed the company itself, is very easily accessible being just ‘one click away’. This enables the auditor to complete their work on both standards in one day.

5.4 Case 4
The IT department of a Middle East telecommunications company decided to opt for ISO/IEC 27001 certification as a means to further improve its approach to information security, and distinguish the company as a whole from future competition in its region of operations.

The company first used a consultant to determine how to apply the standard across the whole organisation and to devise an appropriate implementation plan. The company then requested the consultant to implement the ISMS for the IT department and train their staff how to operate, maintain and improve it.

During the process the IT security department learnt how to marry its quest for technical excellence with commercial realities, making it better able to gain management commitment to information security.

The initial scoping study took 15 consultancy days and the build process for the IT department’s ISMS, including putting it and the organisation in a state of readiness for certification, took 26 consultancy days. The ability of the consultant to build the ISMS with only review and approval effort from the client owes much to the company’s prior investment in documenting its processes and procedures for ISO 9000.

5.5 Case 5
A government of a small Commonwealth country decided that it was strategically important for each ministry within its civil service to comply with ISO/IEC 27001 as a prerequisite for establishing e-commerce as a new pillar of the country’s economy.

The Ministry of IT and Telecommunications used consultants to teach its staff how to apply the standard, to assist them to build ISMSs for four pilot sites and devise a rollout plan for the rest of the civil service. The pilot sites were the Treasury, the Passport and Immigration Office, the branch of the Prime Minister’s Office responsible for the registration of births, marriages and deaths, and the Ministry of Social Security.

The senior civil servants responsible for these ministries/departments personally led their own teams of civil servants to build their respective ISMSs. Two years on, these systems are still fully operational and their owners remain proud of their achievements. The Ministry of IT and Telecommunications is rolling out the standard to other ministries, including itself, without consultancy support.

The project consumed about 100 consultancy days. The time spent by the pilot sites was concentrated over a two month period and was intensive. The
senior civil servants involved publicly proclaimed that this was a worthwhile investment and indeed the Ministry of IT and Telecommunications observed that awareness of information security and the consequent adoption of best practice had increased significantly. The time from when the senior civil servants were first trained in the standard and certification was a shade under four months for each pilot site.
DEFINITIONS

Availability
The property of being accessible and useable upon demand by an authorised entity.

Confidentiality
The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Integrity
The property of safeguarding the accuracy and completeness of assets.

Malware
A collective name for any sort of software which seeks to cause damage or inconvenience e.g. viruses, spyware, Trojan horses etc.
A.1 Accreditation
Accreditation for certifying bodies is given by an Accreditation Body. In the UK the body is the UK Accreditation Service (UKAS).

Accreditation of CBs for management systems is governed by international criteria which cover, inter alia, the following aspects of the CB:

- Ownership;
- Organisation;
- Quality control procedures;
- Conflict of interests;
- Independence.

There are also criteria relating to specific skill requirements and audit tasks associated with the audit for conformance to specific management system standards. The general criteria are similar to, and cover the same ground as, the audit standards issued by ICAEW and other Institutes.

The general criteria ISO/IEC 17021 apply and the specific amplifications for ISO/IEC 27001 are set out in ISO/IEC 27006.

A.2 Auditor qualifications
Individual auditors may also be certified by the International Register for Certified Auditors (IRCA). Auditors are certified to perform audits against specific standards.

For 27001 IRCA has a qualification scheme for four grades of auditor: ISMS Provisional Auditor; ISMS Auditor; ISMS Lead Auditor; ISMS Principal Audit.

In principle the qualification scheme is not dissimilar from the accountancy training for audit, except it is focused on the one standard. CBs, and others, also run training courses for auditors.

ISO also publishes standards for the conduct of audits – ISO/IEC 19011. This standard contains similar material to ICAEW documents on auditing.
APPENDIX

SOURCE OF FURTHER INFORMATION

British Computer Society
1st Floor, Block D
North Star House
North Star Avenue
Swindon,
Wiltshire UK, SN2 1FA
01793 417424 Customer services 0845 300 4417
www.bcs.org

BSI
389, Chiswick High Road
London W4 4AL
020 8996 9001
www.bsigroup.co.uk – BSI management system services and solutions

Certification bodies
A list of certification bodies can be found at
www.ukas.com/about_accreditation/accredited_bodies/certification_body_schedules.asp

Certified organisations
A list of certified organisations can be found at
www.iso27001certificates.com

Department for Business Innovation and Skills
Communications and Content Industries Directorate
Information Security Policy Team
1–19 Victoria Street
London SW1H 0ET
Fax 020 7215 5442
E-mail infosecpolicyteam@berr.gsi.gov.uk
www.berr.gov.uk/whatwedo/sectors/infosec
Infosec Health Check Tool: www.securityhealthcheck.berr.gov.uk

Gamma Secure Systems Limited
Diamond House,
149 Frimley Road
Camberley
Surrey GU15 2PS
01276 702500
Papers supporting the integration of information security into internal control.
www.gammassl.co.uk

International Register of Certificated Auditors (IRCA)
12 Grosvenor Crescent
London SW1X 7EE
020 7245 6833
www.irca.org
ISMS user groups
Information about the ISMS user groups can be found at www.xisec.com

United Kingdom Accreditation Service (UKAS)
21–47, High Street
Feltham
Middlesex
TW13 4UN
020 8917-8400
www.ukas.com

NOTE: all telephone numbers are for the UK – from overseas replace the first 0 with 0044.
THE AUTHORS

William List CA hon FBCS CITP Deceased

William List qualified as a Chartered Accountant and specialised in computer audit and security for over 40 years. He was a computer audit (now IRMA) partner in KPMG based in London.

He was a member of the UK Standards Committee which developed the Information Security Management Standards ISO/IEC17799 and ISO/IEC 27001:2005 and monitors all the extant and developing ISO Information Security standards. He had been researching the linkage between information security, assurance and the internal control component of Corporate Governance.

He was a past chairman of the British Computer Society (BCS) standing security expert panel and served on various BCS and accounting Institutes’ committees for 30 years. He was a member of the Institute of Chartered Accountants of England and Wales IT Faculty Committee and IT Faculty Technical Committee.

David Brewer PhD BSc MIOD

Dr. David Brewer is a director of Gamma Secure Systems Limited, Camberley. He was one of the first consultants to provide computer security advice to the British Government (1982), a co-author of the European IT Security Evaluation Criteria (now ISO/IEC 15408) and a co-author of BS 7799-2:2002 (now ISO/ IEC 27001). He is an internationally recognised information security consultant and has published numerous research papers. He has more than 28 years experience in IT, 23 of which have been in information security and has worked on numerous software engineering and information security assignments on a world-wide basis.

Dick Price FCA QICA FIIA

Dick Price has over 30 years experience in computer security and audit, originally qualifying as a Chartered Accountant and subsequently gaining the Qualification in Computer Auditing promoted by the Institute of Internal Auditors, who subsequently awarded him a Fellowship.

He undertakes a wide variety of computer audits and information security reviews, including mainframe, minicomputer and client-server environments. He also increasingly provides consultancy support to organisations that are implementing ISO 27001 (Information Security Management Systems).

Dick has been instrumental in helping to raise awareness of the need for Information Security Management and is the Institute of Internal Audit’s representative at the IST/33 committee for the ISO 27000 series of standards. He is a long-standing member of the Qualification in Computer Audit Committee of the IIA-UK and Ireland.