ISO/IEC 27001:2013

Technical guidance for transitioning from ISO/IEC 27001:2005

January 2015

Protect • Comply • Thrive

ISO/IEC 27001:2013

Technical guidance for transitioning from ISO/IEC 27001:2005

Introduction

ISO/IEC 27001:2005 has been superseded by ISO/IEC 27001:2013. The International Accreditation Forum (IAF) has announced that, as of 1 October 2014, no more accredited certificates to ISO 27001:2005 will be issued. From that date, certification bodies may only issue certificates to the new version of the Standard, ISO 27001:2013.

The deadline for certification bodies (CBs) to transition from ISO 27001:2005 to ISO 27001:2013 has been set as 1 October 2015. Once transitioned, CBs will look to transition their clients promptly, and will carry out transition audits at their next scheduled surveillance visits.

If your ISMS is currently certified to the 2005 version of ISO27001, then you need to act now to comply with the requirements of the 2013 version of the Standard.

This green paper explains the differences between the two versions of the Standard and outlines the changes you will need to make to your ISMS to maintain its compliance with – and certification to – ISO27001.

The information security management system (ISMS)

ISO27001 sets out the requirements of an ISMS, which is defined as 'a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's information security to achieve business objectives'[1]. An ISMS focuses on protecting three key aspects of information:

- **Confidentiality**
  The information is not available or disclosed to unauthorised people, entities or processes.
- **Integrity**
  The information is complete and accurate, and protected from corruption.
- **Availability**
  The information is accessible and usable by authorised users.

ISO/IEC 27000, which provides the standard definitions used in ISO 27001:2013, states that information security can also involve other properties, such as authenticity, accountability, non-repudiation and reliability.

Overview of notable changes to ISO27001

The 2013 version of ISO27001 is substantially different from the 2005 iteration. This section lists the notable changes to the Standard. See **Summary of changes to management system clauses**, below, for detailed information about specific changes.

The Standard no longer formally adopts the Plan-Do-Check-Act (PDCA) process model, leaving it to the organisation to determine and adopt a continual improvement model that suits its own environment.

The Standard states that the order in which requirements are presented does not reflect

[1] ISO/IEC 27000:2014, section 3.2.1.

their importance or the order in which they should be implemented.

The *Terms and definitions* clause has been removed, and reference is instead made to the current version of ISO27000, which provides terms and definitions for all ISO27000-series standards. While this change at first appears purely cosmetic, it does result in a change of definition for such key terms as 'risk' (now the 'effect of uncertainty on objectives' rather than the 'combination of the probability of an event and its consequence'). It also means that when ISO27000 is updated, the terms and definitions for ISO27001 are automatically updated.

The scope now requires that organisations consider 'external and internal issues', 'interested parties', and the information security requirements of those interested parties. This is intended to ensure that the ISMS is relevant to the organisation's activity, and to provide assurance to its stakeholders that it is appropriate.

The ISO 27001:2013 information security risk assessment requirements are less prescriptive than those of ISO 27001:2005, and are aligned with ISO 31000:2009, the international standard for risk management:

- Threats and vulnerabilities are no longer referred to in the management system requirements.
- The risk assessment does not have to be asset-based.
- Risk treatment is to be achieved through the selection of controls determined necessary by a risk assessment. These controls are then compared with the Annex A controls to ensure that no essential controls have been omitted.
- Risks are treated and residual risk is accepted by 'risk owners' rather than 'asset owners'.

Management involvement is strengthened in leadership and review.

Documentation is no longer addressed through 'control of documents' and 'control of records'. The *Documented information* subclause now describes 'documented information required by this International Standard' and 'documented information determined by the organisation as being necessary for the effectiveness of the information security management system'. This allows the organisation greater latitude in determining the necessity of specific records and documents. It also simplifies the security procedures for the handling of documents and information.

There is a significant expansion of the requirements relating to setting information security objectives, evaluating information security performance, and measuring the effectiveness of the ISMS.

The requirement that internal auditors shall not audit their own work is absent in the 2013 version of ISO27001, but the need to ensure objectivity and impartiality remains.

Preventive action is no longer a separate requirement.

Finally, a number of requirements for communication have been introduced.

The new structure of ISO27001

ISO 27001:2013 adopts Annex SL[2], the harmonised structure now used for all ISO management system standards. This new structure provides a clearer view of the requirements of the ISMS than before, as there are now more top-level clauses into which the requirements have been rearranged:

0. *Introduction*
1. *Scope*
2. *Normative references*
3. *Terms and definitions*
4. *Context of the organisation*
5. *Leadership*
6. *Planning*
7. *Support*

[2] Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2013.

8. *Operation*
9. *Performance evaluation*
10. *Improvement*

Annex A has also been restructured into fewer controls (114), which have been divided into a larger number of categories:

- *A.5. Information security policies*
- *A.6. Organisation of information security*
- *A.7. Human resources security*
- *A.8. Asset management*
- *A.9. Access control*
- *A.10. Cryptography*
- *A.11. Physical and environmental security*
- *A.12. Operations security*
- *A.13. Communications security*
- *A.14. System acquisition, development and maintenance*
- *A.15. Supplier relationships*
- *A.16. Information security incident management*
- *A.17. Information security aspects of business continuity management*
- *A.18. Compliance*

ISO 27001:2005	**ISO 27001:2013**
Structure The ISMS requirements are spread across five clauses, which approach the ISMS from a managerial perspective: 4. *Information security management system* 5. *Management responsibility* 6. *Internal ISMS audits* 7. *Management review of the ISMS* 8. *ISMS improvement*	**Structure** The ISMS requirements are spread across seven clauses, which do not have to be followed in the order they are listed: 4. *Context of the organisation* 5. *Leadership* 6. *Planning* 7. *Support* 8. *Operation* 9. *Performance evaluation* 10. *Improvement*

Implications for transition

The most obvious feature of the new structure is the addition of clause 4, ***Context of the organisation***. The 2013 version of the Standard now ensures that the ISMS is aligned with the organisation's business objectives and processes, as well as ensuring that it fulfils business, regulatory and contractual obligations from the very beginning.

The new Standard also provides greater focus on communication, spreading the responsibility for information security further across the enterprise and business partners.

Summary of changes to management system clauses

0. Introduction

The Plan-Do-Check-Act (PDCA) process approach to establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS has been removed, as have all references to it. (The 2005 version of the Standard referenced it in clause 4, *General requirements*.)

It is worth acknowledging that the ISO Directive for management system standards[3] says: "An effective management system is usually based on managing the organisation's processes using a 'Plan-Do-Check-Act' approach in order to achieve the intended outcomes".

1. Scope

Subclauses 1.1 and 1.2 have been condensed into one paragraph, removing any overlap with the requirements in clauses 4 to 10.

2. Normative references

ISO27000 is quoted as a normative reference and is described as 'indispensable' for the application of ISO 27001:2013.

The code of practice ISO 27002 is no longer defined as a normative reference.

3. Terms and definitions

The list of terms and definitions has been replaced by a reference to the current version of ISO 27000, which standardises terms and definitions for the entire ISO27000 family of standards. (At the time of writing, the current version is ISO 27000:2014.)

This change means risk is now defined as the:

> effect of uncertainty on objectives
>
> [SOURCE: ISO Guide 73:2009] NOTE 1 to entry: An effect is a deviation from the expected — positive or negative.
>
> NOTE 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event (2.25), its consequence (2.14), or likelihood (2.45).
>
> Note 3 to entry: Risk is often characterised by reference to potential events (2.25) and consequences (2.14), or a combination of these.
>
> Note 4 to entry: Risk is often expressed in terms of a combination of the consequences (2.14) of an event (including changes in circumstances) and the associated likelihood (2.45) of occurrence.
>
> Note 5 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.
>
> Note 6 to entry: Information security risk is associated with the potential that **threats** (2.83) will exploit **vulnerabilities** (2.89) of an information asset or group of information assets and thereby cause harm to an organisation.

Please see ISO 27000:2014 for other definitions.

4. Context of organisation

4.1 Understanding the organisation and its context

This subclause requires the organisation to 'determine external and internal issues that are relevant to its purpose and affect its ability to achieve the intended outcome(s)' of the ISMS.

It references subclause 5.3 of ISO 31000:2009 (*Risk management - Principles and guidelines*), which considers establishing the external and internal context of the organisation, and the context of the risk management process. This includes ensuring 'that the objectives and concerns of external stakeholders are considered when developing risk criteria' and should align the organisation's security stance with its stakeholders' expectations. (See comments on subclause 5.2 *Policy*, below.)

4.2 Understanding the needs and expectations of interested parties

This subclause requires the organisation to determine the interested parties that are

[3] ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2013.

relevant to its ISMS and the requirements they have relevant to information security. These requirements may include 'legal and regulatory requirements and contractual obligations'.

4.3 Determining the scope of the information security management system

This subclause introduces the requirement for the organisation to determine the 'applicability' of its ISMS to establish its scope, and states that, in doing so, the organisation should consider the aspects identified in clause 4. There is an explicit requirement for 'interfaces and dependencies' to be considered as well.

4.4 Information security management system

This is a slight variation on subclause 4.1 of ISO 27001:2005, with the addition of a requirement to continually improve the ISMS. (As described above, the reference to the PDCA model has been removed.)

5. Leadership

The term 'leadership' has been introduced, as have requirements specifically relating to the 'top management' of the organisation subject to the ISMS.

5.1 Leadership and commitment

These requirements are more holistic than those in the 2005 version of the Standard. They also include the first reference to information security objectives, in subclause 5.1 a). Objectives are also referenced in subclauses 5.2 b) *Policy*, 6.2 *Objectives and plans to achieve them*, 8.1 *Operational planning and control* and 9.3 *Management review*.

There is a new requirement to integrate the ISMS requirements into the organisation's processes and the requirement for communication (subclause 4.2.4 c) in the 2005 version) is enhanced.

5.2 Policy

Throughout the Standard, the top-level policy requirement is consistently referred to as the 'information security policy'. (The 2005 version referenced the 'information security policy' and 'ISMS policy' as two different items, but acknowledged that one was a subset of the other and that they could both be described in a single document.)

Subclause 5.2 c) requires the information security policy to include a commitment to satisfy the applicable requirements of the ISMS.

5.3 Organisational roles, responsibilities and authorities

ISO 27001:2013 introduces the requirement that top management assigns (rather than determines) and communicates the responsibility and authority both for ensuring the ISMS conforms to the Standard and for reporting the ISMS's performance.

6. Planning

6.1 Actions to address risks and opportunities

6.1.1 General

Organisations should consider the external and internal issues and requirements of third parties and determine the risks and opportunities that need to be addressed in order to achieve their intended outcomes.

6.1.2 Information security risk assessment

The information security risk assessment process must include risk acceptance criteria as well as criteria for performing information risk assessments that consistently produce 'valid and comparable results'. (In ISO 27001:2005 the requirement was for 'comparable and reproducible results'.)

The risk assessment process should identify, analyse and evaluate the risks associated with the confidentiality, integrity and availability of information within the scope of the ISMS. Risk analysis should include an assessment of the consequences of the risk materialising, the realistic likelihood of the risk occurring, and the levels of risk. Evaluating the risks will compare the analysed levels of risk to the risk criteria and prioritise them for treatment.

As well as risks being identified, 'risk owners' must also be identified. (The 2005 version of the Standard required 'asset owners' to be identified.) 'Risk owner' is defined as a 'person or entity with the accountability and authority to manage a risk' [ISO 27000:2014].

6.1.3 Information security risk treatment

Taking into account the results of the risk assessment, an information security risk treatment process should be defined and applied in order to select the appropriate risk treatment options and design or identify required controls from any source. These controls should be compared to those provided in Annex A to ensure that no necessary controls have been omitted. The Standard states that the controls in Annex A are not exhaustive.

A Statement of Applicability containing the necessary controls should be produced. Subclause 6.1.3 d) strengthens the requirement that the inclusion of controls in the Statement of Applicability – as well as the exclusion of those from Annex A – is justified.

The requirement for a risk treatment plan remains. 'Risk owners' must approve it and accept the residual information security risks. (6.1.2 a) requires risk acceptance criteria to be defined.)

6.2 Information security objectives and planning to achieve them

This subclause builds on some of the requirements of subclause 5.1 of the 2005 version of the Standard, and requires information security objectives to be established, communicated and updated. They should take applicable information security requirements and risk assessment and treatment results into account, and should be consistent with the information security policy.

'If practicable', the objectives should be measured.

The plans for achieving information security objectives should include what will be done, what resources will be required, who will be responsible, when it will be completed, and how the results will be evaluated. This is a more specific set of requirements than found in ISO 27001:2005 (subclauses 4.2.2 a) and, to an extent, 4.2.2 b)).

7. Support

Training, awareness and competence (ISO 27001:2005 subclause 5.2.2) is now split into *Competence* (7.2) and *Awareness* (7.3).

7.1. Resources

What was covered in six subclauses in the 2005 version of the Standard (5.2.1 a) to f)) is now provided for in one sentence, with the remaining aspects covered elsewhere in the Standard.

7.2 Competence

Where ISO 27001:2005 required organisations to ensure the competence of responsible personnel by providing relevant training, ISO 27001:2013 goes further, requiring that organisations ensure all personnel are competent to do any work affecting information security 'on the basis of appropriate education, training, or experience'.

Where its employees are not deemed competent, an organisation should provide training or mentoring, reassign them, or hire/contract competent persons.[4]

7.3 Awareness

The requirements for awareness have been enhanced and some specific requirements have been added. All persons working under the organisation's control are to be aware of the information security policy and their contribution to the ISMS – including the benefits of improved information security performance, and the implications

[4] ISO 27000:2014 defines competence as the 'ability to apply knowledge and skills to achieve intended results'.

of not conforming with the ISMS requirements.

7.4 Communication

The organisation shall determine the need for internal and external communications, including who should communicate, what they should communicate on, when and with whom they should communicate it, and the processes to be used. This is in addition to the other new requirements for communication found throughout the Standard.

7.5 Documented Information

ISO27001 now acknowledges that an organisation's documentation requirements are dependent on its size and 'type of activities, processes, products and services', on 'the complexity of processes and interactions', and – new in ISO 27001:2013 – on 'the competence of persons'. (See *7.2 Competence*, above.)

Where subclause 4.3 of ISO 27001:2005 (*Documentation requirements*) listed the specific documents required for an ISMS, ISO 27001:2013 recognises that each ISMS is specific to the organisation that implements it and that ISMS documentation will therefore vary from organisation to organisation.

Subclause 7.5 *Documented information* states only that the ISMS should include the documented information 'required' by the Standard, and relies on the organisation to identify for itself the actual documents it needs.

For convenience, all the documentation requirements of ISO 27001:2013 – not all of which are relevant to all organisations – are listed below. (The relevant subclause numbers are shown in parenthesis.)

- The scope (4.3).
- The information security policy (5.2 e)).
- The information security risk assessment process (6.1.2).
- The information security risk treatment process (6.1.3).
- Statement of Applicability (6.1.3 d)).
- The information security objectives (6.2).
- Evidence of competence (7.2).
- Documentation necessary for the effectiveness of the ISMS (7.5.1 b)).
- Documentation necessary to have confidence that the processes required for operational planning and control have been carried out as planned (8.1).
- The results of information security risk assessments (8.2).
- The results of information security risk treatments (8.3).
- Evidence of the information security performance monitoring and measurement results (9.1).
- Internal audit programme(s) and audit results (9.2 g)).
- Evidence of the results of management reviews (9.3).
- Evidence of non-conformities and any subsequent actions taken, and the results of any corrective actions (10.1).

The Standard requires the organisation to consider the format ('e.g. language, software version, graphics') and media ('e.g. paper, electronic') for documented information.

The requirements for the creation, updating and control of documented information are largely similar to the 2005 version of the Standard, except for explicit reference to retention and disposal, and the control of documented information of external origin.

8. Operation

8.1 Operational planning and control

This subclause covers some of the '*Implement and operate the ISMS*' requirements from ISO 27001:2005 clause 4.2.2. It includes a requirement to control planned changes and review the consequences of unintended changes. It also explicitly states that outsourced processes are to be determined and controlled. (See also *4.3 Determining the scope of the information security management system*, above.)

8.2 Information security risk assessment

This subclause effectively replaces 4.2.3 d) in the 2005 version of the Standard ('The organisation shall … review risk assessments at planned intervals and review the residual risk and the identified acceptable levels of risks'), adding a reference to the criteria for performing information security risk assessments established by subclause 6.1.2 a).

8.3: Information security risk treatment

This subclause effectively replaces part of 4.2.2 b) in the 2005 version of the Standard, and states that organisations should implement a risk treatment plan.

9. Performance Evaluation

9.1 Monitoring, measurement, analysis and evaluation

Developed from subclauses 4.2.2 d) and 4.2.3 c) of the 2005 version, this subclause requires the organisation to determine the information security processes and controls that need to be monitored and measured in order to evaluate the performance and effectiveness of the ISMS.

The organisation must determine:

- what needs to be monitored and measured;
- valid methods for monitoring, measurement, analysis and evaluation that produce comparable and reproducible results;
- when the monitoring and measuring should be performed;
- who should monitor and measure;
- when the results of the monitoring and measurement should be analysed and evaluated;
- who should analyse and evaluate the results.

9.2 Internal Audit

This subclause recasts clause 6 of the 2005 version in simpler terms. The objective of internal audits is now described in fewer subclauses, and refers to 'the organisation's own requirements' rather than the specific considerations previously listed.

As in ISO 27001:2005, the audit programme should take into consideration the importance of the processes concerned and the results of previous audits. The specific restriction that 'auditors shall not audit their own work' has been removed, but the requirement that the selection of auditors and the conduct of audits should ensure objectivity and impartiality remains.

The requirement that 'the management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes' has been removed.

ISO 27001:2013 introduces the requirement that audit results are 'reported to relevant management'. Together with the competence requirements of subclause 7.2, the practical impact of this change is likely to be negligible.

9.3 Management Review

Subclause 9.3 simplifies clause 7 of ISO 27001:2005 (*Management review of the ISMS*). The explicit requirement for a management review to be completed 'at least once a year' has been removed: ISO 27001:2013 states that 'top management' should review the ISMS at 'planned intervals' to 'ensure its continuing suitability, adequacy and effectiveness'. The Standard no longer lists required inputs, instead stating that the management review should consider actions from previous reviews, changes in relevant issues, feedback on information security performance, feedback from interested parties, risk assessment results and opportunities for continual improvement.

The management review output requirements have been consolidated into a single sentence stating that decisions related to continual improvement opportunities and any need to change the ISMS should be included.

10 Improvement

10.1 Nonconformity and corrective action

The key change from subclauses 8.2 and 8.3 of ISO 27001:2005 is the removal of the requirement for the organisation to eliminate all nonconformities.

Now, the organisation must evaluate the need for the elimination of nonconformities to prevent their recurrence, having controlled and corrected them or dealt with their consequences. Corrective actions must be appropriate to the effects of the nonconformities. The term 'preventive action' is no longer used in the Standard.

10.2 Continual improvement

The *Continual improvement* subclause is largely unchanged from section 8.1 of the 2005 version of the Standard. ISO 27001:2013 adds the requirement to continually improve the 'suitability' and 'adequacy' of the ISMS, and removes any specific instruction on carrying out continual improvement of the ISMS.

ISO 27001:2005	ISO 27001:2013
Process The Standard clearly states that it follows the PDCA (Plan-Do-Check-Act) model.	**Process** The Standard does not specify any particular process model. The Standard requires that a process of continual improvement is used.

Implications for transition

Organisations that currently conform to ISO 27001:2005 will find the removal of a specified process model to be of negligible impact – PDCA is still valid under ISO 27001:2013. Organisations wishing to align the new continual improvement requirements with a process model used elsewhere in the organisation will also have minimal problems.

ISO 27001:2005	ISO 27001:2013
Governance and management Senior management plays a major role. Management and board engagement is strong but the distinction between board and management is not clear.	**Governance and management** Management roles are described as 'management' and 'top management', removing reference to the board. The organisation is the part of the business that falls within the scope, and not necessarily the legal entity. The board initiates the ISMS; management oversees the implementation of the ISMS.

Implications for transition

ISO 27001:2013 removes references to the board as part of the management system. In small organisations, the board and general management will still likely overlap, which may in practice blur the distinction between the two entities.

Organisations with an existing ISO 27001:2005 ISMS may need to clarify the roles of 'management' and 'top management' to distinguish the two entities.

ISO 27001:2005	ISO 27001:2013
Risk assessments The definition of risk is the 'combination of the probability of an event and its consequences'. The organisation identifies risks against assets. The asset owner determines how to treat the risk, accepting residual risk. Controls are drawn from Annex A. Annex A is not exhaustive and additional controls can be drawn from other sources. The Statement of Applicability records whether a control from Annex A is selected and why.	**Risk assessments** The definition of risk is the 'effect of uncertainty on objectives', which may be positive or negative. The risk assessment and risk treatment plan processes are aligned to ISO31000. Baseline controls based on regulatory, business and contractual obligations may be identified and implemented before the risk assessment is conducted. The organisation identifies risks to the organisation's information. The assessment does not have to be asset-based. The risk owner determines how to treat the risk, accepting residual risk. Controls are drawn from any source or control set. Selected controls are compared to those in Annex A. The Statement of Applicability records whether a control from Annex A is selected and why.

Implications for transition

There is a significant difference between the two approaches to risk assessment, and making the transition to the approach prescribed in ISO 27001:2013 can take a significant shift in thinking. Adoption of the practices described in ISO31000 may smooth this process, but it must be rethought from first principles.

The most significant changes are that:

- You can assign baseline controls based on your contractual, business and regulatory requirements ahead of the risk assessment.
- The risk assessment is not asset-based.
- Risk treatments and the acceptance of residual risk are handled by the risk owner.

Summary of new controls

A.6.1.5 – Information security in project management

All projects will address information security, regardless of the nature of the project. This ensures that information security is dealt with from the bottom up.

A.12.6.2 – Restrictions on software installation

Change controls are more carefully delineated, directing specific procedures to cover the installation of software by users.

A.14.2.1 – Secure development policy

Rules for the development of software and systems are established and applied. This relates to controls 14.1.1 and 14.1.3, which address the control of information systems and applications.

A.14.2.5 – Secure system engineering principles

This control replaces deleted controls with the broader notion of the use of good engineering and architecture to preserve system security.

A.14.2.6 – Secure development environment

The organisation should establish secure development environments for system development and integration across the whole development lifecycle. This control is deliberately broad to allow input from the earliest stages of the ISMS (identifying the nature of the organisation), rather than restrictively demanding measures that may not be relevant.

A.14.2.8 – System security testing

The organisation must test security functionality during development.

A.15.1.1 – Information security policy for supplier relationships

This control provides additional assurance to that covered by confidentiality and non-disclosure agreements.

A.15.1.3 – Information and communication technology supply chain

This control requires agreements with suppliers to address the information security risks associated with information and communications technology services and product supply chain.

A.16.1.4 – Assessment of and decision on information security events

Information security events are examined and assessed to determine whether they qualify as information security incidents. This control applies an additional step in the incident management process.

A.16.1.5 – Response to information security incidents

In conjunction with control A.16.1.4, above, this control assures a more rigorous response to incidents and a more comprehensive incident management process.

A.17.2.1 – Availability of information processing facilities

Availability of information and processing facilities is clearly addressed as a continuation of the information security continuity controls in A.17.1.

Summary of deleted controls

The following controls no longer appear in ISO 27001. Other controls from ISO 27001:2005 are either wholly present in ISO 27001:2013 or are covered by new or modified controls.

A.6.1.1 – Management commitment to information security

A.6.1.2 – Information security coordination

A.6.1.4 – Authorisation process for information processing facilities

A.6.2.1 – Identification of risks related to external parties

A.6.2.2 – Addressing security when dealing with customers

A.10.4.2 – Controls against mobile code

A.10.7.4 – Security of system documentation

A.10.8.5 – Business information systems

A.10.10.2 – Monitoring system use

A.11.4.2 – User authentication for external connections

A.11.4.3 – Equipment identification in networks

A.11.4.4 – Remote diagnostic and configuration port protection

A.11.4.6 – Network connection control

A.11.4.7 – Network routing control

A.11.5.2 – User identification and authentication

A.11.5.5 – Session time-out

A.11.5.6 – Limitation of connection time

A.11.6.2 – Sensitive system isolation

A.12.2.1 – Input data validation

A.12.2.2 – Control of internal processing

A.12.2.3 – Message integrity

A.12.2.4 – Output data validation

A.12.5.4 – Information leakage

A.14.1.2 – Business continuity and risk assessment

A.14.1.4 – Business continuity planning framework

A.15.1.5 – Prevention of misuse of information processing facilities

A.15.3.2 – Protection of information systems audit tools

ISO 27001:2005

Controls
Annex A contains 133 controls across 11 control categories.

Controls from other sources may be used to plug gaps not covered by Annex A controls.

ISO 27001:2013

Controls
Annex A contains 114 controls across 14 control categories.

Controls (from any source) are identified before referring to Annex A.

Implications for transition

While many controls have been retained from the 2005 version of the Standard, the 2013 iteration has been restructured, so older controls may now act on different control objectives. Although your risk assessment will drive how you select the controls to manage your information risks, you should re-examine how each control is implemented in order to ensure that your information security objectives are being fulfilled.

It is also worth noting that controls are selected *before* consulting Annex A, which allows organisations to select (from any source) the controls that fit best with their processes before filling in the remaining gaps with the Annex A controls.

ISO 27001:2005

Documentation
The Standard recognises two forms of documentation: documents and records.

Documents include policies, procedures, process diagrams, etc.

Records track work completed, audit schedules, etc.

ISO 27001:2013

Documentation
The Standard makes no distinction between documents and records.

Documents and records are subject to the same control requirements.

Implications for transition

This should have little impact on an existing ISMS, especially if the organisation already uses a quality management system (QMS), such as one based on ISO/IEC 9001. The primary distinction between the 2005 and 2013 versions is that documents

and records are no longer distinct, and so the security procedures for each are streamlined.	
ISO 27001:2005	**ISO 27001:2013**
Measuring effectiveness There is a requirement to define how the effectiveness of controls is measured and how that measurement will be assessed. The organisation must identify its own measurement and monitoring regime in order to prove the efficacy of its ISMS.	**Measuring effectiveness** The Standard requires a process for measuring the effectiveness of the ISMS, its processes and controls. It specifies the requirements for measurement. The Standard mandates a process for defining the measurement and monitoring regime.
Implications for transition The process specified in ISO 27001:2013 is much more rigorous and is open to external examination, which will prove useful in ensuring that the ISMS complies with the Standard. As such, there is little to lose from adopting this methodology, even if the organisation opts to continue using the 2005 specification in the short term.	
ISO 27001:2005	**ISO 27001:2013**
Certification An ISMS can be certified to ISO 27001:2005 by any accredited certification body. **Existing certifications to ISO** 27001:2005 are valid until 1 October 2015, after which organisations must have transitioned to the new version of the Standard. All new certificates to the Standard must now be issued to ISO 27001:2013.	**Certification** An ISMS can only be certified to ISO 27001:2013 by an accredited certification body that has itself transitioned to the new version of the Standard. Certification bodies have until the end of April 2015 to transition. After 1 October 2015, all certificates will be to the new version of the Standard.
Implications for transition Achieving accredited certification to the new version of the Standard depends on your certification body being recognised by an accreditation body (UKAS in the UK) as capable of carrying out ISO 27001:2013 certifications. Your certification body may conduct surveillance audits of your ISMS against the requirements of ISO 27001:2005 until it requires you to transition to ISO 27001:2013, but will be unable to certify your organisation against it. In the United Kingdom, all accredited certification bodies are expected to transition to ISO 27001:2013 by the end of April 2015. Your surveillance audits will continue to be carried out against the 2005 version of the Standard until then, after which you are more likely to be assessed against ISO 27001:2013 – though you should check this in advance with the certification body concerned. Global conformity to ISO 27001:2013 is required by 1 October 2015, when all transitions by certification bodies must be completed.	

Please note: If you are in any doubt about the best course of action for your particular circumstances, we advise you to contact IT Governance on **+44 845 070 1750** or **email us** today.

ISO 27001:2005	ISO 27001:2013
Integration with other standards Although the Standard is designed to integrate with other ISO/IEC standards, it should be noted that many reference standards (ISO14001 and ISO9001, for example) have been updated since 2005 and integration may not be as easy.	**Integration with other standards** The Standard is designed to better integrate with other ISO/IEC management system standards. Terms and definitions are standardised across the ISO 27000 family, using those provided in ISO27000, and the Standard adopts Annex SL, the harmonised structure now utilised for all ISO management system standards.

Implications for transition

It is good practice to ensure that other standards with which you comply are up to date and integrate correctly. This is increasingly difficult with older standards, and you will need to put in additional effort to make sure they remain aligned.

General conclusions

There are numerous benefits to achieving certification to the new version of the Standard.

- Large organisations can continue using any continual improvement process they currently employ (PDCA is no longer a requirement).
- Equally, organisations required to use specific process models (based on COBIT®, ITIL®, etc.) have reduced barriers to entry.
- The Standard is more flexible in general.
- The ISO31000 risk assessment link ties information security risk management into corporate risk management approaches.
- As more standards begin to use the Annex SL structure, it will be simpler to maintain coherency/integration.

If you are currently certified to ISO 27001:2005, your certification body may have already got in touch with you to inform you of the deadline when you will be expected to transition to ISO 27001:2013.

Revising your ISMS needn't be the daunting undertaking it may at first seem. IT Governance offers a full range of ISO 27001:2013 transition resources to help you revise your existing ISMS to comply with the new version of the Standard whatever your resources or expertise. See below for more details.

Useful Resources

IT Governance offers a unique range of products and services, including books, standards, pocket guides, training courses, staff awareness solutions and professional consultancy services.

Standards

ISO/IEC 27001:2013 and ISO/IEC 27002:2013

This package includes both the new (2013) editions of ISO/IEC 27001 and ISO/IEC 27002 that have been updated to reflect international best practice for information security.

Tools

ISO 27001:2005 to ISO 27001:2013 Conversion Tool

This tool maps the controls in ISO 27001:2005 to those in ISO 27001:2013, and provides guidance where controls have been deleted, relocated, adjusted and added to the Standard, helping certified organisations make the transition from their existing ISO 27001:2005-compliant ISMS to an ISO 27001:2013-compliant ISMS.

Implementation solutions

ISO 27001:2013 implementation packages

The Basics
Do It Yourself
Get A Little Help
Get A Lot of Help
We Do It For You

IT Governance's packaged ISO27001 implementation solutions will enable you to implement an ISO 27001:2013-compliant ISMS at a speed and for a budget appropriate to your individual needs and preferred project approach. Each fixed-price solution is a combination of products and services that can be accessed online and deployed by any company in the world.

Books

An Introduction to Information Security and ISO27001:2013

Written by an acknowledged expert on the new ISO27001 Standard, *An Introduction to Information Security and ISO 27001:2013* is the ideal resource for anyone wanting a clear, concise and easy-to-read primer on information security. It will ensure the systems you put in place are effective, reliable and auditable.

ISO27001/ISO27002: A Pocket Guide

Information is one of your organisation’s most important resources. Keeping it secure is therefore vital to your business. This pocket guide provides a concise introduction to the 2013 iterations of these two important information security management standards.

Nine Steps to Success - An ISO 27001:2013 Implementation Overview

Completely up to date with ISO 27001:2013, this is the new edition of the original no-nonsense guide to successful ISO27001 certification. *Nine Steps to Success* outlines the nine essential steps to implementing an effective ISO 27001:2013-compliant ISMS.

Training courses

ISO 27001:2013 Certified ISMS Transition Training Course

Save time and money with a single training course designed to provide an essential ISO 27001:2013 knowledge update for ISMS implementers and auditors. Ensure you upgrade your IBITGQ ISO27001 qualifications to maintain your professional development and career prospects.

Consultancy

ISO 27001:2013 Transition Consultancy

IT Governance’s ISO27001 Transition Consultancy service provides you with all the necessary support, guidance and advice you need to successfully transition your ISMS to compliance with ISO 27001:2013.

IT Governance Solutions

IT Governance sources, creates and delivers products and services to meet the evolving IT governance needs of today's organisations, directors, managers and practitioners.

IT Governance is your one-stop shop for corporate and IT governance information, books, tools, training and consultancy. Our products and services are unique in that all elements are designed to work harmoniously together so you can benefit from them individually and also use different elements to build something bigger and better.

Books

Through our website, www.itgovernance.co.uk, we sell the most sought-after publications covering all areas of corporate and IT governance. We also offer all appropriate standards documents.

In addition, our publishing team develops a growing collection of titles written to provide practical advice for staff taking part in IT governance projects, suitable for all levels of staff knowledge, responsibility and experience.

Toolkits

Our unique documentation toolkits are designed to help small and medium organisations adapt quickly and adopt best management practice using pre-written policies, forms and documents.

Visit www.itgovernance.co.uk/product-demos to view and trial all of our available toolkits.

Training

We offer training courses from staff awareness and foundation courses, through to advanced programmes for IT Practitioners and Certified Lead Implementers and Auditors.

Our training team organises and runs in-house and public training courses all year round, covering a growing number of IT governance topics.

Visit www.itgovernance.co.uk/training for more information.

Through our website, you can also browse and book training courses throughout the UK that are run by a number of different suppliers.

Consultancy

Our company is an acknowledged world leader in our field. We can use our experienced consultants, who have multi-sector and multi-standard knowledge and experience, to help you accelerate your IT GRC (governance, risk, compliance) projects.

Visit www.itgovernance.co.uk/consulting for more information.

Software

Our industry-leading software tools, developed with your needs and requirements in mind, make information security risk management straightforward and affordable for all, enabling organisations worldwide to be ISO27001-compliant.

Visit www.itgovernance.co.uk/software for more information.