ISO 27001 Security Certification

Busting Myths and Building Trust

Author:

Rahul Jayachandran,
Practice Manager- Consulting,
Paladion Networks

PALADION
HIGH SPEED CYBER DEFENSE

Why do You Need ISO 27001 Certification?

Confidential information, whether corporate, professional, or personal, must be protected. The growing number and severity of security breaches in different industry domains shows how vital such protection is. Digitization has multiplied the risks of information theft and unauthorized data manipulation, replication, dissemination, corruption, and destruction. When information misuse leads to bank accounts raids, identity theft, loss of confidential data or loss of control over critical resources, the consequences for companies, clients, and others can be devastating.

> "Information misuse can have major financial and reputational impact on the organizations and its clients."

ISO 27001 standard helps in systematically and holistically managing security incidents. The international ISO 27001 standard defines requirements for an information security management system (ISMS). An ISMS is a systematic approach to securely managing sensitive organizational information. It can be used to protect financial data, intellectual property, employee records, patient medical details, and any other confidential or valuable information.

Certification for compliance with ISO 27001 is applicable for any size of organization and any business domain. This includes organizations such as datacenters and IT outsourcing companies that manage data on behalf of others.

Operational and Strategic Advantages

Certification to the ISO 27001 security standard means that your organization has deployed an ISMS for its information to ensure:

- Confidentiality. Only authorized entities may access the information.
- Integrity. The information is correct with no unauthorized modification.

- Availability. Authorized entities can still access the information when needed.

An additional benefit is the contribution to sustainable and secure organizational growth, thanks to the security policies defined in the certification process. In particular, certification encourages a proactive approach to planning and managing IT assets. Positive perception of ISO 27001 certification by customers, partners, and other entities dealing with your organization helps builds trust, a key element for convincing others to do business with your organization.

"Positive perception of ISO 27001 certification by customers and partners builds their trust in your organization."

Four Myths about Certification to Be Busted before You Start

The success of your ISO 27001 certification depends on the notions and beliefs your employees hold about it. Misconceptions about the nature of certification can make them anxious about the effort required or dismissive of the advantage to be gained. The following misunderstandings are among the most frequent. They should be tackled as soon as they are detected.

Myth#1: ISO 27001 certification is "just an IT thing"

There is a tendency to consider the IT department as being solely responsible for implementing information security procedures. However, while information security includes IT, it also extends to include people and processes within and outside IT department. ISO 27001 certification is not therefore "just an IT thing." Senior management support in all departments is important for the successful implementation of an information security management system and the ISO 27001 certification to which it leads.

"Senior management support in all departments, not just IT, is important for successful information security management and ISO 27001 certification."

Myth #2: ISO 27001 certification is only a "bunch of documents"

At the heart of successful certification is clear, security-oriented thinking. Documents are used to organize the actions from that thinking, and to record the results. The set of records produced as part of the ISMS implementation helps the organization to determine whether the information security goals have been achieved as planned. The records also help in giving the management a quantitative measurement of the effectiveness of security systems. Consequently, documentation is an important part of ISO 27001 certification. However, documentation is not an end in itself.

Myth #3: ISO 27001 certification requires huge investment in technology

While investment in technology can be advantageous, focusing on technology alone misses the point. Above all, effective certification that brings real benefits to the enterprise means cultural change. An information security culture has to be embraced by the entire organization. Suitable, affordable technology can catalyze and accelerate this transformation. However, management and employees must make the necessary investment of time and effort too.

Myth #4: ISO 27001 certification is simply a marketing tactic

While ISO 27001 certification may well give an enterprise a competitive advantage or unique selling point, certification is more than a marketing tactic. The certification process can bring organizational enlightenment and encourage new improvements.

It should also enhance awareness among all employees of the value of the information they create and use, and of the responsibilities they have towards their customers. As a result, customer and stakeholder trust is strengthened, as is the reputation of the enterprise. The marketing benefit is just one of the several.

How to Implement Your ISMS and Become ISO 27001 Certified

The current version of the standard, ISO 27001:2013, consists of 114 security controls, 35 control objectives, and 14 security domains. Certification can nevertheless be done in a straightforward and efficient way. Below are 12 simple steps for an organization to proceed to certification and compliance.

Step 1: Get Management Buy-In

One of the main reasons for ISMS implementation failure is lack of cooperation from management. In some cases, budget allocations are too small. In others, too few human resources are assigned to perform successful implementation and certification. Better management engagement and cooperation can often be achieved by highlighting two areas. The first area is current security gaps within your organization that could negatively affect its results and reputation. The second is the positive opportunities certification offers to stimulate business growth. Security is most effective when embedded into a sound corporate governance framework.

Step 2: Define the Scope

It is important to identify the scope of the project to deploy an ISMS and achieve certification. This ensures there is a focused, systematic approach in implementing security best practices within your organization. A scope document is one of the mandatory documents to be presented as part of the certification audit.

Step 3: Establish a Governance Structure and an Information Security Policy

An ISMS implementation project needs to be correctly managed, like any other project in your organization. In particular, well defined roles and responsibilities are important for successful execution. It must also be remembered that adopting an ISMS in an organization is not an IT decision, but a business strategy decision. It is therefore important to identify an information security governance team or group that includes senior business executives, and that drives ISMS implementation across the organization.

> "Identify an information security governance team to drive ISMS implementation across your organization."

Your organization should then develop a detailed information security policy in consultation with its governance team. The information security policy is a governing or top-level document covering all the security requirements and based on best practices. The policy helps management to define the security goals in line with other organizational goals.

Step 4: Define Your Risk Management Methodology and Perform Risk Assessment

ISO 27001 takes a risk-based approach to information security. Risk assessment is therefore an important task in ISMS implementation. Before performing the risk assessment, it is important for your organization to identify the acceptable level of risk: in other words, its risk appetite. The goal of risk assessment is to then reduce the potential security risks that are not acceptable to the organization.

Your organization should define a methodology for conducting this risk assessment. As part of the assessment, an asset register should be developed with all the details concerning information assets (digital, paper-based, and any other kind.)

Your organization can then follow either an asset based or non-asset based approach for the risk assessment.

A risk management methodology should include rules for identifying:

- Information assets.
- Vulnerabilities in the organization, its processes, and systems affecting information security.
- Threats which could exploit these vulnerabilities
- The impact to the organization due to the threats being realized
- The probability of these threats occurring
- Existing controls used by the organization to mitigate these threats.

Your risk management methodology should define the parameters for quantitative or qualitative measurement of the vulnerabilities, threats, and risks. The risk ratings should take into consideration the existing controls. Your organization should also develop a risk register and create a risk assessment report that documents all the steps taken during risk assessment.

Step 5: Define Your Risk Treatment Plan and Make a Statement of Applicability

Based on the risks identified and their risk rating, a treatment plan should be defined. Risk treatment can include multiple decisions that are taken in consultation with management and the information security governance team. Your organization may refer to the 114 security controls provided in the ISO 27001 standard or to any control outside the standard for the risk mitigation.

The risk treatment plan should define how the control needs to be implemented, who is responsible for the implementation, and the timeline for implementation completion.

As an output of the risk assessment from Step 4, your organization should develop a Statement of Applicability document that defines the applicable controls for the organization. This document is presented to the auditor conducting the ISO 27001 certification audit.

Step 6: Develop an Information Security Framework

The information security framework contains the definition of the policies and processes for your organization to ensure the ISMS is implemented in the right way. The requirements for these policies and processes are identified as part of the risk assessment activity (Step 4.) The processes then act as risk mitigation steps.

> "Implementation of new security policies will mean a change in the culture of your organization."

Your organization can decide upon the extent of the set of process to be defined and implemented, according to the goals you have set for the project. If the management goal is simply an ISO 27001 certification, the framework can be restricted to the mandatory set of documents for the certification auditor. For a robust information security management system, a correspondingly comprehensive list of documents can be developed. The implementation of new policies will then mean a corresponding change in the culture of your organization.

Step 7: Conduct Security Awareness and Training Programs

Employees may baulk at changes in culture and behavior required by new policies and procedure. Training and awareness are therefore crucial steps in an ISMS implementation.

Security awareness of all employees in the different domains of security is mandated by the standard and part of certification. In addition to attending security awareness sessions, the team and stakeholders concerned by each process defined in Step 6 must be trained to enable them to properly implement that process. The process implementation might be a new way of working or the deployment of new technologies for better security.

Step 8: Operate and Monitor

With this step, the application of ISO 27001 and the ISMS becomes a daily routine in the organization. Each team should ensure it has internalized the cultural change required to ensure the security of the information that it handles. As part of the ISMS operations, your organization should implement a vulnerability management program to address technical security vulnerabilities in the devices and applications of your organization. As part of the documents required, you must maintain a record of the ISMS implementation and operation.

To ensure continuous improvement of the ISMS in your organization, it is important that the effectiveness of the security controls is measured frequently and that corrective actions are taken as and when needed. Metrics should be defined for all the security processes and controls for this. There should be a mechanism to report the effectiveness of your organization's ISMS to management and to the information security governance team.

Step 9: Validate ISO 27001 Certification Readiness

A frequent internal audit should be conducted to ensure the ISMS has been implemented in the right way and that the security objectives set by the management are being met through the ISMS. Internal audits should also ensure the readiness of your organization to receive the external auditor. Your organization should ensure that the proper preventive and corrective actions are identified and planned to resolve any identified non-compliance.

Step 10: Management Review

Management review meetings are of high importance for successful ISMS implementations and achieving the state of readiness required for ISO 27001 certification. Management should be informed about the progress of the implementation and about any decisions that have a major impact on the ISMS.

"Management review meetings are a major success factor in ISMS implementations and ISO 27001 certification."

Step 11: ISO 27001 Certification

A trusted partner like Paladion can make a critical difference in successful ISO 27001 certification. The identification of the right partner for assistance with certification is an important task. This partner should provide all the required documents to the auditor for the stage 1 audit. It should also demonstrate the implementation of security processes for the stage 2 audit, and play the role of subject matter expert in helping the internal teams to adopt new security practices. In addition, the partner should be available for the management review meeting that follows the certification audit.

Step 12: ISMS Automation

Your organization can also opt for a well-designed automation tool to accelerate the implementation of an ISMS and the ISO 27001 certification process.

The following features merit consideration when choosing an ISMS automation tool:

- Knowledge repository of information security vulnerabilities, threats, and security controls.
- Built-in customizable workflow.
- Built-in risk management methodology aligned to ISO 27001.
- Automated risk assessment process.
- Ready to use security awareness content.
- Out of the box ISO 27001 audit checklist as part of the compliance management feature.
- Automated tracking and closure of audit findings
- Reports and dashboards.

Further Questions and Answers for ISO 27001 certification

Who should be involved?

A typical ISO 27001 certification process will involve senior management, the CIO/CSO, the systems and network teams, the application teams, the physical security team, the legal and compliance team, and the human resources department, together with a Paladion consultant and an external certification auditor.

How much will it cost?

The cost of the project depends on the scope of the certification (security objectives, size of the organization, number of sites, departments, employees), the current security posture of

your organization, and the capacity of your organization to absorb improved security practices.

How long will it take?

The duration of the certification process depends on various parameters. These include the scope of the certification, the current security posture of your organization, resource availability, budget, any particular demands your organization has, prior ISO experience, and willingness to change. Remember also that the role of an information security management system implemented for certification is to provide continuing monitoring and improvement afterwards as well, because implementation does not stop at the certification. The framework has to be absorbed into the organization's BAU process and evolved over a period of time.

Conclusion

ISO 27001 certification can already be justified by the proof it offers to management, employees, customers, and other organizational stakeholders that information is being managed securely. In addition to building this trust, operational and strategic benefits allow an organization to identify a positive return on its investment of time and effort. Any myth or misconception that could compromise the success of certification should be dealt with as soon as possible. Thereafter, a progression of 12 simple steps can lead an organization to the implementation of an effective ISMS (information security management system) and the achievement of certification.

Paladion has already assisted many organizations of different sizes and in different industries to successfully obtain ISO 27001 certification. The market leading technology and services offered by Paladion can accelerate the certification process and help organizations to achieve and maintain an excellent, enduring security posture.

PALADION
HIGH SPEED CYBER DEFENSE

ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by independent analyst firms and awarded by CRN, Asian Banker, Red Herring, amongst others.

For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

WW Headquarters: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-844-507-7668

Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +97433559018, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net