Is your company up-to-date with the latest ISO 27001 standard?

Summary of key changes to ISO 27001:2013
the international standard for security managment.

stickman
CYBER SECURITY BY DESIGN

Introduction

ISO 27001, written formally as ISO/IEC 27001, is an international standard for information security management. It includes a number of policies and procedures, and provides security controls to effectively manage an organisation's information risk management system.

Without proper implementation of ISO 27001, an organisation may find its security controls are unproductive and disorganised.

With a risk-based, six-step methodology, ISO 27001 serves as a prototype for establishing and improving the security management structure of an organisation.

The six steps of ISO planning are:

- Implementing a security policy.
- Defining the scope of the information security management system (ISMS).
- Carrying out a risk assessment.
- Managing identified risks.
- Selecting the objectives and controls accordingly for implementation.
- Preparing a statement of applicability.

What are the major changes?

ISO 27001 is not the same as the standards it replaces. The major changes are:

- Alignment of risk management requirements with the principles of ISO 31000.
- Mandatory conformity to high-level structure by all management system standards, thus leading to easy integration in case of more than one management system.
- Changes in terminology and removal or relocation of definitions.
- Replacement of preventive action with "actions to address, risks and opportunities".
- Modification of controls in Annexure A to counter evolving threats.
- Increased emphasis on objectives, monitoring, performance and metrics.

The 2005 version of the standards followed the Plan-Do-Check-Act (PDCA) model whereas ISO 27001:2013 does not follow any specific model. Organisations that have already implemented ISO 27001 can continue with the PDCA model while those adapting it now need to identify how they will ensure continual improvement. ISO 27001:2005 identifies two forms of documentation: documents and records. Documents include process structures, policies, and procedures. Records include audit schedules and work histories. The 2013 version made no differentiation between documents and records.

Besides the major changes, the basic difference between the two sets of standards is the structure, with the first version having five basic sections and the revised version having seven basic sections. The revised standard is based on the Annex SL template, and according to ISO, all future Management System Standards will use the same template to give all of them the same outlook.

What are the major changes? cont’d

The following table shows the basic clauses of the two versions of the standard. ISO 27001:2013 has more clauses but is easier to manage than the previous version.

ISO/IEC 27001:2005

- Information and security management system
- Management responsibility
- Internal ISMS audits
- Management review of ISMS
- ISMS improvement

ISO/IEC 27001:2013

- Context of the organisation
- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement

Summary of new controls

ISO 27001:2013 comes with the addition of some new controls to the standard, summarised as follows:

A.6.1.5 This control makes it necessary to make information security a compulsory part of project management, regardless of the nature of project.

A.12.6.2 This control restricts every user from installing any unauthorised software on the company systems without getting permission and the verification of the analyst.

A.14.2.1 This control checks and ensures the integration of security during all software development phases.

A.14.2.5 This control mandates the security of system engineering principles and their documentation.

A.12.2.6 This control ensures that all risks have been properly identified and assessed.

A.14.2.8 This control makes it compulsory to implement and follow software testing procedures.

A.15.1.1 This control makes it mandatory to develop a security policy for the supplier's access that is in line with the access control policy.

A.15.1.3 This control ensures agreements discussing the security and risks of the supply chain are carried out.

A.16.1.4 This control checks that there should be a procedure to analyse and classify security issues.

9 steps to help with your transition

The ISO 27001 standard was first published in 2005 and 2013 is the first revised version of the standard. To make an easy transition from the earlier version to the revised version, here are some steps that can serve as a helpful guide:

1 Make a list of all stakeholders

To begin with, make a list off all the interested parties and stakeholders, which include all people and organisations directly influencing or being influenced by your company's information security. Half of the job is done if you have already complied with control A.15.1.1 of the previous version, including all regulatory, statutory and contractual requirements.

2 Define the interfaces

As per the new version, you need to identify all interfaces between your organisational activities and those carried out by third party. Include this in your scope definition.

3 Line up your ISMS goals with your organisational strategy

According to this requirement of ISO 27001:2013, make your ISMS objectives in line with the strategic course of your organisation.

4 Change your risk assessment process

Identify your risk owners and use any methodology that seems easy for you. You are no longer required to base your methodology on identifying threats, vulnerabilities and assets. Also identify outsourced processes and their control methodology.

5 Gain consent from risk owners

ISO 27001:2013 requires you to gain consent or approval of your risk treatment plan and acceptance of any remaining information security risks.

6 Develop an effective communication plan

Develop a communication plan that clearly indicates the communication links as to who will communicate to whom and what to communicate in terms of both internal and external communication.

9 steps to help with your transition cont'd

7 Make a decision on management procedures

Preventive actions have now become a part of the risk assessment process in the 2013 revision, and the remaining management procedures of Document Control, Internal Audit and Corrective Action have been removed. Make a decision on whether you want to delete the Management Procedures or not. In any case, you need to maintain the aforementioned three procedures even if they you don't document them.

8 Develop new policies and procedures

Once you choose related controls to be applicable, whether or not you have written them before, it becomes mandatory upon you to develop the following documents:

- Secure System Engineering Principles (A.14.2.5)
- Incident Management Procedure (A.16.1.5)
- Supplier Security Policy (A.15.1.1)
- Business Continuity Procedure (A.17.1.2)

9 Organise your controls and mention the status in the SoA

For each control in the Statement of Applicability (SoA), specify if you have implemented it or not. Annex A has retained most of the old controls, while adding a few more. The added new controls include:

- A.6.1.5 Information security in project management
- A.14.2.1 Secure development policy
- A.14.2.5 Secure system engineering principles
- A.14.2.6 Secure development environment
- A.14.2.8 System security testing
- A.16.1.4 Assessment of and decision on information security events
- A.17.2.1 Availability of information processing facilities

How can Stickman help?

Stickman Consulting specialises in helping companies implement ISO 27001 and achieve PCI DSS compliance.

If you need help implementing ISO 27001, contact us today.

Stickman Consulting
Contact: Gergana Kiryakova
Level 11, Suite 2,
210 George Street, Sydney, 2000
Ph: 1800 785 626
e: gergana.kiryakova@stickman.com.au
w: www.stickman.com.au

About Us

Stickman Consulting help businesses to achieve PCI DSS (Payment Card Industry Data Security Standards) Compliance and implement ISO 27001.

Stickman has been certified by the PCI SCC as a PCI DSS Qualified Security Assessor (PCI DSS - QSA) that enables Stickman to provide organisations such as Banks, Payment Service Providers and Merchants with:

- PCI DSS Assessment
- PCI DSS Implementation and Remediation Services
- PCI DSS Monitoring and Maintenance
- PCI DSS Certification

Stickman

Level 11, Suite 2,
210 George Street, Sydney, 2000
1800 785 626

www.stickman.com.au