Comparing ISO 27001:2005 to ISO 27001:2013

October 2013

Protect • Comply • Thrive

Comparing ISO 27001:2005 to ISO 27001:2013

Description of an ISMS

An ISMS, or information security management system, is "part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources"[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; it is protected from corruption.
- Availability
  The information is accessible and usable to authorised users.

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

Comparing ISO 27001:2005 to ISO2 7001:2013

ISO 27001:2005	ISO 27001:2013
Structure The specification is spread across 5 clauses, which approach the ISMS from a managerial perspective.	**Structure** The specification is spread across 7 clauses, which do not have to be followed in the order they are listed.
4. Information security management system 5. Management responsibility 6. Internal ISMS audits 7. Management review of the ISMS 8. ISMS improvement	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 'Context of the organisation'. The 2013 edition of the standard now ensures that the ISMS is aligned with the organisation's	

[1] ISO/IEC 27000:2012.

business objectives and processes, as well as ensuring that the ISMS fulfils the business, regulatory and contractual obligations from the very beginning.

Furthermore, the content of the standard provides greater focus on communication, spreading the responsibility for information security further across the enterprise and business partners.

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

For organisations with an existing ISMS, the change to remove the requirement of the PDCA model may be negligible – the PDCA process is still valid. Organisations wishing to align the current continual improvement process with one used elsewhere in the organisation will also have minimal problems.

Organisations beginning a new ISO 27001:2013 ISMS, however, will need to identify the best continual improvement process for their business, if one is not already in place. For most organisations, PDCA – which has a substantial pedigree – will still prove to be a practical and sound method to deploy.

Governance and management Senior management plays a major role. Management and board engagement is high but the separation 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 that 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 implementation may need to clarify the role of 'management' and 'top management' to clarify the roles of the two entities.

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, so additional	**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 ISO 31000. Baseline controls based on regulatory, business and contractual obligations may be identified and implemented before the risk assessment is conducted.

controls can be drawn from other sources. The Statement of Applicability records whether a control from Annex A is selected and why.	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 ISO 31000 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 is handled by the risk owner.

Controls Annex A contains 133 controls across 11 control categories. Controls from other sources are used to 'plug gaps' not covered by Annex A controls.	**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 of the controls have been retained from the 2005 edition, the 2013 edition has been restructured, so older controls may now act on different control objectives. While your risk assessment will drive how you select 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.

Documentation The standard recognises two forms: documents and records. Documents include policies, procedures, process diagrams, etc. Records track work completed, audit schedules, etc.	**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 ISO/IEC 9001. The primary distinction between the 2005 and 2013 editions is that documents and records are no longer distinct, and thus the security procedures for each are streamlined.

Measuring effectiveness There is a requirement to define how to measure effectiveness of controls and how those measurements will be assessed. The organisation must identify their own measurement and monitoring regime in order to prove the efficacy of the ISMS.	**Measuring effectiveness** The standard requires a process for measuring effectiveness of the ISMS, its processes and controls. It specifies the requirements for measurement. The standard sets requirements for a process for defining the measurement and monitoring regime.

Implications for transition

The process specified in the 2013 edition is much more rigorous and 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.

Certification An ISMS can be certified by any accredited certification organisation. Certification against ISO 27001:2005 is likely to remain valid for up to 3 years, even after ISO 27001:2013 certification has begun.	**Certification** There is currently no accredited certification programme. Accredited certification is expected to begin Q1 2014.

Implications for transition

This is likely the most significant reason to avoid rushing into updating to the 2013 edition of the standard. Until the 2013 accredited certification process is established, there will always be some degree of uncertainty regarding whether your implementation will be considered compliant. For organisations looking to receive certification more than six months from publication of the 2013 version, however, it may be worthwhile beginning the process of transitioning to the 2013 edition. For those seeking to certify earlier or soon after certification of 2013 begins, however, the 2005 edition remains a solid choice.

Integration with other standards The standard is designed to integrate with other ISO/IEC standards, although many reference standards (14001 and 9001, for instance) have since been updated.	**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 ISO 27000:2012.

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

ISO 27001:2013 is clearly a step up for the standard, but ISO 27001:2005 is by no means immediately irrelevant. The general advantages of each are as follows:

ISO 27001:2005

- There is a current accredited certification scheme for this version of the standard, and this is likely to continue for approximately 18 months.
- Certificates awarded against 2005 may remain valid for up to 3 years.
- It is familiar and well recognised, so expertise and literature is readily available.

ISO 27001:2013

- Large organisations can continue using any continual improvement process they currently use (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 ISO 31000 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.

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

Includes both the new (autumn 2013) editions of ISO/IEC 27001 and ISO/IEC 27002. Is made up of both new International Standards that have been updated to reflect international best practice for information security.

Books

- Introduction to Information Security and ISO 27001

Most organisations implementing an information security management regime opt for systems based on the international standard, ISO/IEC 27001. This approach ensures that the systems they put in place are effective, reliable and auditable.

- ISO 27001/ISO27002 Pocket Guide

Information is one of your organisation's most important resources. Keeping it secure is therefore vital to your business.

- Nine Steps to Success - An ISO 27001(2013) Implementation Overview

Completely up to date with ISO27001:2013, this is the new edition of the original no-nonsense guide to successful ISO27001 certification. Ideal for anyone tackling ISO27001 for the first time, Nine Steps to Success outlines the nine essential steps to an effective ISMS implementation.

Training courses

- ISO27001 2013 Certified ISMS Transition Training Course

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

IT Governance Solutions

IT Governance source, create and deliver 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/free_trial.aspx 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.aspx 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, with 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.aspx 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.aspx for more information.

Contact us: + 44 (0) 845 070 1750

www.itgovernance.co.uk servicecentre@itgovernance.co.uk