CYBERGUARD
COMPLIANCE

ISO 27001 Overview

More than ever, information security is one of the central concerns for companies. The volume, value, and sensitivity of company data is increasingly important. In order to protect this information, and to be seen to be protecting it, more and more companies are placing increased value on IT Compliance and Cybersecurity. For companies which specifically operate internationally, becoming ISO 27001 registered is a key component to gain the trust of your international clients.

The main drivers for security are undoubtedly globalization, government directives, regulatory requirements, terrorist activities, and escalating cyber threats. Furthermore, companies seeking opportunities to contract with governments or large corporate clients are discovering that ISO 27001 is often a prerequisite for doing business. Registration is therefore seen as a powerful assurance of your commitment to meet your obligations to customers and business partners.

Pursuing the right registration for your company can be overwhelming, particularly because there are so many variations. These variations are sometimes renamed or superseded by newer standards, which can cause some confusion.

Governance and Information Security

The last few years have seen corporate governance requirements become more defined and specific. Information technology has become more pervasive, underpinning and supporting almost every aspect of a company. The role of IT in corporate governance, in that case, has equally become more clearly defined and IT governance is increasingly recognized as a specific area for board and corporate attention.

The ISO 27000 Family of Standards

The ISO 27000 family of standards offers a set of specifications, codes of conduct, and best practice guidelines for companies that support strong IT service management. Of primary interest to information security are ISO 27001, ISO 27002 and ISO 27005.

ISO 27001 is a technology and vendor neutral information management standard, but it is not a guide. Of the above three standards for IT security governance, ISO 27001 offers the specification, which is a prescription of the features of an effective Information Security Management System (ISMS). As the specification, ISO 27001 states what is expected of an ISMS. This means that, in order to achieve registration or to pass an audit, your ISMS must conform to these requirements.

While ISO 27001 offers the specification, ISO 27002 provides the code of conduct, guidance, and recommended best practices that can be used to enforce the specification. ISO 27002, then, is the source of guidance for the selection and implementation of an effective ISMS. In effect, ISO 27002 is the second part of ISO 27001.

Just as ISO 27002 provides a set of guidelines for best practice in implementing an ISMS, ISO 27005 provides guidelines for information security risk management. As part of constructing a suitable and secure ISMS, you must assess the risks to your information and be prepared to mitigate these risks.

These information security standards are the essential starting point for any company commencing an information security project. Any company contemplating such a project should purchase and study copies of ISO 27001, ISO 27002, and ISO 27005. From the perspective of a larger company that uses ISO 31000 to structure its enterprise risk management system, ISO 27001 has been written to dovetail into the ISO 31000 guidance.

The Information Security and Regulatory Environments

The two key reasons for the growing interest in registration to ISO 27001 are the proliferation of cyber threats to information and the growing range of regulatory and statutory requirements that relate to the protection of information. Information security threats are global in nature, and indiscriminately target every company and individual who owns or uses (primarily) electronic information. These threats are automated and loose on the Internet. In addition, data is exposed to many other dangers, such as acts of nature, external attack, internal corruption, and theft.

The last fifteen years have seen the emergence of a growing body of legislation and regulation around information and data security. Some such regulations focus upon the protection of personal data, while others aim at corporate financial, operational, and risk management systems. A formal information security management system that provides guidance for the deployment of best practice is increasingly seen as a necessity in terms of compliance, and registration is increasingly required of companies (and governments) before they will engage in any significant commercial transactions.

International Recognition

In the United States, accreditation of registrars is handled by ANAB, which maintains a list of all companies qualified to approve ISO 27001 registrations.

ISO 27001 is not only recognized throughout the US, but also has a broader appeal in other key markets via the International Accreditation Forum (IAF). The IAF ensures that ISO 27001 registration is recognized across the world through a “mutual recognition arrangement”, agreed by more than 60 national accreditation bodies.

Market Value of Registration

In addition to the protection of your data and compliance with laws that mandate secure data handling like HIPAA, it is simple to argue that there is a distinct market value to ISO 27001 registration. It is financially prudent to protect your company’s data and to meet the legal requirements of nations in which you seek to do business.

Achieving registration is a valuable and visible proof of your company’s willingness to meet internationally-accepted data security standards. Achieving this international standard is not simply marketing: as nations implement their own regulations regarding data protection such as the UK’s Data Protection Act, Canada’s PIPEDA, and the EU’s General Data Protection Regulation (GDPR), the ability to prove that your company complies with ISO 27001 is likely to open business opportunities across the globe. It should be noted that many markets have already shown a desire for ISO 27001 registration, with over 22,000 companies worldwide having achieved registration.

Registration vs Conformance

It is possible for a company to simply select controls from those provided in ISO 27002 because the good practice identified is universally applicable. Because it was not designed to be the basis of a registration scheme, however, it does not specify the system requirements with which an ISMS must be compliant in order to qualify for registration.

Those specifications are contained in ISO 27001. In technical terms, this means that a company that is using ISO 27002 on its own can conform to the guidance of the code of practice, but it cannot get an outside body to verify that it is complying with a standard. A company that is using ISO 27001 and ISO 27002 in conjunction with one another can design an ISMS that is in line with the specification and which follows the guidance of the code of practice and is, therefore, capable of achieving external registration.

In order to achieve internationally-recognized registration, your ISMS must be audited by an auditing firm approved by the appropriate body associated with the EA and IAF (in the US, this is the ANAB).

Registration and Other Management Standards

ISO 27001 is designed to be compatible with other management standards, such as ISO 9001 and ISO 14001. It is also compatible with ISO 31000 and ISO 20000. The numbering systems and document management requirements are designed to be compatible, and thus enable companies to develop management systems that integrate the requirements of each standard a company may be using.

This compatibility is currently being improved through the adoption of Annex SL, which lays out a standardized structure for management standards. This enables companies to more readily adopt new standards and to minimize overlaps and interference. Companies should seek ISO 27001 registration from the registrar they currently use (e.g. CyberGuard Compliance) for registering their ISO 9001 or other management system. The experience of the company's quality manager in this process will be invaluable to the ISMS project.

Information Security and Technology

Most people think of information security as a technology issue. They think that anything to do with securing data or protecting computers from threats is something that only technological specialists, and specifically computer security professionals, can deal with.

This could not be further from the truth. It is the computer user who should decide which threats are to be protected from, and what trade-offs between security and flexibility he or she is prepared to accept. Yes, once these decisions have been made, the computer security expert should design and implement a technological solution that delivers these results, but they should operate according to the user’s risk assessment.

In an organizational environment, those decisions should be made by the management team, not by the IT team. An ISMS overtly and specifically recognizes that decision-making responsibility should sit with the company's management and that the ISMS should reflect their choices and provide evidence as to how effective the implementation has been.

As a result, it is not necessary for an ISMS project to be led by a technology expert. In fact, there are many circumstances which can be counter-productive. These projects are often led by quality managers, general managers, or other executives who can develop something that has a company-wide influence and importance.

Preparing for an ISMS Project and the Continual Improvement Cycle

The Plan Do Check Act (PDCA) cycle is a continual improvement methodology that was conceived in the 1950s by W. Edwards Deming and says that business processes should be treated as though they are in a continuous feedback loop so that managers can identify and change those parts of the process that need improvement. An ISMS project can be a complex one. It is likely to encompass the entire company and should involve everyone from the management down to the mail room operatives.

Implementation may well take many months or, in some cases, years. ISO 27001 offers a structured approach to the development and implementation of the ISMS. The clauses describe the requirements of the ISMS and Annex A provides controls that can be used to manage the specific risks that the company faces. There are no mandated stages to the project, but you need to apply a continual improvement process from the outset and the PDCA cycle is one possible methodology.

The process, or an improvement to the process, should first be planned, then implemented and its performance measured. By comparing these measurements against the planned specification, you will be able to identify any deviations or potential improvements. These can then be reported to management for a decision regarding the correct action to take.

Risk Assessment and Risk Treatment Plans

An ISMS must be designed to meet the individual requirements of each company. Not only does every company have its own specific business model, objectives, unique selling features, and culture, it also has different appetites for risk. In other words, something that one company sees as a threat that it must mitigate, another might see as an opportunity that it should grasp.

Similarly, one company may be less prepared to invest in defenses against an identified risk than another. For this and other reasons, every company that implements an ISMS must do so against the results of a risk assessment whose methodology, findings, and recommendations have been approved by the board of directors. ISO 27001, in fact, requires a risk assessment to be carried out and, while it does not specify a methodology, it is very clear that this risk assessment must produce consistent, valid, and comparable results to analyze and assess the risks.

While ISO 27001 offers no specific methodology for identifying risks, ISO 27005 is designed to assist the satisfactory implementation of information security based on a risk management approach. It supports the general concepts specified in ISO 27001 and offers a structured and rigorous process for analyzing risks and creating the risk treatment plan.

System Documentation

The most time-consuming, and frankly the most critical, part of the entire project is the development of the documentation that sets out how the ISMS works. There are several different approaches to this process, from using external consultants to tackling it in-house. The major argument in favor of performing this task in-house (apart from reducing or avoiding consultancy costs) is that you will develop a greater depth and awareness of your internal security environment. By developing such expertise and experience within the company, any further such projects can be dealt with more quickly and with a greater degree of confidence.

Contact CyberGuard Compliance

CyberGuard Compliance has assembled top tier leadership to help our current and prospective clients through the entire ISO 27001 process. For further information regarding ISO 27001, or to request a free consultation from CyberGuard Compliance, please visit their “Contact Us” page to submit an informational form or call 866.480.9485 today. Or, feel free to contact the ISO Practice Leader directly:

Gary Pennington, CIA | ISO Practice Leader

T/ 866.480.9485

E/ ContactUs@CGCompliance.com