InformationShield

The New ISO 17799:2005 – Security Policy Implications For Business

By David J. Lineman

In July 2005 the International Standards Organization released a new version of the Information Security standard, ISO/IEC 17799. Since the original version was released in 2000, many businesses have based their information security programs on this standard. This paper explains the changes in the new 2005 standard and how they may impact an organization's information security policy program.

ISO 17799 – The First Wave

In 2000, the International Organization for Standardization (ISO) released its first information security standard, called ISO/IEC 17799:2000. It was based almost exclusively on the control objectives of the British standard, BS7799 Code of Practice for Information Security. The ISO standard, like BS 7799 divided the discipline of information security into ten key domains. Within each domain, there were a number of sub-topics, leading to a total of 123 detailed control objectives within 34 topic areas.

Because the ISO standard represented the most widespread information security framework available at the time, many organizations decided to base their information security programs on this framework.

The New Standard Emerges

Like all ISO standards, ISO 17799 is maintained by a work-group that consists of individuals from various ISO member organizations. The workgroup that manages the ISO 17799 standard is called the Joint Technical Committee, ISO/IEC JTC 1, *Information technology*, Subcommittee 27, *IT Security techniques*, Working Group 1, *Requirements, services and guidelines*. For the sake of brevity, we will call them "The Committee." One

of the confusing aspects of all ISO standards, and one of the challenges of interpreting the impact of new standards, is the detailed naming conventions used for both committees and documents.

Recognizing the rapid technical change and evolving threats within information security, The Committee convened to come up with an updated standard that better reflected the current state of the industry. The result, released in July 2005 was ISO/IEC 17799:2005, *Information technology – Security techniques – Code of practice for information security management*.

According to a press release from ISO, "Several changes to business environments and new ways of doing business were important in driving the development of the revised ISO/IEC 17799:2005. We recognized:

- the growing dependence on the use of external services and the management of service delivery;
- changes to the risks and threats facing businesses;
- new and emerging technologies and greater connectivity, and the impact this has on protecting information, and
- growing security requirements for regulatory compliance."

Summary of Changes to the new ISO 17799

For businesses that have based their security programs on ISO 17799:2000, two key questions must be answered:

1. What has changed in the standard?
2. What should we do in response to these changes?

This new standard contains 11 security control "clauses" collectively containing a total of 39 main security categories and one introductory clause introducing risk assessment and treatment. The 2000 standard had 10 high-level "domains" that have been preserved in the new standard, plus the addition of a new clause on incident management and response.

In general, there are five fundamental areas of change that are likely to impact businesses using the new standard:

1. Topic renaming and reshuffling
2. Additional emphasis on risk assessment
3. Additional emphasis on roles and responsibilities
4. More detailed guidance in control areas
5. Additional security control requirements

In the following sections we will discuss the impact of each of these areas.

1.0 The Name Game – Topic renaming and reshuffling

Much of the difference between ISO 17799:2000 and 17799:2005 is renaming and category reshuffling. Organizations that were used to referring to the ISO security domains and subtopics by number will have to get used to an entirely new numbering scheme. The new 2005 standard starts with the first security domain as *5.0 Information Security Policy*, with it's sub-domains as 5.1, 5.2 etc. The previous 2000 standard began with Information Security Policy as section 3.0. This creates a numbering difference that cascades into the various topics of the standard.

There also a number of naming changes. For example, what was *Section 5 – Asset Classification and Control* in the old standard is now *Section 7 – Asset Management*. Within the major control domains, many of the sub-topics are identical to the old standard. Some of the name changes are so minor is to be questionable. For example, section "12.2 Correct Processing of Applications" was renamed from "Security in Application Systems" with all the same topic subcategories.

Impact: While the working committee probably had good reason to rename many of these categories, this creates a barrier to deciphering the new standard and comparing it to what is in place.

For organizations who chose to name or number their policies based on the ISO naming conventions, a lot of rework will be required to correspond with the new naming and numbering. For most organizations, however, the time and resources required to update policies simply for name changing will not be practical. Instead, organizations should focus on the detailed control objectives within each domain and section, and compare them to their existing internal controls. As a good methodology we suggest creating a gap-analysis and comparison table as shown in Table 1.

Table 1: Sample Topic Mapping Matrix

17799:20005 Topic	1799:2000 Topic	Internal Control
8.1 Prior to Employment	6.01 Security In Job Definition And Resourcing	Employment Screening
6.1 Internal Organization	4.1 Security Infrastructure	Information Security Roles and Responsibilities
10.9 Electronic Commerce Services	8.07.03 Electronic Commerce Security	Security and Privacy of Online Transactions

For organizations that do wish to rename policies based on the new naming conventions, we suggest that this is done as part of the normal policy document review and approval cycle of the organization. However, we do

not recommend that the specific category numbers are used, since these are prone to change throughout the lifecycle of the standard.

2.0 Additional Emphasis on Risk Assessments

The 2005 standard includes a special "introductory" security control clause called Risk Assessment and Treatment. This section stresses the importance of choosing internal controls based on a formal risk assessment methodology. This section is referred to throughout the document, especially in the areas of detailed guidance.

Impact: Organizations that wish to eventually certify to the 2005 standard will have to establish a formal risk-assessment process that is documented. In short, there is no other way for an organization to logically pick and choose which of the various detailed controls in the 39 various topic areas should be implemented. In addition to the requirements of the ISO 17799:2005 standard, many international laws and regulations relating to data security and privacy require formal, documented risk assessments.

The 2005 standard does not into a lot of detail on risk assessment methodology, but instead refers to other documents, such as *ISO/IEC TR 13335-3 (Guidelines for the Management of IT Security: Techniques for the Management of IT Security)*. However, the requirements of having risk assessment as part of the entire control framework are referenced throughout the detailed guidelines of the standard.

3.0 Additional emphasis on definition of roles and responsibilities

While the proper definition of the "information security infrastructure" was part of the original 2000 standard, the 2005 version takes this to a new level. From an outline or structure perspective, the main requirements for properly defining information security roles and responsibilities falls into clause *6.0 Organization of Information Security*. While many of the detailed control requirements have moved unchanged into the 2005 standard, several additions were made including contact with authorities and special interest groups. Within the detailed guidance in each of the 39 topic areas, the proper definition of roles and responsibilities is mentioned for each topic.

Impact: It is clear that organizations who wish to adopt the ISO 17799:2005 standard must have proper definition of information security roles and responsibilities. While most organizations have documented information security policies (75% according to recent studies), very few have written definitions of information security roles and responsibilities. These including documented security requirements for various organizational roles.

For organizations who do not have a properly defined and documented information security infrastructure, *Information Security Roles and Responsibilities Made Easy* by Charles Cresson Wood can help. In addition to providing information security job requirements for over 40 different organization roles, this resource provides specific tools and techniques for generating management awareness of information security staffing needs.

4.0 More Detailed Specifications

In general, the level of detail provided for each control requirement has been greatly expanded. In the 2000 standard, high-level control statements were provided with a minimum of explanation. In the 2005 standard, each control topic has three main components:

Control: A specification of the overall requirement. Usually 2-3 sentences of high-level requirements. For example, *6.2.2 Addressing security when dealing with customers*, states:

"All identified security requirements should be addressed before giving customers access to the organization's information or assets."

Implementation guidance: A more detailed list of items that should be addressed within the high-level control objective. For the above example in protecting interactions with customers, specific elements of the customer interaction are listed, such as service level agreements, access control policies, contractual requirements, the right to monitor and many others.

Other Information: This section has references to other parts of the standard. In our example, this section discusses the risk of third-parties further outsourcing to other third-parties.

Impact: Overall, this extra detail greatly enhances the ISO/IEC 17799:2005 standard as a reference guide for implementing an information security program. As with any information security framework, the level of detail and coverage of the information security risk depends on the organization's internal risk assessment and overall business environment. Many of the detailed implementation topics are likely to show up in standards or procedures documents, rather than impacting the higher-level policy statements. However, organizations that are seeking certification will most-likely face a tougher job in demonstrating compliance with the standard.

5.0 Additional Security Control Requirements

While much of change to the 2005 standard was in naming and organization, several important addition control requirements were added. Organizations who are attempting to seek future certification should complete a detailed gap analysis between their current controls and what is specified in the new

2005 standard. Once gaps are identified, each of the various control requirements can be input into the risk assessment process to determine which should be implemented. Organizations who find gaps in their information security policy coverage can refer to Information Security Policies Made Easy, Version 10 by Charles Cresson Wood. ISPME contains over 1300 pre-written information security policies covering each of the detailed control requirements within the 39 ISO categories.

The following sections give a brief overview of the new control topics to be considered.

- **Security of Third Party Services**

  According to ISO, substantial changes were made to the standard to reflect the increase in third-party services and outsourcing. Most of the security requirements relating to third parties are included within the domain *Organization of Information Security* (formerly called Organizational Security), section 6.2 External Parties. These include:

  6.2.1 Identification of risks related to external parties
  6.2.2 Addressing security when dealing with customers
  6.2.3 Addressing security in third party agreements

  There are several changes within this category, including much renaming and reshuffling of categories. For example, *Section 6.1 Internal Organization* was renamed from "Information Security Infrastructure." However, most of the topics covered are the same as in the old standard.

  The old 2000 standard had a third major section called "Outsourcing." The category has been removed, and its topics covered within *6.2.3 Addressing Security in third party agreements*. Additional outsourcing topics are covered in *10.3 Third Party Service Delivery Management*.

- **Security of Personnel**

  The section entitled *Human Resources Security*, which used to be entitled *Personnel Security*, underwent the majority of changes from the 2000 to the 2005 standard. First, the entire set of sub-topics was reorganized to better represent the employment lifecycle. The following table summarizes the changes:

Old Categories	New Categories
6.01 Security In Job Definition And Resourcing	8.1 Prior to Employment
6.02 User Training	8.2 During Employment
6.03 Responding to Security Incidents and Malfunctions	8.3 Termination of Employment

The previous sub-topic, *6.01.03 Confidentiality Agreements*, was moved to 6.1.5. The new topic "8.2 During Employment" covers the important topic of user training and awareness, but also added *8.2.1 Management Responsibilities* and *8.2.3 Disciplinary Process*.

- **Incident Response and Management**

A fundamental change to the standard is the addition of a new top-level clause (or domain), *13 Information Security Incident Management*. In the 2000 standard, incident response was covered in the *Personnel Security* domain under section *6.03 Responding to Security Incidents and Malfunctions*. It has been completely removed and its topics included under the new domain 13.

Despite the addition of this new section, many of the sub-topics have remained the same. For example, *Reporting Information Security Events and Weaknesses and Learning from Information Security Incidents* have been maintained in the new standard.

Organizations who want to manage to the new 2005 standard will have to have well-defined policies and procedures for incident response. New requirements were added for the management of information security incidents and for collection of evidence. One of the more fundamental changes is the explicit definition of persons responsible for the management of incidents. This is in keeping with the overall updates to the 2005 standard. Control topics that should be covered include:

1. Personnel reporting of incidents
2. Definition and training on proper reporting channels
3. Roles and Responsibilities for incident management
4. Handling of incidents, including forensics
5. Incident reporting management systems
6. Reporting to law enforcement
7. Collection of evidence

Collection of evidence is an important new addition to the 2005 standard. Recent court cases have ended up being at least partially decided on an organization's internal controls around electronic evidence collection and maintenance. It seems clear that the courts require organizations to have the proper controls in place. Organizations that do not have these controls should consider this one of the highest priorities in updating their information security programs.

- **Protecting Against Threats and Vulnerabilities**

Another addition to the new 2005 standard is an increase focus on the management of vulnerabilities. This shows up in the 2005 standard as an additional section *12.6 Technical vulnerability Management*, under the domain of *Information Systems Acquisition, Development and Maintenance*.

Many organizations now have some form of vulnerability management in place. At the most basic level, this includes keeping up with the latest patches. However, they may not have these formalized as written policies, standards and procedures, and they may not have documented specific job responsibilities for vulnerability management. For example, policies should cover such topics as:

- Sources of vulnerability data
- Patch Management
- Vulnerability Assessment and Reporting
- Technical baseline management

The new standard has increased emphasis on roles and responsibilities for managing vulnerabilities. According to the standard, the "organization should define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required;"

- **Communications and Operations Management**

The domain of *Communications and Operations Management* was changed in several ways. First, a new section *10.2 Third Party Service Delivery and Management* was added. (This relates closely with the topics covered in the Organizational Security domain.)

To reflect the increase in global electronic commerce, a new section *10.9 Electronic Commerce Security* was added. Topics include:

10.9.1 Electronic commerce
10.9.2 On-Line Transactions
10.9.3 Publicly available information

Controls in these categories involve the authorization of individuals performing transactions, end-to-end protection of transactions via encryption and digital certificates, and maintaining privacy in e-commerce activities. The topic of *Publicly Available Information* addresses the need for data to be properly classified and approved before being made available on public internet sites.

Another change to this domain is in the area of *10.10 Monitoring*. Three new topics have been added including:

10.10.3 Protection of log information
10.10.4 Administrator and operator logs
10.10.5 Fault logging

Due to the large number of changes, this category should be an early focus of any gap analysis between current systems and the new standard.

- **Topic: Physical Security**

Most of the changes within physical security involved renaming and reshuffling of categories. For example, the 2000 standard category called "general controls" was split up and divided into the two other main categories of the physical security domain, *9.2 Secure Areas* and *9.2 Equipment Security*.

One new topic area was added to this domain, *9.1.4 Protecting against external and environmental threats*. An obvious addition after the physical disasters that have occurred in the last few years, this control covers requirements for dealing with physical destruction of properly from fire, floods, earthquakes and other disasters. This analysis usually comes as part of the organizations risk-assessment, with controls, policies and procedures outlined in the disaster recovery plan. Very few companies who were sophisticated enough to adopt the 2000 standard would not have some of this analysis as part of their information security management system.

To Certify of Not to Certify

The British standard, BS 7799 has a second part – Code of Practice for Information Security Management System (ISMS). This standard provides a framework for organizations to get certified on their adoption of the controls of the British standard. When ISO 17799:2000 was released, it did not have a certification component. Organizations wishing to certify their information security management system (ISMS) either used the British standard (which covered identical topics) or simply didn't certify.

ISO has announced that a new certification standard will be published in late 2005, allowing organizations to finally become certified to the new ISO/IEC 17799:2005 requirements. This document, to be called *ISO/IEC 27001 Information security management systems — Requirements,* will define the requirements for certification. A list of certifying authorities is being maintained at the ISMS International User Group Web site (www.xisec.com).

Obtaining the standard

Organizations can purchase the new ISO/IEC 17799:2005 standard through authorized resellers. Digital copies can be purchased and downloaded through the British Standards Institute at www.bsi-global.com.

Summary

For most organizations that have already adopted the ISO/IEC 17799:2000 standard, the updated ISO 17799:2005 will impact them in several major areas. While there were many changes in naming and organization, the 2005 standard did introduce several new technical areas, including electronic commerce and vulnerability management. Organizations should do a gap-analysis between their current policies and these new controls within the areas that have been updated. The newer, detailed implementation guidance of the 2005 standard should help this process. For organizations that find policy gaps in their coverage of the standard, *Information Security Policies Made Easy, Version 10*, contains a complete set of over 1300 pre-written information security policies that cover all topic areas of the new 2005 standard.

References

[1] ISO/IEC 17799:2000 – Code of practice for information security management - Published by ISO and the British Standards Institute [http://www.iso.org/]

[2] ISO/IEC 17799:2005, Information technology – Security techniques – Code of practice for information security management. Published by ISO [http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html]

[3] ISO/IEC TR 13335-3 (Guidelines for the Management of IT Security: Techniques for the Management of IT Security) – Published by ISO. [http://www.iso.org/]

[4] Information Security Policies Made Easy, by Charles Cresson Wood. Published by Information Shield, Inc. 2005. [http://www.informationshield.com]

[5] Information Security Roles and Responsibilities Made Easy, by Charles Cresson Wood. Published by Information Shield, Inc. 2002-2005. [http://www.informationshield.com]

[6] ISO/IEC 27001 Information security management systems — Requirements, Due for release in late 2005.

About Information Shield - Information Shield is a global provider of security policy solutions that enable organizations to effectively comply with international regulations. Information Shield products are used by over 7000 customers in 59 countries worldwide. Find out more at our Regulatory Resource Center at www.informationshield.com or contact the author at dave@informationshield.com

informationshield.com
2660 Bering Drive Houston, TX 77057 TEL 1.888.641.0500 FAX 713.783.5365