FAQ

How the changes to ISO/IEC 27001 affect you

A new version of the Standard for Information Security Management, ISO/IEC 27001 has been released. This guide is aimed at helping you understand the changes and how they may impact on organisations currently certified to ISO/IEC 27001:2005, or contemplating implementation of the Standard. Significant differences between the old and new versions of the Standard will be highlighted.

Changes to the structure of the Standard

The basic structure has been revised to align with Annex SL to Part 1 of the ISO/IEC Directives. It is intended that all management system Standards will adopt this format at their next revision. The major Clause numbers and titles of all ISO management system Standards will be the same while the introduction, scope and normative references will include details specific to the discipline. This will introduce further consistency for organisations that have integrated management systems that cover multiple Standards, such as ISO 9001, Quality Management Systems and ISO 14001, Environmental Management Systems.

ISO/IEC 27001 is the first Standard to adopt the Annex SL structure. The 2013 Standard looks very different to the 2005 version. To help understand the differences, a cross reference table from between the two versions has been included below.

The structure of the ISO/IEC 27001:2013 is as follows:

0 Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Context of the organisation
5 Leadership
6 Planning
7 Support
8 Operation
9 Performance evaluation
10 Improvement

Clauses of ISO/IEC 27001:2013 in more detail

0 Introduction

The Plan-Do-Check-Act section has now been removed, however Clause 10 still requires continual improvement.

1 Scope

There is a stronger focus on assessment and treatment of risks tailored to meet the needs of the organisation. Exclusions to Clauses 4 to 10 are not permitted, however it does not refer to exclusions of controls in Annex A.

2 Normative references

ISO/IEC 27001 is listed as the only normative reference. The Code of Practice, ISO/IEC 27002, is not listed as a normative reference as it was in the previous version.

3 Terms and definitions

Terms and definitions have been removed from the Standard and reference is now made to ISO/IEC 27000:2012.

4 Context of the organisation

This is a new Clause that requires the organisation to determine external and internal issues and a Note makes reference to ISO 31000:2009, Risk management—Principles and guidelines (4.1). The needs and expectations of interested parties are to be determined (4.2). The scope of the ISMS needs to consider the issues identified and the requirements of the interested parties (4.3). The requirement to continually improve the ISMS is included in 4.4.

5 Leadership

This replaces the previous Management Responsibility Clause, and sets the requirements to be met by ‘top management’. The requirements and properties for an information security policy are defined here. It is noted that where the previous version required an Information Security Management System Policy, the new version refers only to an Information Security Policy.
6 Planning

Clause 6.1.1 General - replaces previous preventive action requirements. References to issues (4.1) and requirements (4.2) are used to determine risks and plan actions to address the risks identified.

Clause 6.1.2 Information security risk assessment – the identification of assets, threats and vulnerabilities is no longer required, now requiring the identification of risks associated with the loss of confidentiality, integrity and availability. It requires risk owners to be identified, rather than asset owners.

Clause 6.1.3 Information security risk treatment – this Clause requires the selection of risk treatment options and determination of controls required to implement the risk treatment options chosen. Controls are to be compared against those in Annex A to verify that no necessary controls are omitted. A Statement of Applicability is still required and must include justification for inclusions and exclusions.

Clause 6.2 Information security objectives – this sets the requirements for information security objectives to be set a relevant functions and levels, and sets requirements for the objectives.

7 Support

Requirements for determining and providing resources, and determination of competence, awareness and communication have little change from the previous version. Requirements for control of documents and records have been revised and the Standard now refers to “documented information” and control of the documented information.

8 Operation

This Clause equates to the old “implement and operate the ISMS” and requires planning, implementing and controlling processes to achieve objectives, performing risks assessments and implementing risk treatment plans. It includes a specific requirement that outsourced processes are determined and controlled.

9 Performance Evaluation

9.1 Monitoring, measurement, analysis and evaluation – this places a stronger requirement for monitoring, measurement and analysis. The organisation is required to determine what needs to be measured, the Standard does not provide any specific requirements as to what is to be measured. Documented information is required to be retained as evidence.

9.2 Internal audit – this remains essentially the same as the 2005 version. Some requirements have been removed as they are now covered in other parts of the Standard.

9.3 Management review – the requirement for specific inputs to the review has been replaced with “shall include consideration of” and topics for outputs are no longer specified.

10 Improvement

This Clause now requires organisations to react to nonconformities and take action to control and correct them. Requirements to determine the causes of nonconformities and take action to eliminate them are essentially unchanged.

The requirement to continually improve the ISMS has been expanded to include the suitability and adequacy of the ISMS as well as the effectiveness, as in the previous version.

Annex A Controls

The number of controls has been reduced from 133 to 114, while the number of sections has increased from 11 to 14. The changes have been a result of removal of some controls, the combining of others and the introduction of some new ones.

The sections in Annex A are now as follows:

- Information security policies
- Organisation of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance
Requirements for documented information

The Standard has replaced requirements for documented procedures and records with requirements for documented information. Previously the requirements for specific documents were listed, however they are now throughout the Standard. The mandatory documented information and their Clause numbers are listed below. It is important to remember that if certification is being sought, the auditors will be looking for evidence of this information.

- ISMS scope (4.3)
- Information security policy (5.2)
- Information security risk assessment process (6.1.2)
- Information security risk treatment process (6.1.3)
- Statement of Applicability (6.1.3 d)
- Information security objectives (6.2)
- Evidence of the competence of the people (7.2)
- Documentation information determined as being necessary for effectiveness (7.5.1b)
- Operational planning and control information (8.1)
- The results of the information security risk assessments (8.2)
- The results of information security risk treatment (8.3)
- Evidence of the monitoring and measurement results (9.1)
- Evidence of the audit programme(s) and the audit results (9.2)
- Evidence of the results of management reviews of the ISMS (9.3)
- Evidence of the nature of nonconformities identified and any subsequent actions taken and corrective actions (10.1)

Annex A controls have various requirements for documented policies, procedure and records.

Where to buy the Standard?

The Standard is available through the SAI Global webshop at www.saiglobal.com/shop or by calling 131 242. You can download a PDF version instantly or order a Hardcopy of the Standard.

- ISO/IEC 27000
- ISO/IEC 27001:2013
- ISO/IEC 27002

Where can I get Training on the new Standard?

SAI Global Assurance Services will be holding a 1 hour webinar overview on the new Standard followed up by Seminars. Email your interest for training to training@saiglobal.com

Our existing training courses will be updated for 2014. They include:

- Demystifying Information Security Management
- Understanding and Implementing an Information Security Management System
- Lead Auditor in Information Security Management Systems
- Auditing Information Security Management Systems

Call 1300 727 444 to register for 2014 training


<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A.5 Information security policies</td>
<td>A.5.1 Management direction for information security</td>
</tr>
<tr>
<td>A.6 Organisation of information security</td>
<td>A.6.1 Internal organisation</td>
</tr>
<tr>
<td></td>
<td>A.6.2 Mobile devices and teleworking</td>
</tr>
<tr>
<td>A.7 Human resource security</td>
<td>A.7.1 Prior to employment</td>
</tr>
<tr>
<td></td>
<td>A.7.2 During employment</td>
</tr>
<tr>
<td></td>
<td>A.7.3 Termination and change of employment</td>
</tr>
<tr>
<td>A.8 Asset management</td>
<td>A.8.1 Responsibility of assets</td>
</tr>
<tr>
<td></td>
<td>A.8.2 Information classification</td>
</tr>
<tr>
<td></td>
<td>A.8.3 Media handling</td>
</tr>
<tr>
<td>A.9 Access control</td>
<td>A.9.1 Business requirements for access control</td>
</tr>
<tr>
<td></td>
<td>A.9.2 User access management</td>
</tr>
<tr>
<td></td>
<td>A.9.3 User responsibilities</td>
</tr>
<tr>
<td></td>
<td>A.9.4 System and application access control</td>
</tr>
<tr>
<td>A.10 Cryptography</td>
<td>A.10.1 Cryptographic controls</td>
</tr>
<tr>
<td>A.11 Physical and environmental security</td>
<td>A.11.1 Secure areas</td>
</tr>
<tr>
<td>A.12 Operations security</td>
<td>A.12.1 Operational procedures and responsibilities</td>
</tr>
<tr>
<td></td>
<td>A.12.2 Protection from malware</td>
</tr>
<tr>
<td></td>
<td>A.12.3 Backup</td>
</tr>
<tr>
<td></td>
<td>A.12.4 Logging and monitoring</td>
</tr>
<tr>
<td></td>
<td>A.12.5 Control of operational software</td>
</tr>
<tr>
<td></td>
<td>A.12.6 Technical vulnerability management</td>
</tr>
<tr>
<td></td>
<td>A.12.7 Information systems audit considerations</td>
</tr>
<tr>
<td>A.13 Communications strategy</td>
<td>A.13.1 Network security management</td>
</tr>
<tr>
<td></td>
<td>A.13.2 Information transfer</td>
</tr>
<tr>
<td>A.14 System acquisition, development and maintenance</td>
<td>A.14.1 Security requirements for Information systems</td>
</tr>
<tr>
<td></td>
<td>A.14.2 Security in development and support processes</td>
</tr>
<tr>
<td></td>
<td>A.14.3 Test data</td>
</tr>
<tr>
<td>A.15 Supplier relationships</td>
<td>A.15.1 Information security in supplier relationships</td>
</tr>
<tr>
<td></td>
<td>A.15.2 Supplier service delivery management</td>
</tr>
<tr>
<td>A.16 Information security incident management</td>
<td>A.16.1 Management of information security incidents and management</td>
</tr>
<tr>
<td>A.17 Information security aspects of business continuity management</td>
<td>A.17.1 Information security continuity</td>
</tr>
<tr>
<td></td>
<td>A.17.2 Redundancies</td>
</tr>
<tr>
<td>A.18 Compliance</td>
<td>A.18.1 Compliance with legal requirements</td>
</tr>
<tr>
<td></td>
<td>A.18.2 Information security reviews</td>
</tr>
</tbody>
</table>