Information technology - Security techniques - Information security management systems – Requirements
Contents

Introduction

Summary of the changes within ISO/IEC 27001:2013

Overview

Detailed review

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

Annex A

ISO/IEC 27002

Summary

Auditor Guidance
Introduction

The International Register of Certificated Auditors (IRCA) has prepared this technical review to communicate to IRCA Certificated Auditors, IRCA Approved Training Organisations and other interested parties our understanding of ISO/IEC 27001:2013.

This document should be read in conjunction with the IRCA Inform article on the summary of changes to ISO/IEC 27001 and ISO/IEC 27002 published in July 2013 in which an initial review of the proposed standards was provided. The purpose of this follow on document is to support a deeper appreciation of the standard and the differences with the first edition, ISO/IEC 27001:2005, as well as supporting the CPD requirements of IRCA certificated ISMS auditors.

The content of this technical review is provided in good faith and is IRCA’s opinion. It should not be reproduced nor used for commercial purposes. IRCA Certificated Auditors and IRCA Approved Training Organisations are advised to familiarise themselves with ISO/IEC 27001:2013 and ISO/IEC 27002:2013 when they are published.

- FDISs released to the National Standards Bodies 20th May 2013

Overview

ISO/IEC 27001:2013 has adopted the recently re styled wording and format for management system standards (Refer to Annex SL). The aim is to enhance the consistency, alignment and therefore the compatibility of ISO Management System Standards (MSS). It will encourage uniformity of management system terminology and assist organisations seeking to implement multiple management system programmes.

This new structure (referred to in Annex SL as the high level structure, or HLS) specifies 10 clauses (compared with the previous 8). In addition, there is a lot of text (identical core text, or ICT) that will be common across all ISO management system standards. There are in addition the information security specific current and new requirements. One point to note is the total absence of requirements for any documented procedures in the body of the standard.

As expected, ISO/IEC 27002 has been updated to reflect the changes made to ISO/IEC 27001:2013.
Detailed Review

Introduction

The Introduction no longer refers to a 'model', just requirements, and it now states explicitly the objective of an information security management system (ISMS) – 'preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed'. It also emphasises that the ISMS is part of and integrated with the organisation’s processes and overall management structure; this reinforces a key message – the ISMS is not a bolt-on to the business. It reinforces this by stating that information security is considered in the design of processes, information systems, and controls.

The contents of an ISMS continues to be made up of the usual components i.e. Policy, Resources, Management Processes, Information security risk assessment and treatment, Statement of Applicability, Documented Information and ISM processes deemed relevant to the organisation.

The Plan Do Check Act (PDCA) cycle applied to ISMS processes and mapped to the ISM Lifecycle in clause 0.2 Process approach of the 2005 edition, has been discontinued for the purposes of this standard.

There is only small but significant difference: previously the standard could be used to assess conformance now it is to assess the organisation's ability to meet the organisation’s own information security requirements.

The compatibility clause remains and is tangibly demonstrated and reinforced by the adoption of Annex SL.

1. Scope

The purpose of this clause is to state the applicability of the standard through the requirements to establish, implement and continually improving an ISMS within the context of the organisation (more of this later). It goes on to require the assessment and treatment of information security risks tailored to the needs of the organisation. This compares to the implementation of security controls in the 2005 edition.

Clause 1.2 Application (and exclusion) has been deleted. This is a significant change – exclusions are not acceptable.
2. **Normative references**

There is only one normative reference; ISO/IEC 27000, *Information technology – Security Techniques – Information security management systems – Overview and vocabulary*. It should be noted that this is currently being revised (from the 2012 edition).

3. **Terms and definitions**

Unlike the 2005 edition, there are no terms and definitions included. All the common terms and definitions from Annex SL are included plus additions, changes and deletions from the 2012 edition of ISO/IEC 27000. A comparison should be made and where necessary, further clarification sought from the other documents referenced.

4. **Context of the organisation**

Clause 4 requires an organisation to establish the context of its ISMS. It has to determine its needs and expectations and those of interested parties and decide the scope of the ISMS.

**Note:** The text in clause 4 is almost entirely unchanged Annex SL HLS and ICT.

4.1 **Understanding of the organisation and its context**

The idea of the context of the organisation’s overall business from the 2005 edition is maintained here. There is an explicit requirement to consider both internal and external issues which might impact the organisation’s purpose and affect its ability to achieve the expected outcomes of the ISMS. There are expectations that these considerations and resulting conclusions will need to be documented. To reinforce the theme that runs throughout the Annex SL there is a note referencing ISO 31000 Risk management – Principles and guidelines.

4.2 **Understanding the needs and expectations of interested parties**

Having identified its interested parties, there are now demands on an organisation to consider their needs and expectations. However, these needs and expectations are only those relevant to the information security. There are expectations that these interested parties and their requirements will need to be documented. Previously the involvement of interested parties was restricted to feedback and communication; now they are at the heart of the ISMS. There is a note clarifying that legal and regulatory requirements and contractual obligations may be included in the requirements of interested parties.
4.3 Determining the scope of the management system

The organisation needs to identify the boundaries and applicability (new for 2013) of the ISMS to establish its scope. There are expectations that this will need to be documented. The concept is not new, although some of the details such as the characteristics of the business, the organisation, its location, assets and technology have been dropped. However, as has been noted, there are no exclusions allowed. So the organisation must carefully consider what is included in and what is excluded from the scope. If something is excluded, it may automatically become an external issue or an interested party.

Three areas must be considered when determining the scope of the ISMS - the external issues (from clause 4.1), the needs and expectations of interested parties (from clause 4.2) as well as any interfaces and dependencies between activities performed by the organisation, and those that are performed by other organisations. Information security management system

This is a synthesis of the entire standard (and a rewording of the previous clause 4.1). The redundant ‘operate, monitor, review’ have been deleted. As mentioned in the Overview, the Plan Do Check Act (PDCA) cycle applied to ISMS processes of the 2005 edition has been deleted.
5. Leadership

Clause 5 requires an organisation to consider and establish the roles of top management in terms of the ISMS and how the information security policy is used as a tool to express its expectations of leadership of the organisation.

Note: The text in clause 5 is almost entirely unchanged Annex SL HLS and ICT.

5.1 Leadership and commitment

This is very familiar and the content is similar to clause 5.1 Management commitment in the 2005 edition. There is a sharper focus on the alignment of the ISMS with strategic organisation direction as opposed to the organisation’s strategic risk management context (in 2005). There are some subtle changes in emphasis; for example top management are now responsible for the information security policy (not the organisation) and they need to direct and support staff to contribute to the effectiveness of the ISMS and support other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility. There is one new requirement - ensuring the integration of the ISMS requirements into the organisation’s business processes; the consequence is that the ISMS cannot be a bolt-on to the organisation’s business.

Although mentioned again in the final clause of the standard, top management must now proactively demonstrate its commitment to the continual improvement of the ISMS.

This all reinforces the personal involvement of top management in all aspects of the ISMS.

5.2 Policy

Again, this is very familiar and the content is similar to clause 4.2.1 Establish the ISMS b) in the 2005 edition. As required in 5.1 Leadership and commitment above, top management must ensure that the information security policy and the information security objectives are established and are compatible with the strategic direction of the organisation. Again, there are some subtle changes in emphasis; for example the information security policy must be made available to interested parties (subject to management approval).
6. Planning

Clause 6 requires an organisation to establish its strategic objectives and to identify risks and opportunities and relate them to the scope of the ISMS.

Note: The text in clause 6 is almost entirely unchanged Annex SL HLS and ICT, but does have significant information security specific additions.

6.1 Actions to address risks and opportunities

6.1.1 General

Risk is not a new concept - there was a risk assessment approach in the 2005 edition (clause 4.2.1 c)); however, taking into consideration the context of the organisation, scope of the ISMS and its intended outcomes the organisation must identify the risks and opportunities which will need to be addressed to ensure the ISMS will achieve its objectives, prevent adverse impacts and enable opportunities for improvement. In other words, a risk assessment is undertaken on the ISMS itself and corrective actions identified and implemented as appropriate.

Although the definition of risk has always had both a positive and negative aspect, Annex SL has introduced the layman understanding of an opportunity being positive and a risk negative. As seen throughout the new standard, specific instances in the 2005 edition have been amended in favour of the generic; an example of this was the prescriptive risk in the 2005 edition of losses of confidentiality, integrity and availability.

6.1.2 Information security risk assessment

This is very familiar (it is similar to 4.2.1 d) and e) in the 2005 edition).

Note that there is no longer an explicit requirement to have a description of the risk assessment methodology and a risk assessment report; they are now implicit in the requirement for documented information about the information security risk assessment process.

6.1.3 Information security risk treatment

Again this is very familiar (it is similar to 4.2.1 f) and g) in the 2005 edition). The Statement of Applicability (SoA) with justification of any exclusions of any controls from Annex A are all present.

Note that there is no longer an explicit requirement to have a risk treatment plan (although the requirement is to formulate one); it is now implicit in the requirement for documented information about the information security risk treatment process.

Once again, there is note referencing ISO 31000 Risk management – Principles and guidelines.
6.2 Information security objectives and plans to achieve them

Information security objectives remain a requirement; however there is now an increased focus on them. They must now be consistent with the information security policy and they have to be at relevant functions and levels. Furthermore, they have to and take into account applicable information security requirements, and risk assessment and risk treatment results. In addition, information security objectives are now specifically required to be measurable (if practicable). Finally, to reemphasise their importance, the organisation must now plan how to achieve its information security objectives; what needs to be done, what resources will be required, who will be responsible, when it will be completed and how the results will be evaluated.
7. Support

Clause 7 addresses the needs of an organisation to determine what resource and competency requirements is has to support the ISMS and how internal and external communications will be arranged and ISMS documentation managed.

Note: The text in clause 7 is almost entirely unchanged Annex SL HLS and ICT.

7.1 Resources

As before, the organisation must determine what resource it requires for the ISMS. There are some explicit resource requirements that have been deleted (considered unnecessary because they are within the general requirement); examples are resources needed to ensure that information security procedures support the business requirements and maintain adequate security by correct application of all implemented controls.

7.2 Competence

The requirement to determine suitable competencies and for people to be competent based on education, training and experience remains. There is a (new) note which provides clarification on what documented information and actions may be required to record the achievement of competence. (The training, mentoring or reassignment of current employees or the contracting of competent persons).

7.3 Awareness

This clause reaffirms the need for persons under the control of the organisation to be aware their contribution to the effectiveness of the ISMS and the implications of not conforming with the ISMS. Now, it goes further by stating that they will also be aware of the information security policy.

7.4 Communication

This clause is (almost entirely) new for ISO/IEC 27001:2013. It requires that the organisation determine what and how ISMS communications will be managed to both internal and external parties – the what, who and when. Additionally, there is also a requirement for communication processes – the how. Previously there was only a need to communicate actions and improvements to interested parties; now the requirement is generic and broader.
7.5 Documented information

The standard refers to a catch-all requirement for documented information required by ISO/IEC 27001:2013 and any other considered necessary by the organisation. It no longer provides a list of required ISMS documentation. However, there is a new emphasis (and requirement) for documented information determined by the organisation as being necessary for the ISMS effectiveness.

Although there is a new clause title (7.5.2 Creating and updating) the requirements for controlling documentation remain essentially the same although worded slightly differently to that which has been seen before. As document control is a fundamental requirement of any management system this revised requirement will certainly be replicated in its new format across other management system standards.
8. Operation

Clause 8 covers the information security requirements of the ISMS and how to address them.
Note: The text in clause 8 is almost entirely unchanged Annex SL HLS and ICT, but does have significant information security specific additions.

8.1 Operational planning and control

Following the new requirements of clause 6.1 (Actions to address risks and opportunities) the standard is calling for consideration of the processes needed to address the issues identified in 6.1 and all that this entails (compare this to the rather weak language in the 2005 edition to 'manage operation of the ISMS' and 'implement procedures and other controls'). This includes implementing plans to achieve the information security objectives. This is a significant new requirement. In particular; establishing the criteria for such processes, implementing them and providing documentation to support these activities. There is also a need to address planned and unplanned changes and mitigate any adverse affects.

Also new is an expectation that the organisation retains control over any processes contracted out or outsourced.

8.2 Information security risk assessment

Having planned the information security risk assessment in 6.1.2 this is the implementation. These are the very familiar requirements from the 2005 edition (clause 4.2.2 b) and c)). The list of changes that needed to be taken into account in the 2005 edition has been deleted.

8.3 Information security risk treatment

Having planned the information security risk treatment in 6.1.3 this is the implementation. These are the very familiar requirements from the 2005 edition (clause 4.2.2 b) and c)).
9. Performance evaluation

Clause 9 requires an organisation to measure the performance of its ISMS against the standard and to review its performance and effectiveness, involving top management in this activity.

Note: The text in clause 9 is almost entirely unchanged Annex SL HLS and ICT.

9.1 Monitoring, measurement, analysis and evaluation

The intent of this clause of the standard is similar to clause 4.2.3 Monitor and review the ISMS of the 2005 edition. However, many of the detailed requirements have been allocated, quite correctly, to clause 9.3 Management Review. There is one element that may cause controversy and that is the introduction of information security performance. The 2005 edition had performance of the ISMS (in its entirety) and this did not cause problems, but there may be difficulties understanding this. Finally, there is a focus on the detail; added are who will do the monitoring and measuring (and when) and who will analyse and evaluate the results.

9.2 Internal Audit

This is almost identical to clause 6 Internal ISMS audits of the 2005 edition. Familiar requirements include… conducting internal audits at planned intervals, …plan, establish, implement and maintain an audit programme(s), … select auditors and conduct audits that ensure objectivity and impartiality of the audit process.

9.3 Management Review

This is similar in intent to 7 Management review of the ISMS of the 2005 edition. The management review content has been amended slightly for ISO/IEC 27001:2013 placing greater emphasis on using information on ISMS performance (trend analysis) to best effect (see 9.3 c 1,2,3). Remember, the heading of Clause 9 is Performance Evaluation. Other inputs remain largely unchanged (although a few prescriptive ones have been dropped; for example techniques, products or procedures, which could be used in the organisation to improve the ISMS performance and effectiveness). However, the outputs have been rationalised greatly; gone is the long prescriptive list (such as modification of procedures and controls and resource needs).

One important change from the 2005 edition is the deletion of the requirement for management review to be at least annually.
10. Improvement

Clause 10 aim is for the organisation to identify and act on ISMS nonconformity through corrective action. The first thing to note is that there is no longer any reference to preventive action. This area is now dealt with in the Planning elements of the standard (clause 6.1 etc).

Note: The text in clause 10 is almost entirely unchanged Annex SL HLS and ICT.

10.1 Nonconformity and corrective action

There are no significant changes to the intent of this requirement (previously clause 8.2). Focus is now placed on identifying and reacting to nonconformities including their “containment”. This will require an organisation to identify if and where similar nonconformities may have arisen elsewhere in the business and to implement corrective action ensuring this does not occur or if it has, that it is corrected.

It should be noted that the language here has changed – it is more user friendly. The organisation must react to the nonconformity, and, as applicable, take action to control and correct it, and deal with the consequences.

No documented procedure is required explaining how the corrective action process operates but an organisation shall retain documented information to evidence that the nature of nonconformities and subsequent actions have been captured along with the results of corrective actions.

10.2 Continual improvement

Again, there are no significant changes to the intent of this brief (but far reaching) requirement (previously clause 8.1). However continual improvement is now required to the suitability and adequacy of the ISMS as well as its effectiveness.

Deleted requirements

There are a number of miscellaneous requirements from the 2005 edition that have been deleted that have not already been mentioned above. For example

- procedures; there are no requirements for procedures in the ISMS, however the requirement still exists in the reference control objectives and controls of Annex A.
- obtaining management authorisation to implement and operate the ISMS.
Annex A (normative) Control objectives and controls

In ISO/IEC 27001:2005 (and ISO/IEC 27002:2005) there were 11 control areas with 39 control objectives and 133 controls; there are now 14 control areas with 35 control objectives and 114 controls. There is one control area that has been split (A.10 Communications and operations management is now A.13 Communications security and A.12 Operations security) and 2 new control areas (A.10 Cryptography and A.15 Supplier relationships). There are 3 deleted (A.10.3 System planning and acceptance, A.11.3 User responsibilities and A.12.2 Correct processing in applications) and 3 new control objectives (A.9.3 User responsibilities, A.15.1 Information security in supplier relationships and A.17.2 Redundancies) and 23 deleted, 7 merged and 6 new controls.

ISO/IEC 27002:2013

ISO/IEC 27002:2005 has been revised to reflect the changes in ISO/IEC 27002:2013.
Summary
It is evident that there have been changes (and improvements) made to ISO/IEC 27001:2013 compared with the 2005 edition. The purpose of this second edition of the standard is not to reinvent a well-established practice but to direct and support organisations in their desire to preserve the confidentiality, integrity and availability of information and all that can mean to their on-going success. By encouraging greater planning and preparedness as well as considering the performance and effectiveness of its ISMS will no doubt support this goal.

The shift to more generic management system standard terminology should be viewed as a positive step forward by all organisations seeking to integrate their systems as well as auditors auditing them. What it will require is possibly greater planning, forethought and commitment by the organisations’ management and interaction with perhaps more interested parties than before.

Auditor Guidance
Auditors must familiarise themselves with the standard and in particular its intent and shift in emphasis of management system components.

Elements new or more pronounced in ISO/IEC 27001:2013 and thus providing auditors the opportunity to refocus their audits include:

- More stringent requirements for organisational planning of the ISMS
- Greater (and more visible) top management commitment and leadership requirements
- Proactive communication policies and programmes
- Solid partnership approach with interested parties
- Individual ownership and responsibilities for the ISMS
- ISMS performance evaluation