QUALITYDIGEST

Published on *Quality Digest* (http://www.qualitydigest.com)

Implementing ISO/IEC 27001

By: BSI Management Systems

How secure do you want your information to be?

With security breaches on the rise, protecting your organization's confidential and valuable information assets is one of the most important safety measures your organization can take. The issues surrounding information security involve more than just hackers and malicious software; they can involve employees, computer theft, and trespassing. Safeguarding information in the 21st century requires a thorough hardening of security processes, procedures, and stated policies that are based on internationally accepted best practices to improve information security defenses and to meet legal, contractual, and regulatory requirements.

In the United States, there are always documented high-profile security breaches that make national headline news. When valuable information is stored and transmitted in a number of different ways, keeping track of that information to ensure it remains secure is difficult to say the least. Since the new era of computer technology, information security has involved securing not just hard copy information, whether stored or sent via postal mail or courier, but also all electronic forms of information, including information stored electronically on a computer or server or sent via some electronic means.

The question then is: How do you safeguard all information?

Safeguarding information is not an exact science and depends on a number of variables, from employee and vendor conduct and disclosure to robbery and theft. The international standard, ISO/IEC 27001—"Information technology—Security techniques—Information security management systems—Requirements," is the result of efforts to address this growing issue.

A brief background of ISO/IEC 27001

The concepts behind ISO/IEC 27001 began in the United Kingdom in the late 1980s, when the United Kingdom Department of Trade and Industry's commercial computer security center developed and wrote a code of good security practice. This code was published as BS 7799 by British Standards Institution (BSI) in 1995.

In 1999, BSI published BS 7799 Part 2—"Information security management systems

—Specification with guidance for use," designed to focus on how to implement an information security management system. It was adopted by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 27001 in November 2005.

Why should organizations implement ISO/IEC 27001?

The information security management system (ISMS) is a systematic approach to managing sensitive company information and mitigating information security issues. The standard ISO/IEC 27001 is designed to help organizations identify, manage, and quantify their information security risks by ensuring the selection of adequate and proportionate security controls.

Today, the international standard ISO/IEC 27001 provides a common framework and specifies requirements for establishing, implementing, and documenting an ISMS. It also specifies security controls an organization can implement to identify the most appropriate control objectives and controls applicable to its own needs. This standard forms the basis of an assessment of the ISMS of the entire organization, or a part of it.

Relevancy of ISO/IEC 27001

ISO/IEC 27001 is relevant for any organization, large or small, in any sector or part of the world. All organizations have confidential and valuable information assets, especially in sectors in which information protection is critical, such as the financial services, health, public, and IT sectors. The standard is also relevant to those organizations that manage information on behalf of others, such as an IT outsourcing firm, and can be used to assure customers that their information is being properly managed and protected.

The framework and processes involved in the ISMS standard can be modified to reflect different business needs, and can be adopted by any organization to manage and mitigate its information security risks. Many organizations possess intellectual property and trade secrets, and while nondisclosure agreements will help protect that valuable information, it does not necessarily mean important information will be contained.

With so many security risks in today's world, it has become increasingly important to continuously improve information security protection efforts. Information security breaches and regulatory noncompliance issues expose organizations to significant increases in tangible and intangible costs, including large fines and charges, loss of customer confidence, damage to corporate reputation, regulatory scrutiny, loss of market share, criminal and civil lawsuits, and can expose consumers to potential identity theft and credit card fraud. Return on investment can now mean reduced risk of imprisonment, reduced risk of investigation, return on insurance, and reduction of incidents.

Improving management systems has become more important than ever in protecting organizations against a growing number of risks. By implementing ISO/IEC 27001, an organization stands a better chance of fighting against information security theft and fraud, and protecting its economic growth, corporate reputation, and its future.

Benefits of implementing ISO/IEC 27001

Implementing the ISMS standard has a number of valuable benefits that can help organizations improve their operations and protect their information assets.

ISO/IEC 27001 provides a common framework and a structured and proactive approach to establishing an ISMS, enabling you to develop, implement, and effectively measure security management practices.

Implementation of the standard allows you to ensure the right people, processes, procedures, and technologies are in place to protect information assets, and demonstrates an independent assurance of your internal controls and meets corporate governance and business continuity requirements.

Additionally, implementation provides a competitive edge by meeting contractual requirements and demonstrating to your customers that the security of their information is important. Independent verification of your system signifies that your organizational risks are properly identified, assessed, and managed, and formalizes information security processes, procedures, and documentation.

Steps to implementing ISO/IEC 27001

Implementing ISO/IEC 27001 involves a number of key steps that an organization will need to consider along the way. When it comes to developing an ISMS, giving it thorough attention will better enable your organization to move through the process effectively and efficiently to create an effective management system that will help protect your organization against risks and dangers

.

Purchase the standard. Purchasing and reading the standard, which is a document that provides a specification for an ISMS and the foundation for third-party audits and certification, will enable your organization to fully understand the fundamentals, guidelines, and requirements of the ISO/IEC 27001 standard.

Consider training. Training is an effective way for an organization to gain the knowledge and skills necessary to understand and implement the ISO/IEC 27001 standard. There is a comprehensive set of training courses available for those organizations that are implementing the standard, from beginner level courses on understanding and implementing the standard to advanced courses in auditing an ISMS.

Assemble a team and agree on your strategy. Gaining full executive management involvement in the implementation process of an ISMS is important to the success of the system. Without involvement and acceptance from top executives, middle managers can experience difficulty in making the case for the system and the implementation process can crumble. Once the team is assembled, determine whether the system will be adopted companywide or by one or more departments.

Review consultancy options. Seeking the advice from an independent consultant will help facilitate the implementation process of the standard, providing your organization with valuable feedback and information to help you make appropriate decisions.

Undertake a risk assessment. To make the most of your ISMS and make it work effectively, conduct a risk assessment of potential security breaches to determine current and potential risks to which your organization is exposed. This review should include all sensitive data within your organization, not just your IT systems. This step will help your organization tailor the standard's guidelines and requirements to reflect specific needs of your ISMS and help to identify proper control objectives and controls applicable to those needs.

Develop a policy document. Creating a policy document provides a written document that details the policies your organization will utilize in implementing your ISMS. It also demonstrates executive management support and commitment to the ISMS process. Distributing it to your staff members and vendors will help ensure that company policies are followed.

Develop supporting documents. Put together a “Statement of Applicability and Procedures” to support your security policy. This should cover a range of areas including asset classification and control, personnel security, physical and environmental security, and business continuity management.

Implement your system. Once you have completed the above steps, it is time to apply your ISMS to your organization. The key to implementing your ISMS is communication and training. During the implementation phase, your organization will begin to operate according to the procedures of the management system; and having gained skills and knowledge for an ISMS will help facilitate the implementation process.

Choose a certification body. Utilizing the ISO/IEC 27001 doesn't stop at implementation. Choosing to certify your system is a pragmatic approach to taking proactive steps in ensuring your organization’s information security and is an important business decision that must have executive management approval for success. Working with an independent, accredited certification body (CB), like BSI Management Systems, to gain certification will demonstrate to customers and stakeholders that your organization is committed to ensuring the safety of valuable information assets.

When choosing your CB, ask for references and keep the following questions in mind to select a CB with relevant experience in your industry and that offers cost-effective quality service.

- Has the CB worked with your industry?
- Will you have the same assessor each time?
- Are assessors or client managers assigned based on technical compatibility or geography?
- How long does it take to receive a certificate after an audit?
- How are disputes handled?
- How do you ensure consistency in audit interpretation?
- What is the typical response time allowed for a nonconformity?
- How mature should the management review process be?

Gain certification. Certification (referred to as “registration” in the United States) to the standard by an independent, accredited, CB demonstrates compliance of an internationally accepted standard and helps address current and future regulatory compliance requirements in a proactive, cost-effective, and sustainable manner. Your CB will walk you through the steps to help ensure your organization achieves certification when the final step of the assessment is complete. An optional preassessment audit is also available to evaluate your ISMS and determine your readiness for assessment.

Once your organization achieves certification, your CB will issue you a certificate of certification to the ISO/IEC 27001 standard, which you can use to promote your success and your compliance.

Continual assessment. As operations in your organization are modified to adjust to current conditions, it is important to assess and update your ISMS on a regular basis to ensure your organization is protected from security issues and always remains in compliance with ISO/IEC

27001. Your CB will check your ISMS periodically so that it continues to meet the requirements of the standard.

As information security risks increase worldwide, organizations need to establish an ISMS and continuously assess and update their information security measures to protect their organization, corporate reputation, economic growth, and their customers.

For more information, BSI is holding a free webinar on Feb. 10, 2010, at 1 p.m. EST. To read more about the webinar or to register, visit www.bsiamerica.com/ISMSbenefits [1].

Quality Insider Article Standards Article Twitter Ed

- Home
- the Insider
- Videos
- Magazine
- Resources
- Search
- Subscribe
- Advertise
- About Us

Source URL (retrieved on *02/22/2010*): http://www.qualitydigest.com/inside/quality-insider-article/implementing-isoiec-27001.html

Links:
[1] http://www.bsiamerica.com/ISMSbenefits