uptime®

for reliability leaders and asset managers

aug/sept 18

THE 5 HABITS OF GREAT RELIABILITY ENGINEERS

uptimemagazine.com

WHY IS ISO27001 SECURITY STANDARD CERTIFICATION SO IMPORTANT?

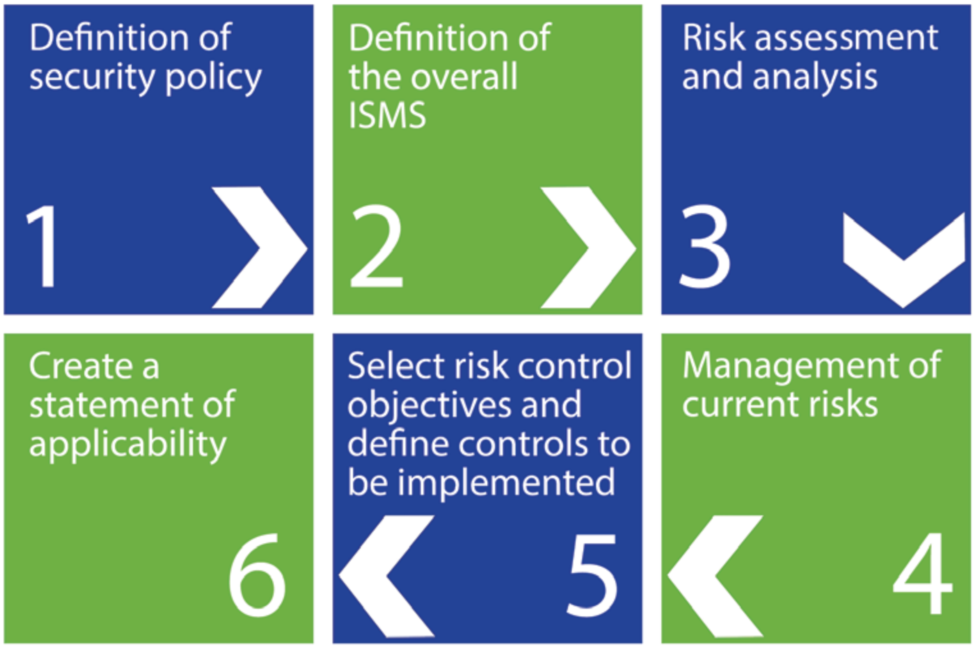
Tyler Caldwell

ISO27001 is a quality standards specification for information security management systems (ISMS). The ISMS is an overall framework that encapsulates business procedures and policies pertaining to the control of a company's information security risk management processes. It covers physical, technical and regulatory controls.

The stated goal of ISO27001 is to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system."

ISO27001 implements a six-part planning process, as shown in Figure 1.

The ISO27001 specification covers management responsibility, documentation, continual improvement, internal auditing, as well as corrective and proactive action. It is an enterprise-wide specification, with all business units falling under its mandate.



Definition of security policy 1

Definition of the overall ISMS 2

Risk assessment and analysis 3

Management of current risks 4

Select risk control objectives and define controls to be implemented 5

Create a statement of applicability 6

Figure 1: Information security management system planning process

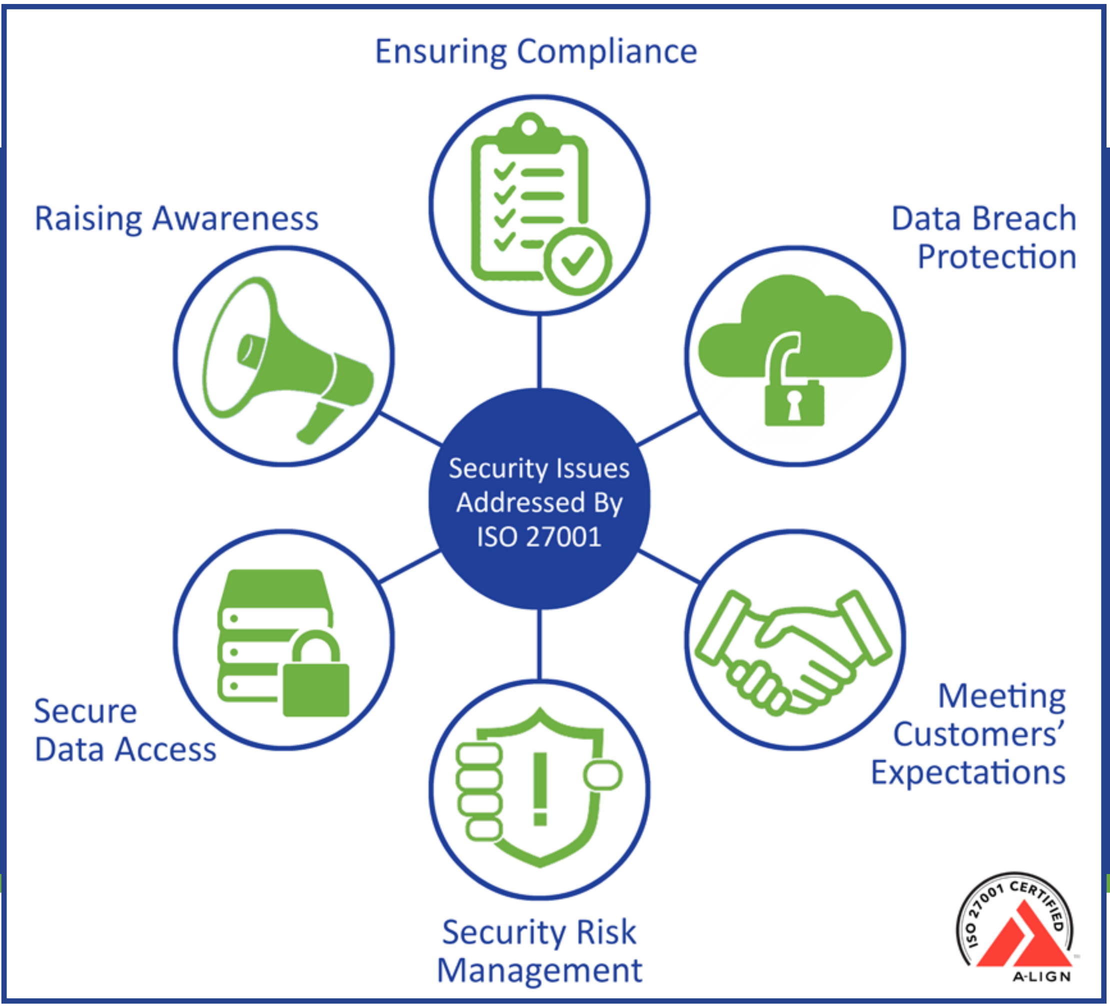


Figure 2: Security issues ISO27001 addresses

> At all times, companies should adhere to the three key requirements for all customers' information assets: **CONFIDENTIALITY, INTEGRITY** AND **AVAILABILITY**

Information Security Issues and How ISO27001 Helps

ISO27001 provides a feature-rich specification for solving many common information security issues. Key information security issues addressed by ISO27001 are:

- Compliance to stringent regulations by providing a governing framework for the management of security risks pertaining to information security, thus ensuring compliance.
- Data breach protection by forcing the identification of risks, as well as implementing procedures designed to detect security breaches. This can be accomplished by following an iterative security program that is regularly reviewed and revised to improve the effectiveness of an ISMS.
- Information availability by making data available when it is needed through secure processes that put information security first.
- Improved information security risk management that provides a framework for identifying risks to information assets and implementing the right technical and management controls. Due to the fact it is a risk-based doctrine, information security is achieved in a more efficient way.
- Meeting customers' expectations by demonstrating a company's competency in managing information security risks. ISO27001 is a recognized standard specification that will be instantly recognized and understood in tenders and proposals.
- Raising the awareness of information security in the enterprise, as senior management sponsorship demonstrates the seriousness of certification to the workforce. Staff training and awareness is a key facet of certification. Information security management systems are defined and key employees are given specific responsibilities. These responsibilities are monitored and measured to ensure adequate performance at all times.

Why Should Companies Take on the Challenge to Achieve ISO27001 Certification?

Customers expect companies to protect their information in a diligent manner. At all times, companies should adhere to the three key requirements for all customers' information assets: confidentiality, integrity and availability.

Having full ISO27001 certification demonstrates very clearly to customers that the company understands the issue of information security and continually strives to prove it is a safe and secure haven for their data assets.

How Does ISO27001 Certification Allow Companies to Better Position Themselves?

Achieving ISO27001 certification delivers a number of benefits to companies with regard to the image they can promote. Certification shows that a company is diligent in matters of security, not simply relating to the internal controls, but also in the management system it has built.

This system encompasses every member of the team, from the CEO on down. Every employee receives awareness training and there are physical and administrative controls in place to ensure policies are followed. The entire company has a role in security within this system.

How Difficult Is It to Achieve ISO27001?

The first year of certification is the most difficult. In the first year, the initial challenge of building controls and developing documentation needs to be overcome. In many cases, companies

> “This is the underpinning foundation of ISO27001 – identifying risks and deciding how to treat them”

have a lot of processes in place already that need better structuring and have to be documented.

Companies also may need to tackle the risk management aspects of certification. This is the underpinning foundation of ISO27001 – identifying risks and deciding how to treat them.

How Do Companies Maintain ISO27001 Certification?

The aim of ISO27001 is for a company's security program to not remain stagnant. The standard promotes the constant refinement of the security program, improving upon it year on year.

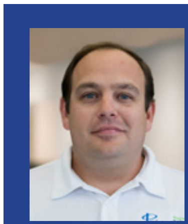
For example, as part of the initial certification process, a company identifies risks to information security. The company then sets a risk level it feels is acceptable. Going forward, the company's aim is to lower that risk level each year as its security program matures.

The key challenge for companies is to continue to identify new risks, as well as manage those identified risks better, with greater granularity, while improving its overall security program by adding new controls and developing new security processes. At the same time, companies must make sure employee training and awareness are maintained.

Why Is Security So Important in the Context of Cloud Computing?

Cloud adoption has been a major trend for several years now, however, one issue that is holding back late adopters is the concern of security, especially for those companies who use third-party providers. Companies require their critical operational data to be highly secure and can be apprehensive about moving their data to the Cloud. As such, companies should look for ISO27001 certified third-party providers who can not only meet their requirements, but exceed their expectations.

Most companies typically have their own IT infrastructure and their own security processes. These applications are typically installed within on-site data centers that are oftentimes mistakenly considered to be highly secure. Many times, they are legacy security systems securing the aged infrastructure. However, companies that become ISO27001 certified have the benefits of a certified security program when moving their information assets to a cloud solution. It is a security program that will mature and become more effective every year and keep up with the latest technology and security threats.



Tyler Caldwell, *Infrastructure/Information Security Manager, manages the infrastructure and security team at Projetech. Tyler's team ensures compliance with company information security policies relating to requirements from the ISO27001 standard, as well as aligning security needs with Projetech's SaaS solutions. www.projetech.com*