



Overview

- What is ISO27001, and how does this standard help organizations more effectively manage their information security?
- What's the relationship between ISO27001 and ISO17799?
- How do these standards relate to ISO9001?
- What does someone coming to this field for the first time need to know in order to initiate, or take on responsibility for, an organizational information security project, and specifically one that is intended to lead to ISO27001 certification?

This paper, written by ISO27001 expert Alan Calder, answers these basic questions and others and points to online resources and tools that are useful to anyone tasked with leading an information security project.

The information in this paper is suitable for all sizes of organizations, and all sectors, anywhere in the world. It reflects the guidance and information available from **The ISO27001 Site**, which can be accessed through www.27001.com

IT Governance and information security

The last few years have seen board corporate governance requirements increasingly more defined and specific. As information technology has become pervasive, underpinning and supporting almost every aspect of the organization, manipulating and storing the information on which the organization depends for its survival, so the role of IT in corporate governance has become more clearly defined and IT governance is increasingly recognised as a specific area for board and corporate attention. A fundamental aspect of IT governance is the protection of the information – and the *availability, confidentiality and integrity* – on which everything else depends.

In parallel, international standards related to information security have emerged and have become one of the cornerstones of an effective IT governance framework.

The information security standards

ISO27001 was preceded by BS7799, which was created in 1995, by the British Standards Institution (BSI). It was a standard to guide the development and implementation of an **Information Security Management System**, commonly known as an *ISMS*.

BS7799 was conceived, from the outset, as a technology-neutral, vendor-neutral **management** system that, properly implemented, would enable an organization's management to assure itself that its information security measures and arrangements were effective.

From the outset, BS7799 focused on protecting the *availability, confidentiality and integrity* of organizational information and these remain, today, the driving objectives of the standard.

Information Security and ISO27001 – an Introduction

Crucially though, it doesn't talk about protection from every single possible threat, but only from those that the organization considers relevant and only to the extent that is justified financially and commercially through a risk assessment.

BS7799 was originally just a single standard, and had the status of a Code of Practice. In other words, it provided guidance for organizations, but hadn't been written as specification that could form the basis of an external third party verification and certification scheme.

As more and more organizations began to recognize the scale, severity and interconnectedness of information security threats, and with the emergence of a growing range of data protection and privacy-related law and regulation, so the demand for a certification option linked to the standard began to develop.

This led, eventually, to the emergence of a second part to the standard, in the form of a specification (a specification uses words like 'shall') numbered as BS7799-2 (or, part 2).

The Code of Practice (which uses words like 'may' and which deals with controls, not with Information Security Management Systems), is now recognized under the dual numbers of ISO17799 and BS7799-1 (or, part 1). It will soon be re-issued with the new number ISO27002.

The relationship between the Code of Practice and the specification was also established at this time: a specification is the basis for certification schemes and ISO27001 mandates the use of ISO17799 as the source of guidance for the selection and implementation of the controls mandated by ISO27001. In effect, ISO 17799 is the second part of ISO 27001.

The most recent version of the Code of Practice, and the one which must be used, is ISO/IEC 17799:2005. BS7799-2:2002 has also undergone revision and internationalisation, and was replaced in November 2005 by ISO/IEC 27001:2005. BS7799-2:2002 has now been withdrawn.

The ISO27000 series of standards will expand over the next few years. A list of those standards already under development is at www.27001.com/Standards.aspx

The information security standards are the essential starting point for any organization that is commencing an information security project. Anyone contemplating such a project should purchase and study copies of both standards, which are available for online purchase in a money-saving kit, in either hard copy or electronic format, from: www.27001.com/products/28.

The information security and regulatory environments

The two key reasons for the growing interest in certification to ISO27001 are the proliferation of threats to information and the growing range of regulatory and statutory requirements that relate to information protection.

Information security threats are global in nature, and indiscriminately target every organization 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, from acts of nature, through external attack to internal corruption and theft.

The last ten years have also seen the emergence of a growing body of legislation and regulation around information and data security, some aimed at ensuring that individual data is protected and some aimed at ensuring that corporate financial, operational and risk management systems are appropriately underpinned. ISO27001 is immensely valuable in demonstrating compliance with laws such as SOX, HIPAA, GLBA, PIPEDA, State Breach Laws, and so on – find more information at www.27001.com/Compliance.aspx

Information Security and ISO27001 – an Introduction

A formal information security management system, that provides guidance for the deployment of best practice, is increasingly seen as a necessity in compliance terms and certification is increasingly required of organizations (and governments) before they will engage in any significant commercial transactions with potential new suppliers. The implications of this for the outsourcing industry are self evident.

The argument for deployment of a formal ISMS are fully developed in a short book called *The Case for ISO 27001*. Available online from www.27001.com/products/13, this book is also designed to provide a project manager with the arguments that may be necessary to get the organization's board to make the appropriate commitment to the project.

Certification vs conformance

It is possible for an organization to develop its ISMS in line with ISO17799 only, because the good practice identified in this Code of Practice is universally applicable. However, because it was not designed to be the basis of a certification scheme, it doesn't specify the system requirements with which an ISMS must be compliant if it is to be so certified.

ISO27001 does contain those specifications. In technical terms, this means that an organization that is using ISO17799 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 the standard. An organization that is using ISO27001 and ISO17799 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 which is therefore capable of achieving external certification.

Certification and other management standards

ISO27001 is designed to be compatible with other management standards such as ISO9001 and ISO14001. It is also compatible with ISO/IEC 20000:2005. The numbering systems and document management requirements are designed to be compatible and to enable organizations to develop management systems that integrate to as great an extent as possible the requirements of each of the management standards that the organization is using.

Generally speaking, organizations should seek ISO27001 certification from the certification body they currently use for certifying their ISO9000 or other management system. The experience of the organization's quality manager in this process will be invaluable to the ISMS project.

There is no reason, however, why organizations shouldn't tackle ISO27001 without having first implemented any other form of management system. In that case, they will choose a certification body on a commercial basis from amongst those available and operating in their country.

A certification body must be accredited by a national accreditation body for it to be allowed to carry out accredited certifications and to award the relevant badge that formally signifies certification. Most countries have their own accreditation services (in the US, for instance, it is ANAB – www.anab.org) and these will all maintain lists of the organizations who are accredited for ISMS certifications.

The website has links (www.27001.com/page.links) to the major international certification organizations.

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 technology people – and specifically computer security people – can deal with.

Information Security and ISO27001 – an Introduction

Nothing could be further from the truth.

The computer user is the person who should make decisions about which threats 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.

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 organization's board and management, and that the ISMS should reflect their choices and provide evidence as to the effectiveness with which they have been carried out.

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

Preparing for an ISMS project and the PDCA cycle

An ISMS project can be a complex one. It is likely to encompass the entire organization, it should involve everyone from the management down to the post room operatives, and it may well take many months – and, in some cases, years.

ISO27001 certification is still relatively new and, as a result, hard experience of successful implementations is in short supply. This means that the handful of publications that describe, from a practical and pragmatic point of view, how to go about achieving certification, should be studied at an early point in the project planning process.

The two most relevant books are,

1. *Nine Steps to Success: an ISO27001 Implementation Overview* (www.27001.com/products/12) and,
2. *International IT Governance: an Executive Guide to ISO27001/ISO17799* (www.27001.com/products/16).

The first book (available in both eBook and soft cover formats) is a short but thorough overview of the steps that are critical to success, while the second (which is also the Open University's post-graduate information security textbook) is a detailed and widely used practical guide to implementing a certified ISMS which was written for non-technical readers and is now in its third edition.

It is web-enabled and gives its readers free access to an online KnowledgeBank of specialist and current information related to ISMS implementations.

ISO27001 sets out how an organization should approach its ISMS project and specifies the components that are essential. You can download a free PowerPoint presentation from www.27001.com/ISMSFreeDemo.aspx that provides an overview of the ISMS project, the time line and the various options for how you might tackle it. As you will see, there are specified stages to the project and what is called the PDCA cycle must be followed.

The PDCA cycle is the Plan-Do-Check-Act cycle that was originated in the 1950s by W. Edwards Deming and which says that 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.

Information Security and ISO27001 – an Introduction

The process, or an improvement to the process, should first be planned, then implemented and its performance measured, then the measurements should be checked against the planned specification and any deviations or potential improvements identified, and reported to management for a decision about what action to take.

Risk assessment and risk treatment plans

An ISMS must be developed and designed to meet the individual requirements of each organization.

Not only does every organization have its own specific business model, objectives, unique selling features and culture, it also has its different appetites for risk. In other words, something that one organization sees as a threat against which it must guard, another might see as an opportunity that it should grasp.

Similarly, one organization might be less prepared to invest in defences against an identified risk than another. For this, and other reasons, every organization that implements an ISMS must do so against the findings of a *risk assessment* whose methodology, findings and recommendations have been approved by the board of directors.

ISO27001, in fact, requires there to be a risk assessment and, while it does not specify a methodology, is very clear that this risk assessment must be based on identifying threats and vulnerabilities at an individual asset level and, from there, analysing and assessing risks.

The recently published risk assessment standard, BS7799-3:2006 provides guidance on risk assessment (www.27001.com/products/29).

Comprehensive guidance on ISO27001 risk management is available in *Information Security Risk Management for ISO27001/ISO17799* (www.27001.com/products/24).

Most organizations will find that risk assessment is impossible without using some form of database risk assessment tool. One can develop one's own tool, or use one that is pre-designed to meet the specific requirements of both ISO27001 and BS7799-3, such as vsRisk, which is available on CD-Rom. It can be quickly and easily be deployed on the desktop. More information is at: www.27001.com/products/31

System documentation

The most time-consuming, but most critical part of the entire project is the development of the documentation that sets out how the ISMS works.

There are a number of different possible approaches to this, from using external consultants to tackling it yourself. The major argument in favour of doing it yourself (apart from avoiding, or reducing, consultancy costs) is that you will develop in your organization a much greater depth and awareness of 'how to do security'.

Without previous experience, development of all the documentation required can be a daunting task, unless you deploy a pre-completed, templated documentation toolkit, like the one that can be found at www.27001.com/ISMSFreeDemo.aspx. This page provides access to an option so that the toolkit (which is linked to *IT Governance: a Manager's Guide to Data Security and BS7799/ISO17799*) can be trialled for free, and also provides other information and resources around ISMS documentation.

Policy Management

All organizations face the challenge of effectively deploying their ISMS documentation, ensuring that it is properly controlled, that it is accessible to everyone who needs to see it, and that there is evidence that users have read and understood all those policies that apply to

Information Security and ISO27001 – an Introduction

them. This sort of audit trail is becoming increasingly important as information-related regulation becomes more wide-spread. The most practical way of dealing with all the policy-management challenges is to deploy a policy management tool. There is more information about these tools here: www.itgovernance.co.uk/page.qpulse.

Training

The best training starting point is:

- Webinar – Mastering ISO27001/ISO17799 (www.27001.com/products/45)
-

COMPLETE ISO27001 ISMS RESOURCES

The ISO27001 One-Stop-Shop	http://www.27001.com
Information security standards online	http://www.27001.com/catalog/11
Risk assessment standard	http://www.27001.com/products/29
Risk Management Book	http://www.27001.com/products/24
Risk assessment tool vsRisk™	http://www.27001.com/products/31
Policy management tool	http://www.itgovernance.co.uk/page.qpulse
<i>The Case for ISO 27001</i>	http://www.27001.com/products/13
<i>Nine Steps to Success: an ISO 27001 Implementation Overview</i>	http://www.27001.com/products/12
<i>International IT Governance: an Executive Guide to ISO27001/ISO1779</i>	http://www.27001.com/products/16
Links to Certification Bodies	http://www.27001.com/page.links
27001 ISMS Documentation Toolkit	http://www.27001.com/catalog/10
ISO 27001 Webinar	http://www.27001.com/products/45

WWW.27001.COM

TOLL FREE: 1-877 317 3454