Chapter 1
Introduction to International Standards Organization Security Standards

This chapter begins by assuming the reader is generally familiar with information security, including what it is, and the potential application of information security within the organization. The assumption is that reader motivations are to apply a discipline to information security to be better at planning, implementing, and maintaining information security and achieving a highly effective information security program that is capable of receiving ISO 27001 certification. This chapter begins discussing such a discipline with an overview of security standards and with specific attention to existing and emerging International Standards Organization (ISO) security standards.

1.1 Objectives

Objectives for this chapter include presentation of the following:

- The cornerstones of information security
- A brief history of the ISO security standards
- A list of ISO security standards and the intent behind each
- An introduction to ISO 27001 and ISO 27002

© 2008 by Taylor & Francis Group, LLC
2  How to Achieve 27001 Certification

- The relationship between ISO 27001 and ISO 27002
- The relationship of ISO 27001 and ISO 27002 to other ISO management standards
- An introduction to the Plan-Do-Check-Act (PDCA) model

This material provides the basis for an introduction of the information security management system (ISMS), which is the foundation of achieving ISO 27001 certification.

1.2 Cornerstones of Information Security

Traditional organizational assets are predominantly tangible in the form of property, equipment, buildings, desks, money, or other negotiable assets, like gold. Security concerns were mostly physical, in the form of guards, walls, vaults, and safes. Organizational assets today have added virtual assets like intellectual property in the form of electronic-based media (e.g., word processing files, spreadsheets, and databases). Moreover, negotiable assets are bits on a hard drive and transactions are executed via bit transfers on a network, wired or wireless. Organizational wealth is largely represented by cyber bits; hence, there is a need to protect these assets via information security controls. The traditional view of information security includes the three cornerstones of information security: confidentiality, integrity, and availability, also known as the CIA of information security. Confidentiality, integrity, and availability are security objectives where the intent of confidentiality is to ensure that only authorized personnel may access information or, to the contrary, ensure that information is not disclosed to unauthorized persons or entities (e.g., automated system or service). To ensure integrity is to guard against unauthorized modification or destruction of information, or that the information remains in the format the creator intended. A loss of integrity is the unauthorized modification or destruction of information. Availability ensures information is ready for use. A loss of availability is the disruption of access to or use of information or an information technology. Figure 1.1 illustrates the three cornerstones of confidentiality, integrity, and availability (CIA). FIPS PUB 199 contains more detail on the three cornerstones of information security.

![Security cornerstones](image-url)

© 2008 by Taylor & Francis Group, LLC
How can an organization manage information security and the three cornerstones of security? One answer is to implement an ISMS and use the ISO standards as a guide to develop an effective ISMS. PDCA provides the methodology to implement an ISMS. ISO 27002 (formerly ISO 17799) provides the foundation for an effective ISMS, and ISO 27001 provides guidance on how to implement an ISMS via the PDCA process.

1.3 The History of ISO Information Security Standards

The U.K. Department of Trade and Industry (DTI) established a working group to produce a code of good security practice. The DTI published the *User Code of Practice* standard in 1989. This standard was essentially a list of security controls that at the time were considered suitable, normal, and good practice, as well as applicable to the technology and environment of the time.

Figure 1.2 presents the development of ISO 27001 and the ISO 17799 (ISO 27002). The DTI user code of practice was published as a British Standard (BS) guidance document and later as a BS with the name BS 7799:1995, Part 1. Part 1 includes a list of controls that was a set of best practices for information security. A second part of the standard was added as BS 7799:1998, Part 2. The intent of Part 2 was an instrument to measure and monitor Part 1 and to provide a benchmark for certification. Following subsequent revision, Part 1 was published as

Figure 1.2 Development of the ISO 27001 and ISO 27002 standards.

© 2008 by Taylor & Francis Group, LLC
How to Achieve 27001 Certification

BS 7799:1999, Part 1, proposed as an international standard (ISO), and published as ISO 17799:2000. Revision of Part 2 was released as BS 7799:2002, Part 2. The standard ISO 17799 was revised yet again and released as ISO 17799:2005, then a name change to ISO 27002:2005 in July 2007 BS 7799, Part 2 was then proposed as an international standard and was published as ISO 27001:2005. The next section presents the ISO road map for international information security standards in the new 27000 series.

1.4 Information Security Standards
Road Map and Numbering

The ISO and the International Electrotechnical Commission (IEC) work jointly on international standards and guidelines. One joint objective is to produce security management standards. The collective effort for producing security standards includes Working Group 1 (WG1), Working Group 2 (WG2), and Working Group 3 (WG3). All these working groups are part of Subcommittee 27 (SC27), which is in turn part of Joint Technical Committee 1 (JTC1). The scope of WG1 is security management standards including areas pertaining to new developments of standards in information security and development of ISMS standards. The aim of WG1 is to have a road map that identifies the requirements for a future set of international standards and guidelines to establish, implement, operate, monitor, and maintain ISMS. To support this road map, the ISO/IEC has decided on a new number series (27000) for international information security standards.

1.5 International Security Management Standards

Table 1.1 presents a list and brief description of some security standards that are or will be published in the ISO 27000 series. Anything marked “pending” is speculative at the time of this writing.

Table 1.1 ISO 27000 Family

<table>
<thead>
<tr>
<th>ISO/IEC Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Pending) Vocabulary and definitions.</td>
<td></td>
</tr>
<tr>
<td>27001</td>
<td>Information Security Management System requirements (specification)</td>
</tr>
<tr>
<td>27002</td>
<td>Code of practice for information security; management</td>
</tr>
<tr>
<td>27003</td>
<td>(Pending) Implementation guidance</td>
</tr>
<tr>
<td>27004</td>
<td>(Pending) Metric and measurement</td>
</tr>
<tr>
<td>27005</td>
<td>(Pending) Risk management</td>
</tr>
</tbody>
</table>

© 2008 by Taylor & Francis Group, LLC
The ISO 27001 standard is discussed in detail throughout this text and is a new international security standard based on BS 7799, Part 2. Organizations that have been certified against BS 7799, Part 2 will have to renew their certification with the latest ISO 27001 standard. ISO 27002 is the new name for ISO 17799. ISO/IEC 27003 covers implementation guidance and is based on Annex B of BS 7799, Part 2; the date for publishing this standard is pending. The PDCA model, also covered in BS 7799, Part 2 (and ISO 27001), not only is used to implement information security standards, but is widely used to implement other management standards, including ISO 9001 and ISO 14001. ISO 27004 will address how to implement metrics to measure to gauge the performance and effectiveness of ISMS operations; again, the date of publishing is pending. ISO 27005 will likely cover risk management and will be comparable to BS 7799, Part 3, Guideline for Information Security Risk Management. Other planned standards at this time in the ISO 27000 series are ISO 27006, which is likely to cover the guide to the certification/registration process, and the ISO 27007 Guideline for auditing Information Security Management Systems.

1.6 Other Proposed Information Security Standards

ISO is considering a few other standards, all of which will be part of an international information security management standards road map, including standards that deal with:

- ISMS monitoring and review guidelines
- ISMS internal auditing
- ISMS continual improvements

Other proposed guidelines are sector specific with a focus on healthcare, telecommunications, finance, and insurance. Under the premise that security is not a goal but a process, standards development and evolution will never stand still. As noted previously, the focus of this text is the ISO standards, and only information security standards from the ISO/IEC have been mapped for the near future. However, other national and international bodies have standards that can help to establish, implement, operate, monitor, and maintain an effective ISMS. These include but certainly are not limited to the National Institute of Standards and Technology (NIST) as well as many defense-related standards from the United States and across the globe.

1.7 Introduction to the ISO/IEC 27001 Standard

The ISO 27001 provides a common model for implementing and operating ISMS, and monitoring and improving ISMS operation. The intent of ISO is to harmonize ISO 27001 with other management system standards such as
ISO/IEC 9001:2000, which addresses quality management systems, and ISO/IEC 14001:2004, which addresses environmental management systems. The goal of ISO is to provide consistent and integrated implementation and operation of the ISMS with other management systems within the organization. The similarities among the standards imply similarities in the supporting tools and functions for implementation, managing, reviewing, auditing, and certification. This implies that if the organization has implemented other management standards or plans, too, there may be one audit and one management system where that management system applies to quality management, environmental management, security management, etc.

The 27001 standard provides guidance to implement an ISMS, as well as to obtain a third-party international certificate to prove that security controls exist and operate according to the requirements of the standard. The 27001 standard describes the ISMS as an overall management system from a business risk approach to establish, implement, operate, monitor, and maintain an ISMS. The ISMS should address all the aspects of the organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources. This text is a supplement to the ISO standards, not a replacement; therefore, the authors recommend obtaining the ISO standards relevant to the current organizational goals for a complete reference set.

With the ISMS in place, senior management now has the means to monitor and control security while reducing the residual business risk. After ISMS implementation, the organization may formally secure information and continue to fulfill the organization’s customer, legal, regulatory, and stakeholder requirements. If certification is a goal, analyze the specifications in ISO 27001 Sections 4 to 8, as these clauses are mandatory for certification. Annex A in ISO 27001 presents a list of control objects and controls that are the same controls as in ISO 27002, but not the same level of detail. Annex B of ISO 27001 contains a table where the Organization for Economic Cooperation and Development (OECD) principles and corresponding ISMS procedures and PDCA phases show how the information security international standards fulfill the requirement of OECD. If the organization has already implemented ISO 9001 or ISO 14001, Annex C contains a table to correspond to ISO 9001, ISO 14001, and ISO 27001.

Figure 1.3 shows the ISO PDCA model used to implement the ISMS; the PDCA model is sometimes referred to as an ISMS cycle. Use this model to develop, maintain, and continually improve the ISMS. The objective of implementing ISMS is to have an overall management system built in consideration of business risk to implement, operate, monitor, maintain, and improve information security. Sections 4 to 8 in the ISO 27001 standard are mandatory reading, as they describe how the organization should implement and construct its ISMS. In these sections, there are general requirements for the ISMS, including how to establish, manage, monitor, and maintain the ISMS.
1.8 Introduction to the ISO 27002 Standard

ISO 27002, *Code of Practice for Information Security*, is a commonly used international standard for information security throughout the world and provides insight to security controls to protect information and information technology. ISO 27002 does not address how to apply the controls. ISO 27001 provides direction on how to establish a management system that superimposes a discipline over how to select controls and how to establish good practices to apply the security controls. The procedures to actually implement the security controls are up to the organization and will vary according to the physical and technical environment.

What is information security and why is it important? Information security is the protection of an organizational asset (i.e., information) from unauthorized disclosure and unauthorized and unintended modification, and ensures the information is ready for use when needed. Legislation and other compliance requirements address privacy and accurate reporting of finances (e.g., Sarbanes–Oxley), and generally include the need for good security controls surrounding information. Traditionally, organizational asset space consisted mostly of tangible assets like equipment and buildings and negotiable assets like stocks, bonds, currency, or gold. The traditional valuation of an organization also included soft measures like goodwill, but relatively less valuation was given to knowledge, intellectual property, or information. The increase in organizational dependence on information, the value of information to the organization, and the value of the organization that finds root in information (e.g., intellectual property) result in the increased need to protect that information. Moreover, threats to the previous assets space were limited to physical proximity, that is, one needed access to the gold to steal it. Additionally, the thief needed the ability to transport the gold from vaults, through a building, past guards, and during escape, including the crossing of county, state, and national borders.

Information assets are mostly stored online as documents, database entries, or other forms of bits on media. Access to the organizational asset information is via a multitude of pathways, including inside the organization by using internal PCs and networks. If the organization connects to partners, the partners’ entire networks...
offer potential pathways. If the organization connects to the Internet, the entire world has potential access. Access to information in the middle of Missouri in the United States is as close as the nearest computer in Malaysia. Access and ease of transport are well beyond the limits of tangible assets.

Additionally, theft and use of intellectual property may be from a country that does not consider such actions to be illegal, and if so, that country may not have extradition agreements with the United States, the United Kingdom, Iceland, or other countries. Moreover, such theft may be state sponsored to increase that country’s ability to compete in the world market. The point is, there are a wide variety of motivations, means, and methodologies that support the threat space to the organizational asset of information. Thus, to remain viable, the organization must take information security seriously and implement an effective ISMS using a disciplined approach. To achieve an effective ISMS, the organization may choose to use the ISO standards as guidelines. ISO 27002 provides 12 chapters addressing security controls:

- Risk assessment and treatment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communication and operations management
- Access control
- Information system acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

These 12 chapters cover approximately 39 key elements and 133 controls. Table 1.2 illustrates the structure and a short description of individual controls in

<table>
<thead>
<tr>
<th>Control</th>
<th>Definition of security control with statement regarding necessary qualities to fulfill the control requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation guidance</td>
<td>Includes information for implementing the control and guidance to fulfill the requirements of the control</td>
</tr>
<tr>
<td>Other information</td>
<td>In some controls there is a clause “Other Information,” where there are references to information related to the specific control</td>
</tr>
</tbody>
</table>

© 2008 by Taylor & Francis Group, LLC
ISO 27002. Use these guidelines to write policies and procedures, and refer to the objective of the clause to derive the intent. Then use details in the specific control to generate the details of the policies and procedures to satisfy the intent.

1.9 Relationship between ISO 27001 and ISO 27002

ISO 27001 presents a management system. That management system is for information security. ISO 27002 presents guidelines for security controls. ISO 27002 is more the what (i.e., a list of useful controls) and ISO 27001 is more the how (i.e., a procedure on how to set up a management system that guides how to establish and maintain the security controls). ISO 27001 is not a set of procedures that addresses each ISO 27002 security control; rather, it presents a management process to establish security awareness, set up an organizational infrastructure, and plan, implement, and maintain the security controls. An organization may not receive certification against ISO 27002; rather, the organization receives certification against the management system for information security; that management system is the ISMS in ISO 27001.

Annex A of ISO 27001 references the same controls as ISO 27002 with exactly the same numbering of those controls; however, there is only a short description of these controls in ISO 27001. Both standards along with the guidance in this text provide the ability to achieve ISO 27001 certification.

1.10 Relationship to Other Management Standards

ISO provides many standards for management systems; ISO 9000 is for quality management, ISO 14000 is for environmental management, and ISO 27000 is for security management. ISO 27001 provides an introduction to the relationship of the ISMS with other management standards. ISO 27001 intends to harmonize with other management system standards to provide consistent and integrated implementation and operation of an enterprise management system. Information security standards use the model of PDCA for implementing, monitoring, and improving the ISMS. Other management standards also use the PDCA model. Common features between management standards include:

- All founded on management commitment
- Responsibility definition
- Document control
- Record management
- Training
- Management review
- Internal audit
- Corrective and preventive actions
- Common PDCA model used for implementing and operation
- Audit processes

Requirements based on similar standards

Certification body responsible for verifying auditor competence

If the opportunity presents, organizations that have more than one management standard to implement and manage may extend their ISMS to cover all management standards. The use of ISMS across many management standards and other essential compliance may be called a compliance management program (CMP). [See Chapter 6.] Benefits to one management system include leveraging investments in a single management system across the organization, a single point of focus for the auditors and certification, and ultimately less cost to the organization.

### 1.11 PDCA and Security Standards Cross-Reference

Any list of international, national, or other best practice standards in support of effective security management is destined to be incomplete. However, this section presents some of the more common standards in relation to the PDCA model (the numbers in brackets correspond to the references listed at the end of this book). Focus is on ISO, NIST, and British Standard Institute (BSI) standards.

#### 1.11.1 Standards to Assist in the Plan Phase


1.11.2 Standards to Assist in the Do Phase


SP 800-5, Security Metrics Guide for Information Technology Systems, available from www.nist.gov. Sounds more useful than it is (in my opinion), being little more than an enormous list of security things that could be measured.


1.11.3 Standards to Assist in the Check Phase


### 1.11.4 Standards to Assist in the Act Phase


