Using Information Shield publications for ISO/IEC 27001 certification

In this paper we discuss the role of information security policies within an information security management program, and how Information Shield publications can assist organizations seeking certification against the newly-released ISO/IEC 27001.

Background and purpose of ISO 27001

Before the international information security standard known as ISO 17799, there was the preceding British Standard BS7799, published by the British Standards Institute (BSI). The original BS 7799 had two parts. BS 7799 Part1 - *Code of practice for information security management* - established the overall requirements for an information security program by breaking security into ten separate topic domains.

BS 7799-1 was eventually adopted as the first international standard for information security, ISO 17799:2000 [1]. BS 7799 Part 2, entitled *Information security management systems — Specification with guidance for use*, was designed to allow an organization to become certified that it was following the techniques defined in Part 1 of the standard. Within Great Britain and around Europe hundreds of organizations became certified against BS7799. Up until last year, if an organization wished to become "certified" it could only be done against the British Standard BS7799.

In 2005, the International Organization for Standardization (ISO) took two important steps relating to information security. First, it updated ISO 17799:2000 and called it ISO 17799:2005 (See the related Information Shield whitepaper, "What's new with the ISO 17799:2005 – Policy Implications for Business.") Second, it adopted the part 2 of BS 7799 and released it as *ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements* [2]. For the first time, organizations can get certified against the ISO 17799:2005 standard.

By definition, ISO 17799:2005 and ISO 27001 are designed to be used by any organization in any industry. However, many smaller organizations may have trouble meeting some of the requirements of ISMS due to limited manpower and resources.

Overview of ISO 27001

Basically, ISO 27001 sets out the requirements for how an organization can implement the security requirements of ISO 17799:2005. According to ISO 27001:

> *"This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS)."*

According to the Standard, an ISMS is defined as:

> *"The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources."*

In other words, the ISMS encompasses your entire information security program, including its relation to other parts of the organization. While ISO 27001 does not provide a complete prescription for a proper information security program, it does list the various organizational functions required for certification, including a list of required documents that must be produced.

ISO 27001 uses a process-based approach, copying the model first defined by the Organization for Economic Cooperation and Development (OECD). The Plan-Do-Check-Act (PDCA) Approach [6] breaks overall organizational processes into four phases, as shown in Figure 1.

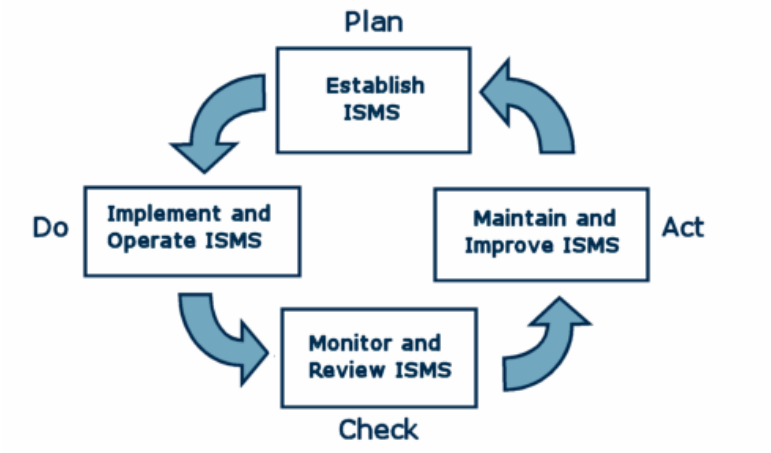

Figure 1: Overview of the PDCA approach used in ISO 27001.

The Role of Information Security Policies in ISO 27001

Written information security policies are the foundation for any Information Security Management System, and are specifically required in ISO 27001. Not only are written policies listed in the definition of an ISMS, they are referred to throughout the ISO 27001 standard. For example, part of the required documentation is an overall policy defining the information security management system:

> *4.3.1 The ISMS documentation shall include:*
> *a) documented statements of the ISMS policy (see 4.2.1b)) and objectives;*

The purpose of ISO 27001 is to certify that an organization is compliant with ISO 17799:2005. The first information security domain listed in the ISO 17799:2005 standard is called "5.0 Information Security Policy." In fact, a written set of information security policies is often considered the best evidence of management's support for the information security function. According to ISO 27001:

> *5.1 Management shall provide evidence of its commitment to the […] ISMS by:*
> *a) establishing an ISMS policy;*

The Benefits of Information Shield Publications

For organizations seeking certification with the new ISO 27001 standard, the pre-written information security policies and expert advice within Information Security Policies Made Easy (ISPME) and Information Security Roles and Responsibilities Made Easy (ISRR) provide the following benefits:

Policy coverage for all ISO 17799:2005 security domains

Information Security Policies Made Easy has pre-written policies for every domain and category of the ISO 17799:2005 standard, including such topics as access controls, network security, data integrity, organizational security, personnel security, encryption, physical security, disaster recovery, incident response and many others. In fact, ISPME is organized around the ISO 17799 outline to make it easier to locate and reference policies, and to help fill in any policy gaps discovered by your organization. (See the *Information Shield Solution Matrix for ISO 1799:2005*. [5])

Documentation requirements of ISO 27001

ISO 27001 is very clear about the documentation requirements of any information security program. In addition to the over 1300 policies within the policy library, ISPME comes with fifteen separate, pre-written information security policy documents. Organizations seeking certification can save considerable time and effort by using the pre-written documents that have been used in thousands of organizations around the world.

In addition to policies, organizations must also document the roles and responsibilities of individuals who will perform the various functions. For example,

> *6.0 Internal ISMS Audits: The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall be defined in a documented procedure.*

Information Security Roles and Responsibilities Made Easy (ISRR) provides documented information security job requirements for over 40 organizational roles. In addition, ISRR provides security-related mission statements for various organizational units, and nine different information security reporting relationships and organizational diagrams. In short, ISRR is the most effective way for organizations to clearly document the security responsibilities of the entire organization as required by ISO 27001.

Supporting a risk-based approach to security

ISO 27001 clearly specifies that organizations much adopt a risk-based approach to security. This means that organization must adopt a documented risk assessment approach, which includes a process for risk acceptance. ISPME provides over 20 pre-written policies that support the performance of risk assessments within the organization. In addition, each of the 1300+ policies found within the ISO policy library contain expert commentary from Charles Cresson Wood, CISSP, CISM, CISA who has over 20 years of information security experience. The commentary for each policy discusses the organizational risks that are mitigated by each corresponding policy statement.

> *4.2.2 The organization shall do the following.*
> *a) Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks (see 5).*

Management Support of Information Security

Section 5 of ISO 27001 details the requirements for demonstrated management support of the information security function.

> *"Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS […]"*

ISPME provides information security policies that define the responsibilities of executive and senior management within the security function. For example, policies that require the establishment of executive level information security review boards and periodic management review of the information security program. In addition, ISPME provides policies that define the requirements of other critical organization roles such as data custodian, data owner, internal audit and many others.

Information Security Roles and Responsibilities Made Easy (ISRR) provides over 80 pre-written documents that support an organization's commitment to information security.

ISRR provides the “glue” that links the security requirements defined in the policies to the organizations roles responsible for performing these functions.

Training and awareness of Information Security

Section 5.2.2 specifies the requirements for education and training of personnel responsible for information security.

The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

> *[Management is responsible for] communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;*

ISPME provides policies that specify the performance and ongoing management of information security awareness and training. ISPME also contains a number of training and awareness methods that have proven useful in organizations worldwide. ISRR provides pre-written job descriptions for organization roles that must be involved in the training and awareness functions.

Monitoring and Review

A critical component of certification with ISO 27001 is the continual monitoring and review of the information security management system.

> *7.1 Management shall review the organization’s ISMS at planned intervals (at least once a year) to ensure its continuing suitability, adequacy and effectiveness.*

Within the context of an ISMS, auditing occurs at both management and technical levels. For example, information systems must be monitored for possible information security events and to preserve transaction and account integrity. Information systems must be monitored for configuration against organizational levels. At the macro level, the entire information security program should be monitored against the stated objectives of the program, and this data should be used to feed back into updates of the entire program.

> *The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall be defined in a documented procedure.*

ISPME has specific policies for the logging and auditing of information technology and security functions, as well as high-level policies defining the business requirements for internal and external audit of the information security program.

Continuous Improvement

In short, ISO 27001 specifies a process of continual information security improvement through monitoring, review and action.

> *The organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review (see 7).*

ISPME helps organization stay up to date on the latest information security technologies and threats. Now in its tenth version, ISPME has been continuously updated since its first release over 15 years ago.

ISRR provides a number of resources to help information security departments secure the support and resources they need. ISRR is the only publication that allows an organization to quickly document the information security requirements of various organizational roles and departments, turning policies and procedures into real action items that are targeted at specific individuals within the organization.

Summary

Organizations seeking certification against ISO 27001 can save considerable time and effort using pre-written information security policies from Information Shield. ISPME Version 10 provides complete policy coverage for the eleven information security domains of ISO 17799:2005. ISPME facilitates a risk-based approach to information security programs by not only defining policies for risk assessments, but by including risk statements and discussion for each of the over 1300 controls within the library. Along with its companion publication, Information Security Roles and Responsibilities Made Easy, ISPME allows an organization to quickly demonstrate management's support for information security in clear and concise policy documents and written functional job requirements.

References

[1] ISO/IEC 17799:2005 – Code of practice for information security management - ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission). Available at ANSI [http://www.ansi.org/]

[2] ISO/IEC 27001:2005 - Information technology — Security techniques — Information security management systems — Requirements. Published by ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission). [http://www.ansi.org/]

[3] Information Security Policies Made Easy, by Charles Cresson Wood, CISSP, CISM. Published by Information Shield, Inc., 2002-2005. [http://www.informationshield.com]

[4] Information Security Roles and Responsibilities Made Easy, *Version 2* by Charles Cresson Wood, CISSP, CISM, CISA. Published by Information Shield, Inc., 2002-2005. [http://www.informationshield.com]

[5] Information Shield Policy Solution Matrix for ISO/EIC 1799:2005. Published by Information Shield, Inc., 2005. [http://www.informationshield.com/iso17799.html]

[6] OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. [www.oecd.org]

informationshield.com

2660 Bering Drive Houston, TX 77057 TEL 1.888.641.0500 FAX 713.783.5365