**Is Your Company Up to Date with the Latest ISO 27001 Standard?**

ISO 27001, written fully 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 organization’s information risk management system. Without proper implementation of ISO 27001, an organization may find its security controls to remain unproductive and disorganized.

With a risk-based six step methodology, ISO 27001 serves as a prototype for establishing and improving the security management structure of an organization. The main six steps of ISO planning are as follows:

* Implement a security policy.
* Define the scope of ISMS
* Carry out Risk Assessment.
* Manage the identified risk
* Select the objectives and controls accordingly to implement.
* Prepare a statement of applicability.

**What are the Major Changes?**

* 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 follows Plan-Do-Check-Act (Model) whereas ISO 27001:2013 does not follow any specific model. Organizations that have already implemented ISO 27001 can continue with PDCA model while those adapting it now need to identify how they will ensure continual improvement. ISO 27001:2005 identifies two forms of documentation, i.e. Documents and Records. Documents include process structure, policies, procedures, etc. Records include audit schedule, work history, etc., whereas 2013 version has no differentiation of documents and records.

Besides the major changes, the basic difference between the two 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 Annex SL template, and according to ISO, all future Management System Standards will be using the same template to give the same outlook to all of them.

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

|  |  |
| --- | --- |
| **ISO/IEC 27001:2005** | **ISO/IEC27001:2013** |
| * Information security management system * Management Responsibility * Internal ISMS audits * Management review of the ISMS * ISMS Improvement | * Context of the Organization * Leadership * Planning * Support * Operation * Performance evaluation * Improvement |

**Addition of New Controls**

ISO 27001:2013 comes with the addition of some new controls to the standard, summarized 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 to install any unauthorized software on the company systems without taking permission and 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** It mandates the security of system engineering principles and its documentation.

**A.12.2.6** It ensures that all risks have been properly identified and assessed.

**A.14.2.8** This control has made 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, which 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 analyze and classify security issues.

**Transition from ISO 27001:2005 to ISO 27001:2013**

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, the following steps 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 organizations 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.

1. **Define the Interfaces**

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

1. **Line up your ISMS goals with your Organizational Strategy**

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

1. **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.

1. **Gain Consent from Risk Owners**

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

1. **Develop Effective Communication Plan**

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

1. **Make a Decision on Management Procedures**

Preventive actions have now become a part of risk assessment process in 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.

1. **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)

1. **Organize your Controls and Mention the Status in SoA**

For each control in the Statement of Applicability, specify if you have implemented it or not. Annex A has retained most of the old controls, while adding a few more. New controls added 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