An Introduction to ISO/IEC 27001:2013
An Introduction to
ISO/IEC 27001:2013

Dr David Brewer
Contents

Foreword vii
Acknowledgements ix

Chapter 1 - Information security management systems 1
Introduction 1
Definitions 1
Purpose and benefits 4
Understanding ISO/IEC 27001 8
Structure of ISO/IEC 27001 11
ISO/IEC 27001's relationship with other standards 15
Certification 16

Chapter 2 - Management system-specific requirements 19
Introduction 19
Definitions 22
How an information security management system works 24
Scope of the information security management system 29
Policy and objectives 37
Risks and opportunities 42
Operation 44
Monitoring, measurement, analysis and evaluation 46
Audits and reviews 55
Management and support 62

Chapter 3 - Information security-specific requirements 77
Introduction 77
Definitions 79
Risk assessment 80
Risk treatment 87
Determining controls 94
The Statement of Applicability 99
Effective risk treatment plans 105

Chapter 4 - Implementation guidance 108
Introduction 108
Implementation strategies 109
Preparation and project planning 111
Documented information 114
Choice of documentation media 116
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessment methods</td>
<td>117</td>
</tr>
<tr>
<td>Determining controls in practice</td>
<td>127</td>
</tr>
<tr>
<td>Critical risks</td>
<td>129</td>
</tr>
<tr>
<td>Overarching and subordinate management systems</td>
<td>130</td>
</tr>
<tr>
<td>Dos and don’ts</td>
<td>131</td>
</tr>
<tr>
<td><strong>Compendium of definitions</strong></td>
<td>135</td>
</tr>
<tr>
<td><strong>Bibliography</strong></td>
<td>139</td>
</tr>
<tr>
<td>Standards publications</td>
<td>139</td>
</tr>
<tr>
<td>Other publications</td>
<td>141</td>
</tr>
</tbody>
</table>
Foreword

ISO/IEC 27001:2013 is the requirements specification standard for an information security management system, or ISMS for short. With more than 17,000 registrations worldwide, it defines the internationally accepted way to manage information security in your organization. You can use it to manage your exposure to information security risk, which is good governance, and to give confidence to others that you do, which is called market assurance.

Since the standard was first published as an ISO standard in 2005, sweeping changes have been made, as all new and revised management system standards have to conform to new ISO directives concerning layout and content. The standard has also been updated to align it with new ISO risk management principles, and to reflect the lessons learnt worldwide in using ISMSs. However, whilst the new standard is very clear about specifying what must be done to create and use an ISMS, implementation is beyond the remit of the document. To compensate for this, this book is full of practical how-to guidance.

It explains the new requirements and provides fresh insights into understanding management systems in general and ISMSs in particular. It gives advice on risk assessment and risk treatment, a clear explanation of the purpose of the ‘Statement of Applicability’ (SOA) and advice on determining controls in practice. There is also guidance on assessing information security performance and the effectiveness of the ISMS processes.

This book has been designed so that you can read it from cover to cover to gain a comprehensive understanding of the new standard, and then later use it as a reference book.

I have more than 15 years’ worldwide experience in working with ISMSs as a standards maker, consultant, auditor, tutor and management system administrator, my first involvement being with the development of the preceding British ISMS standards, BS 7799-2:1998, BS 7799-2:1999 and BS 7799-2:2002. The advice that I have given in this book is derived from this practical experience, supplemented by the insights afforded by being a member of the international ISO/IEC 27001:2013 development team. The advice that I offer here has been tried and tested over many years and has met with the approbation of many organizations and certification bodies. This book is a ‘must-have’ for organizations and
Foreword

individuals keen on having a straightforward overview of the new ISMS standard and practical guidance on how to implement it.

David Brewer
Acknowledgements

Figures 2, 3, 5, 10, 11, 12, 13, 14, 17, 18 and Table 5 have been reproduced by kind permission of IMS – Smart Limited.
Chapter 1 - Information security management systems

Introduction

The aim of this chapter is to provide an understanding of what a management system is and how to interpret a management system standard. The chapter also introduces the subject of certification.

The remainder of this chapter is laid out in the following subsections:

• definitions;
• purpose and benefits;
• understanding ISO/IEC 27001;
• structure of ISO/IEC 27001;
• ISO/IEC 27001’s relationship with other standards; and
• certification.

Definitions

ISO/IEC 27000 defines the terms used in ISO/IEC 27001, together with their sources. Those that are fundamental to understanding management system concepts in general are reproduced and discussed here. Other definitions are reproduced and discussed in Chapter 2 or Chapter 3 as appropriate. If a term is not defined in ISO/IEC 27000, then the definition given in the Oxford English Dictionary (in this case, in this book, as found in its online edition on Oxford Dictionaries Online) is to be used. It is important to use these definitions, otherwise there is a risk of misunderstanding the requirements of the standard.

The definitions necessary for an understanding of this chapter are:

management system: ‘set of interrelated or interacting elements of an organization...to establish policies...and objectives...and processes...to achieve those objectives...’


organization: ‘person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives...’

ISO/IEC Directives, Part 1, Annex SL, Appendix 3, Clause 3.01
**Chapter 1 - Information security management systems**

**top management:** ‘person or group of people who directs and controls an organization...at the highest level...’

ISO/IEC Directives, Part 1, Annex SL, Appendix 3, Clause 3.05

**policy:** ‘intentions and direction of an organization...as formally expressed by its top management...’

ISO/IEC Directives, Part 1, Annex SL, Appendix 3, Clause 3.07

**objective:** ‘result to be achieved...’

ISO/IEC Directives, Part 1, Annex SL, Appendix 3, Clause 3.08

**process:** ‘set of interrelated or interacting activities which transforms inputs into outputs’

ISO/IEC 27000:2012, Clause 2.54

**documented information:** ‘information required to be controlled and maintained by an organization...and the medium on which it is contained...’

ISO/IEC Directives, Part 1, Annex SL, Appendix 3, Clause 3.11

It is important to appreciate that an organization does not have to be a company. Indeed, there is a note to the definition, which says: ‘The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private’ (ISO/IEC Directives, Part 1, Annex SL, Appendix 3, Clause 3.01). It therefore follows that if the organization is part of a larger organization then, from the perspective of the smaller organization:

- the larger organization is referred to as either ‘another organization’ or an ‘external organization’, the two phrases being synonymous with one another;
- top management refers to the leader(s) of the smaller organization, not to the leader(s) of the larger organization.

This relationship is illustrated in Figure 1.

In order to gain further insight into the definition of a management system, consider the following.

- *Oxford Dictionaries Online* provides a number of meanings for the word ‘of’, the most relevant of which is ‘indicating an association between two entities, typically one of belonging, in which the first is the head of the phrase and the second is something associated with it...’. Thus, for example, one might say ‘the information security policy of ABC incorporated’.
- There will be people within the organization that will establish policy. Indeed, top management is responsible for establishing the
information security policy (see Clause 5.2). However, if a management system was only made up of people, the definition would say ‘a person or group of people with the organization that establishes…’. The definition does not refer to people. Instead it refers to ‘…interrelated or interacting elements…’ (ISO/IEC Directives, Part 1, Annex SL, Appendix 3, Clause 3.04).

• An ‘element’, according to Oxford Dictionaries Online, is ‘an essential or characteristic part of something abstract…’, so it is more than just people. However, these elements cannot be just anything that is associated with the organization; they have to establish policy, objectives and processes to achieve those objectives, perhaps directly or through interaction with other elements.

• ‘Establish’, according to Oxford Dictionaries Online, means to ‘set up on a firm or permanent basis…’. Accordingly, an information security policy document would be part of the ISMS, as are top management and the information security controls.

The final remark about the inclusion of information security controls in the ISMS may come as a surprise for some people, but the validity of this conclusion can be derived from the new ISO definition of a management system. Some controls (e.g. firewalls) certainly enforce policy. Indeed, the sole detailed definition of such policy may reside only within the technology used to implement the control. However, all controls can be considered as working together to establish a process that attempts to transform unsafe actions into safe ones (where an unsafe action is one that does not preserve the confidentiality, integrity or availability of information within the scope of the ISMS). Thus, given the new ISO
Chapter 1 - Information security management systems

definition of a management system, the information security controls ought to be considered as being part of the ISMS.

In conclusion, our interpretation of the ISO definition of an ISMS is:

   everything that is associated with the organization that interacts to establish information security policy, information security objectives and information security processes to achieve those objectives.

‘Documented information’ is a new term that has been traditionally referred to as documentation and records. A good way to think of this is that there are two types of documented information:

• specifications, which specify what an organization intends to do (i.e. in the future); and
• records of performance, which record what has happened (i.e. in the past).

As an item of documentation, e.g. a web page, could contain both types, ISO has decided to use a single term to cover both documentation and records.

It is also important to note that it ought now to be very rare that a management system standard gives names to documents. ISO/IEC 27001, Clause 5.2 starts by stating ‘Top management shall establish an information security policy…’ and continues by requiring that policy to have certain characteristics, e.g. it ‘includes a commitment to continual improvement of the information security management system’ (ISO/IEC 27001, Clause 5.2 d). The clause also states that the policy ‘be available as documented information’ (ISO/IEC 27001, Clause 5.2 e). This is not a requirement to have a document called ‘information security policy’. It is a requirement that the information specified in Clause 5.2 be documented. How an organization does this, and how it wants to refer to it, is up to the organization to decide and no one else. It could, for example, put the information required by Clause 5.2, together with other information (whether required elsewhere by the standard or not), on an intranet web page entitled ‘Integrated management system policy’.

Purpose and benefits

Reasons to have an ISMS

There are various reasons why organizations seek to have an ISMS. These seem to fit broadly into two categories: market assurance and governance. Market assurance concerns the ability of an ISMS to inspire confidence, within the marketplace, in an organization’s ability to look after information securely. In particular, it inspires confidence that the organization will preserve the confidentiality, integrity and availability of
customer information. Governance concerns how organizations are managed. In this case, an ISMS is recognized as a proactive way to manage information security.

The two categories are clearly related. An organization may choose to have an ISMS in order to inspire confidence within the marketplace. Once it has its ISMS, as it matures, the people within the organization may experience the benefits of being able to better manage information security. Thus, the organization’s reasons for having an ISMS may expand to cover both market assurance and governance. Likewise, another organization might start out by having an ISMS for reasons of better management. However, as its ISMS matures, it may communicate its experiences and news concerning successful certification audits to the marketplace and learn the power of market assurance to attract new customers.

**Market assurance**

A typical scenario is when a company demands various assurances from its suppliers in order for them to continue as suppliers to that company. The norm used to be that such companies would require their suppliers to conform to ISO 9001, but now companies are also seeking assurances from their suppliers with regards to ISO/IEC 27001.

In the case of quality, if the company incorporates, or otherwise uses, the products and services of its suppliers into its own offerings, then the quality of those offerings also depends on the quality of the suppliers’ products and services. Likewise with regards to information security, the company will have a duty of due care to preserve the security of the information in its custody. If that information is shared with a supplier, then the company would be failing in its duty of care if the supplier’s handling of that information was insecure. It matters not if the company seeks to do this for reasons of governance or market assurance, it only matters that it does.

As a supplier may be part of a chain, it is easy to see how the requirement for information security ripples down to even the smallest organizations.

Another scenario is when a supplier seeks to have an ISMS in anticipation that a customer may require it, or to distinguish itself from its competition.
Chapter 1 - Information security management systems

Governance

All organizations have a system of internal control, whether it is formal or informal. It is the means by which top management marshals the organization’s resources to achieve its objectives.

There are two parts to a system of internal control: the part for doing the job; and the part for doing the job the way top management wishes.

In the wake of a series of UK reports that dealt with the conduct in the boardrooms of UK organizations, the UK Audit Practices Board published a set of guidelines (Audit Practices Board, 2001; The Institute of Chartered Accountants in England & Wales, 1999) on the structure of a system of internal control; see Figure 2. The Audit Practices Board’s intention was to advise audit firms on how to audit, given the new requirement to consider risks other than financial risks. The advice was for audit firms first to gain empathy with the audit client’s organization by understanding the organization’s mission and business objectives. Only then could the audit firm start to identify the business risks. Not all of these would be applicable to the organization, for example because the consequence and/or likelihood would be very low. Having identified the applicable risks, the audit firm could then proceed to identify the associated internal controls and review them for effectiveness. Recommendations, once implemented, would then be fed back into the risk assessment process.

![Figure 2: The UK Audit Practices Board’s model of internal control](image)

There is a similarity in this model with the concept of continual improvement embodied in ISO management system standards. Indeed, one way to regard a management system standard is that it provides a
particular perspective on a system of internal control. For example, ISO/IEC 27001 considers that part of internal control which is concerned with information security risk; see Figure 3. The overlap represents the common components of these standards, and is now referred to by ISO as the identical core text (see ‘Identical core text, discipline-specific text and deviations’, below). These common components, augmented by risk assessment/treatment processes (such as those of ISO/IEC 27001), form an ideal 'engine' to drive all systems of internal control. This is because of the formalized structure that such standards bring to the Audit Practices Board’s model, providing top management with a proactive, continual improvement, management method to assist them to achieve their organization’s objectives.

Information security management system benefits

One of the key benefits of a management system is that it encourages organizations to look ahead and take action to prevent bad things from happening to them. It does this by requiring organizations to assess and treat the risks that may arise and affect their ability to achieve their intended outcomes. This is not a one-off activity. Organizations are required to perform the risk assessment and risk treatment processes at planned intervals, and when significant changes are proposed or occur.

The approach to risk assessment is very flexible, allowing organizations to select the approach that works best for them. For example, an organization can use a method that will work across disciplines, such as finance and quality, in addition to information security, if it wants to.
Organizations are required to determine their own risk criteria against which to assess their risks.

Taken together, these requirements facilitate a proportionate and dynamic approach to information security: proportionate in that controls are appropriate to the organization’s appetite for risk, and dynamic in response to ever changing threats on the horizon and changes in organizational direction and objectives.

However, all organizations that conform to the standard are required to consider the same set of 114 controls and justify their inclusion or exclusion from their risk treatment plan. This allows quite diverse organizations to be compared against a common standard. It provides a common language for describing information security controls, allowing one organization to understand what another has done.

Another key benefit is that an ISMS encourages organizations to take stock of their achievements, to question the effectiveness of their ISMS and to make changes accordingly. There are requirements for management review and internal auditing, but once again these are intended to be appropriate to the organization’s needs.

Understanding ISO/IEC 27001

General

Management system standards define the requirements for management systems. Thus, ISO/IEC 27001 defines the requirements for an ISMS. There are a variety of observations that one can make about ISO/IEC 27001 which ought to help provide understanding on how to read and interpret the standard. These observations concern:

- the order of implementation;
- conformance;
- self-healing properties;
- alternative requirements;
- impartiality;
- duplicated requirements; and
- notes.

Certification is outside the scope of ISO/IEC 27001, or indeed any other management system standard. The subject is nevertheless within the scope of this book and is introduced in the final section of this chapter.

Requirements can be implemented in any order

The introduction to ISO/IEC 27001 (Clause 0.1) states:
‘The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.’

This means that the requirements can be implemented in any order. The implementation strategies discussed in Chapter 4 make particular use of this property.

For conformance all requirements must be met

The standard also states (Clause 1):

‘Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this International Standard’.

This means that for conformity with the standard, an ISMS must conform to all the requirements in Clauses 4 to 10. In particular, if at some point during the life of the ISMS something changes so that a requirement is no longer met, then the ISMS as a whole no longer conforms.

An ISMS that conforms is self-healing

Clause 10 contains requirements for taking action to identify and correct nonconformities. These have the effect of making the ISMS self-healing. It is as if, as soon as part of the ISMS no longer conforms, the corrective action requirements spring into action to correct the nonconformity, thereby rendering the whole ISMS in conformance once again. Viewed in this way the life of the ISMS is a sequence of conformity – nonconformity – corrective action – conformity and so on.

It does not matter if the organization knows about one or more nonconformities at the time of a certification audit, provided that it is dealing with them in accordance with the requirements of Clause 10. From a certification perspective, it is a good opportunity to see the corrective action component of the ISMS in action.

Alternative requirements

Take care when reading lists. If the list ends with the word ‘or’ it means that the ISMS must conform to at least one item in the list (i.e. the use of the word ‘or’ should be interpreted as meaning ‘and/or’). If it ends with the word ‘and’ it means that the ISMS must conform to every item in the list. For example:
• ISO/IEC 27001, Clause 7.2 b) states ‘ensure that these persons are competent on the basis of appropriate education, training, or experience’. This means that people are required to be competent on the basis of appropriate education and/or training and/or experience. Thus, someone might be competent on the basis of education and training, whilst someone else might be competent simply on the basis of their experience.

• ISO/IEC 27001, Clause 9.3 states ‘Top management shall review the organization’s information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness’. If it transpires that the ISMS is no longer suitable or adequate (or effective), then the ISMS would not conform with this clause.

Impartiality

The standard may at first view appear somewhat bland. This is because the intention is only to state what shall be done, not how it might be done. If the latter type of requirement were to appear in a management system standard it would force all organizations to do it that way, and that may not be the best way for all organizations. ISO/IEC 27001 therefore aims to be impartial, showing no preference for a particular method. Guidance, however, is provided in other standards in the 27000 series (see the penultimate section of this chapter: ‘ISO/IEC 27001’s relationship with other standards’) and in books such as this.

Duplicated requirements

Care has also been taken to ensure that requirements are only stated once. This is because there is a danger that duplicated requirements at best confuse and at worst contradict.

It is now ISO practice, for example, to state the requirement for documented information within the clause, or group of clauses, to which it relates. For instance, Clause 4.3 states the requirements for determining the scope of the ISMS. The final paragraph states ‘The scope shall be available as documented information’ (ISO/IEC 27001, Clause 4.3). Thus, the requirements for documented information are to be found throughout the standard. They are not, however, also collated into one place as that would give rise to duplication.

Notes

A note in an ISO management system is intended to assist readers to understand a requirement. It does not modify the requirement, or imply
that a particular way of meeting the requirement is itself a requirement. A sure test of one’s understanding of a note is that the requirement should not change if the note was ignored.

Structure of ISO/IEC 27001

The new ISO directives

Since April 2012 all new and revised management system standards must conform to new rules regarding the structure and content of management system standards. The objective is to ensure that when a requirement ought to be common to more than one management system standard that it is identically worded. This has benefits when an organization wishes to have a single management system (often referred to as an integrated management system) that conforms to more than one management system standard. For example, an integrated management system might conform to ISO 9001 (quality), ISO/IEC 27001 (information security) and ISO 22301 (business continuity). In this case (once all three standards conform to the new directives), the core requirements, say for documented information, will be identically worded.

High-level structure

The high-level structure for all new and revised management system standards is the same. The structure of ISO/IEC 27001, which is shown below, conforms to this high-level structure.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Introduction</td>
</tr>
<tr>
<td>1</td>
<td>Scope</td>
</tr>
<tr>
<td>2</td>
<td>Normative references</td>
</tr>
<tr>
<td>3</td>
<td>Terms and definitions</td>
</tr>
<tr>
<td>4</td>
<td>Context of the organization</td>
</tr>
<tr>
<td></td>
<td>4.1 Understanding the organization and its context</td>
</tr>
<tr>
<td></td>
<td>4.2 Understanding the needs and expectations of interested parties</td>
</tr>
<tr>
<td></td>
<td>4.3 Determining the scope of the information security management system</td>
</tr>
<tr>
<td></td>
<td>4.4 Information security management system</td>
</tr>
<tr>
<td>5</td>
<td>Leadership</td>
</tr>
<tr>
<td></td>
<td>5.1 Leadership and commitment</td>
</tr>
<tr>
<td></td>
<td>5.2 Policy</td>
</tr>
<tr>
<td></td>
<td>5.3 Organizational roles, responsibilities and authorities</td>
</tr>
<tr>
<td>6</td>
<td>Planning</td>
</tr>
</tbody>
</table>
6.1 Actions to address risks and opportunities
6.1.1 General
6.1.2 Information security risk assessment
6.1.3 Information security risk treatment
6.2 Information security objectives and planning to achieve them

7 Support
7.1 Resources
7.2 Competence
7.3 Awareness
7.4 Communication
7.5 Documented information
7.5.1 General
7.5.2 Creating and updating
7.5.3 Control of documented information

8 Operation
8.1 Operational planning and control
8.2 Information security risk assessment
8.3 Information security risk treatment

9 Performance evaluation
9.1 Monitoring, measurement, analysis and evaluation
9.2 Internal audit
9.3 Management review

10 Improvement
10.1 Nonconformity and corrective action
10.2 Continual improvement

Identical core text, discipline-specific text and deviations

The requirements that are identical to all new and revised management system standards are known collectively as the identical core text. Requirements that are specific to a particular discipline (e.g. information security) are referred to collectively as discipline-specific text. Such text may be embedded in the identical core text.

As an aid to readability, some identical core text requirements are prefaced by the subject name of the standard, e.g. the words ‘information security’. These requirements are not ‘quality’ or discipline-specific.

If the identical core text is changed in a way that is not discipline-specific (i.e. the change would be equally meaningful in other disciplines), then it is called a deviation. ISO has permitted deviations in those standards produced immediately after the publication of the new directives. ISO/IEC 27001 does contain some deviations. These are identified in Table 1. Embedded information security-specific text is also identified in Table 1.
1, marked with an asterisk. Note that this table refers only to the ISMS requirements, i.e. to Clauses 4 to 10, and not to notes. Please also note that the identical core text quoted is taken from ISO/IEC Directives, Part 1 (2013), Annex SL, Appendix 3.

Much of ISO/IEC 27001 consists of identical core text. This is the subject of Chapter 2.

The bulk of the discipline-specific text is concentrated in Clauses 6.1.2, 6.1.3, 8.2 and 8.3. This is the subject of Chapter 3.

<table>
<thead>
<tr>
<th>ISO/IEC 27001 Clause</th>
<th>Change or addition</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2 b)</td>
<td>The words ‘relevant to information security’ have been added.</td>
</tr>
<tr>
<td>4.3 c)</td>
<td>The list item ‘c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.’ has been added.</td>
</tr>
<tr>
<td>4.4</td>
<td>The phrase ‘including the processes needed and their interactions’ has been deleted.</td>
</tr>
<tr>
<td>5.1 b)</td>
<td>The word ‘business’ has been deleted together with the note that explains what a business process is.</td>
</tr>
<tr>
<td>5.2 b)</td>
<td>The words ‘includes information security objectives (see 6.2) or’ have been added.</td>
</tr>
<tr>
<td>5.2 c)</td>
<td>The words ‘related to information security’ have been added.</td>
</tr>
<tr>
<td>5.3</td>
<td>The requirement has been changed to read ‘Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.’ The original identical core text read ‘Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.’</td>
</tr>
<tr>
<td>6.2 c)</td>
<td>The words ‘information security’ have been added.</td>
</tr>
<tr>
<td>7.4</td>
<td>Two new list items ‘d) who shall communicate; and e) the processes by which communication shall be effected.’ have been added.</td>
</tr>
<tr>
<td>8.1 (1st paragraph)</td>
<td>The identical core text completes the sentence with the word ‘by’, followed by two bullet points: ‘— establishing criteria for the processes — implementing control of the processes in accordance with the criteria’. All of this has been deleted and the third bullet point turned into a stand-alone sentence.</td>
</tr>
<tr>
<td>ISO/ IEC 27001 Clause</td>
<td>Change or addition</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td></td>
<td>The words ‘information security’ have been added.</td>
</tr>
<tr>
<td>8.1 (2nd paragraph)</td>
<td>In the identical core text, this sentence is a bullet point. Two previous bullet points have been deleted.</td>
</tr>
<tr>
<td>8.1</td>
<td>The sentence ‘The organization shall also implement plans to achieve information security objectives determined in 6.2.’ has been added.</td>
</tr>
<tr>
<td>9.1 (1st paragraph)</td>
<td>The first paragraph is pure identical core text, but it has been moved from the end of section 9.1 to the beginning of the clause.</td>
</tr>
<tr>
<td>9.1 (list)</td>
<td>A note has been added after b): ‘The methods selected should produce comparable and reproducible results to be considered valid.’</td>
</tr>
<tr>
<td>9.1 (list)</td>
<td>A new list item ‘d) who shall monitor and measure;’ has been added.</td>
</tr>
<tr>
<td>9.1 (list)</td>
<td>A new list item ‘f) who shall analyse and evaluate these results;’ has been added.</td>
</tr>
<tr>
<td>9.1 (last paragraph)</td>
<td>The words ‘monitoring and measurement’ have been added to what is now the final paragraph of this clause.</td>
</tr>
<tr>
<td>9.3 c)</td>
<td>The word ‘feedback’ is used instead of ‘information’ to avoid saying ‘…information on the information…’.</td>
</tr>
<tr>
<td>9.3 c)</td>
<td>A new list item ‘4) fulfilment of information security objectives;’ has been added.</td>
</tr>
<tr>
<td>9.3 d)</td>
<td>A new list item ‘d) feedback from interested parties;’ has been added.</td>
</tr>
<tr>
<td>6.2 c)*</td>
<td>The words ‘and risk assessment and risk treatment results’ have been added.</td>
</tr>
<tr>
<td>9.1 a)*</td>
<td>The words ‘including information security processes and controls’ have been added.</td>
</tr>
</tbody>
</table>
ISO/IEC 27001’s relationship with other standards

- ISO/IEC 27000 provides an overview of all the standards in the 27000 series, together with the vocabulary of terms that they use. The principal standards are:
- ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary;
- ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements;
- ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance;
- ISO/IEC 27005, Information technology — Security techniques — Information security risk management;
- ISO/IEC 27006, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems;
- ISO/IEC 27007, Information technology — Security techniques — Guidelines for information security management systems auditing;
- ISO/IEC TR 27008, Information technology — Security techniques — Guidelines for auditors on information security controls;
- ISO/IEC 27010, Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications;

Table 1: Deviations and embedded information-security specific text

<table>
<thead>
<tr>
<th>ISO/IEC 27001 Clause</th>
<th>Change or addition</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.3*</td>
<td>A new list item 'e) results of risk assessment and status of risk treatment plan; and' has been added.</td>
</tr>
</tbody>
</table>

ISO/IEC 27001’s relationship with other standards
Chapter 1 - Information security management systems

- ISO/IEC DTR 27016, Information technology — Security techniques — Information security management — Organizational economics;
- ISO/IEC WD 27017, Information technology — Security techniques — Code of practice for information security controls for cloud computing services based on ISO/IEC 27002;
- ISO/IEC CD 27018, Code of practice for data protection controls for public cloud computing services;

The definitive standards are ISO/IEC 27001 and ISO/IEC 27002. Traditionally, these are revised and republished at the same time. If a supporting standard has an earlier publication date then it will be aligned to the 2005 versions of ISO/IEC 27001 and ISO/IEC 27002.

Certification

Certification is a process to confirm conformity with a standard. Third-party certification is performed by a certification body and, if it is accredited, it will perform those certifications in conformance to ISO/IEC 27006. Accredited certification is only offered in respect of a management system standard, e.g. ISO/IEC 27001, ISO 9001, ISO 14001 etc.

The process starts with an initial audit, which is conducted in two stages. The objective of the stage 1 audit is for the certification body to gain an understanding of the ISMS in the context of the client organization's ISMS policy and objectives, and, in particular, of the client organization's state of preparedness for the audit. In doing so, the certification body will review the documented information that is required by the standard (see Chapter 4 ‘Documented information’). If requirements are met, the initial audit is likely to proceed to its second stage.

The objectives of the stage 2 audit are:

a) to confirm that the client organization adheres to its own policies, objectives and procedures; and
b) to confirm that the ISMS conforms to all the requirements of ISO/IEC 27001 and is achieving the client organization’s policy objectives.

Assuming that no nonconformities are found (or if there are, they are corrected to the satisfaction of the certification body), the organization will be certified. Thereafter, the organization will be subject to regular ‘surveillance’ audits which have the objective of ensuring that conformance is being maintained. These audits are usually performed...
every six months, although for very small organizations they may be conducted annually. Every three years there is a ‘recertification’ audit, which may be regarded as a repeat of the original stage 2 audit. The objective is to confirm the continued conformity and effectiveness of the ISMS as a whole, and its continued relevance and applicability for the scope of certification.
