The Evolution of BS7799 to ISO27001 and ISMS Certifications

White Paper
June 2006

by Rebecca Herold, CISSP, CISM, CISA, FLMI

Contents

The need to protect information has been following a crescendo of awareness over the past few years to climax with literally thousands of information security and privacy-related news reports during 2005. Consumers have been become aware of the need for protection through cases of identity theft and fraud. Security incidents impact businesses in both the short-term and the long-term from the costs required to not only clean up incidents and implement better security controls to prevent similar incidents from recurring but also from diminished trust and lost business.

✎ According to an autumn 2005 independent survey of nearly 10,000 adults in the United States conducted by the Ponemon Institute:

20% indicated they terminated a relationship with a company after being notified of a security breach

40% say they are considering terminating the relationship

5% hired lawyers upon learning that their personal information may have been compromised

---

Growing numbers of laws and regulations are being passed and implemented throughout the world. Such legislation has justifiably captured the attention of business leaders who are now more seriously considering how to meet compliance regulations and perform information security due diligence than ever before. Establishing an effective information assurance program to incorporate information security into business activities is now high on the executives' to-do list.

Information Security Management Systems Integrate Security into Business

A well-documented information security program will not be effective if it is not successfully integrated throughout the enterprise within all business practices. Information security practitioners are increasingly realizing that establishing a formal Information Security Management System (ISMS) will complement their existing information security efforts and work to effectively integrate information security throughout the enterprise business services, products, operations, and management. As a result, information security will truly become more effective and will more clearly support business success.

BS7799-2 specifically outlines and details the implementation and documentation requirements for an ISMS. In effect, an ISMS is the approach by which a BS7799-based information security program validates and documents its existence, documenting how information security processes must be implemented within a specified organizational scope. When an organization pursues certification, the ISMS is what is audited and ultimately certified.

BS7799-2 and the supporting ISO/IEC 17799 documents have evolved over the years. There was a major rewrite to ISO/IEC 17799 in 2005. ISO27001 is the new industry standard for an ISMS. It was formalized in October 2005 and replaces the previous BS7799 standard.

What Is New About ISO/IEC 17799?

Over the years, many organizations have built their information security programs around the controls and domains listed in ISO/IEC 17799. A large number of organizations have written and organized their information security policies and procedures using the ISO/IEC 17799 as a model framework and to represent a leading international practice.

The revised version of ISO/IEC 17799 was published on June 15th, 2005, at which time the officially published 2000 version was withdrawn. The 2005 version contains 17 new controls, and a few of the old ones were merged, incorporated with others, or deleted. The 2005 version contains a total of 134 controls.

The 2005 version has 11 domains, or *clauses*; the 2000 version has 10 domains. The domains align pretty closely, however there were a few slight title changes as indicated in Figure 1. A few notable and definite improvements in the 2005 version include the addition of content addressing issues related to:

- Third-party and outsourcing security

- Managing systems updates

- Security following personnel termination

- Responding to incidents

- Ensuring appropriate mobile and remote computing device security

ISO/IEC 17799:2000	ISO/IEC 17799:2005
Security Policy	Security Policy
Security Organization	Organizing Information Security
Asset Classification & Control	Asset Management
Personnel Security	Human Resources Security
Physical & Environmental Security	Physical & Environmental Security
Communications & Operations Management	Communications & Operations Management
Access Control	Access Control
Systems Development & Maintenance	Information Systems Acquisition, Development and Maintenance
	Information Security Incident Management
Business Continuity Management	Business Continuity Management
Compliance	Compliance

Figure 1: Mapping chapters from the 2000 version to the 2005 version.

✎ ISO/IEC 17799:2005 is a code of practice for information security management and is not applicable for ISMS certification. BS7799 Part 2:2002 and ISO/IEC 27001 are currently used for ISMS certification.

Certification Process

There are generally three phases in the ISMS certification process.

- First phase—The organization prepares for ISMS certification by developing and implementing the ISMS, integrating the ISMS into the enterprise business processes, training all personnel and creating ongoing ISMS awareness activities, and creating an ISMS maintenance process.

- Second phase—This step involves engaging an accredited certification body to audit the ISMS. Successful certification will last for 3 years, after which the ISMS must be recertified to maintain certification.

- Third phase—The certification body goes onto the ISMS site regularly, for example every 6 to 9 months, to perform surveillance audits.

Benefits of Obtaining ISMS Certification

There are many business benefits for establishing an ISMS and pursuing certification. To consider just a few, an ISMS

- Can reduce liability risk and demonstrates due diligence as well as lower business insurance premiums

- Demonstrates credibility for, and trust in, how the organization protects information; this demonstration leads to increased satisfaction and confidence of stakeholders, business partners, and customers

- Demonstrates executive management support for internationally accepted security and privacy standards, principles, and practices

- Ensures that security and privacy controls and practices are built-in to all levels of an organization (at least within the ISMS scope) and that all personnel are educated on security and privacy as they relate to the business

- Establishes a holistic, quality management–based security and privacy program that also subsequently creates verifiable evidence of due care activities

- Helps to bring organizations into compliance with a wide range of legal, regulatory, and statutory requirements, such as the United States Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), 21 CFR Part 11, and the Sarbanes-Oxley Act (SOX), as well as California's SB1386, the European Union Data Protection Directive, Canada's PIPEDA, and Australia's Federal Privacy Act

- Improves business continuity and availability by identifying threats and appropriately minimizing internal and external risks

- Is increasingly recognized worldwide as a security and privacy differentiator for regulatory oversight as well as competition

- Provides a documented, consistent, and repeatable process for enterprise information security and privacy governance

- Provides an organization with market differentiation that creates a more positive company image that relays the importance of information security and privacy and could very well positively affect the revenues and asset or share value of the organization

- Reduces operational risk by mitigating vulnerabilities and lessening risks through clearly defined and consistent activities

- When implemented properly and successfully, an ISMS will significantly limit security and privacy breaches that can cost millions (through such things as lost or compromised information, fines and penalties, downtime, internal and external threats, consumer driven litigation, and so on)

Benefits of Requiring Business Partners to Have Certified ISMS Programs

Many data breach and security incidents have actually been the result of mistakes and poor practices by third-party outsourced vendors who were performing activities for other companies. However, it was the primary company that ultimately made the headlines, and whose business was most impacted. For example, consider only incidents involving third-party backup tape handlers in just the United States:

- DHL Delivery Service lost an ABN Amro backup tape containing data on 2 million of their customers in November 2005; the tape was subsequently found December 19

- UPS lost Citigroup computer backup tapes containing information about 3.9 million individuals in June 2005

- Iron Mountain lost Time-Warner's computer backup tapes containing information about 600,000 current and former employees in May 2005

- Iron Mountain lost Bank of America computer backup tapes containing information about 1.2 million federal employees in February 2005

- Iron Mountain lost Ameritrade computer backup tapes containing information about 200,000 customers in April 2005

These are just a few of the hundreds of incidents that have occurred and been reported over the recent years involving organizations to whom businesses outsourced information handling, storing, transportation, or processing. Many organizations are outsourcing very specialized data processing and management activities in an effort to save money or because they just don't have the resources, experience, or capabilities to do it themselves. Organizations also commonly outsource to get specific expertise that their personnel may not possess, and which they cannot afford to hire or purchase. For example, if you outsource your applications programming activities, you will reasonably expect that the individuals doing this work know about application security issues and will incorporate adequate security controls into the product they create for you. You will also reasonably expect them to know how to protect information in a shared customer environment; making sure that the programming code they create for your organization does not get sent by accident to another customer, that the test data they use for your organization does not get used by another of their customers, and so on.

Outsourcing is becoming quite commonplace, particularly with many top financial, healthcare, tax reporting, and credit reporting companies. Even agencies within the United States government have outsourced processing of sensitive information. Chances are there are people within your organization considering outsourcing some of your data processing activities.

When entrusting third parties with your company's confidential data, you are placing all control of security measures for your organization's data completely into the hands of someone else. That trust cannot be blind. Many of the recent security incidents have resulted from loose security practices within outsourced third-party organizations that were custodians of another company's customer or employee personal information.

When you outsource critical data processing and management activities, how can you stay in charge of the security of the outsourced data and minimize your business risks? How do you know the third party is complying with your regulatory responsibilities? How can you demonstrate to regulators that you are in compliance with data protection requirements and promises when someone else possesses your data?

You need to hold such outsourced organizations to strict security standards. In many instances, the standards will be more stringent than your own organization's security requirements. Accordingly, requiring business partners to conform to ISO27001 or have a certified ISMS helps to protect your organization from business partner security and privacy incompetence.

Challenges for Obtaining ISMS Certification

Although there are many significant benefits to implementing a certifiable ISMS, do not think that doing so will be a simple task that can be accomplished in a matter of a couple of months let alone weeks. There are many associated challenges. Consider them now so that you can plan accordingly when creating your own implementation plans. A few of these challenges include:

- Obtaining executive management commitment. Successful implementation of an ISMS is dependent upon visible and active executive management support. ISMS enforcement authority must come from executive management.

- Setting the ISMS scope. Organizations must understand that an ISMS typically governs multiple manageable security domains. Organizations often try to create a scope that is much larger than can feasibly be managed, or they do not create realistic security domains.

- Risk analysis. The basis for the ISMS controls must be risk. Organizations must identify risks to be able to prioritize and implement appropriate safeguards within the ISMS. Many organizations do not perform a risk analysis or do not truly understand the risks within their environment.

- Implementation flaws. An ISMS should leverage other existing business frameworks, such as ITIL and COSO. Without doing so, duplication of effort and implementation conflicts occur.

- Asset identification and classification. Organizations must know the information assets they are protecting and why they need to be protected. Unfortunately, most organizations lack or have a poor or inaccurate asset inventory and information classification system. These deficiencies lead to inconsistent and flawed implementation.

- Resources. Implementing an ISMS requires participation from everyone within the organization, including support from multiple business leaders and understanding from all personnel within the organization who must follow the policies and procedures.

- Personnel awareness and training. Organizations must communicate the ISMS information security policies, processes, standards, and responsibilities to personnel, otherwise they cannot expect them to know, understand, or follow the directives. Unfortunately, most organizations have grievously insufficient or ineffective awareness and training programs.

- No magic bullets. There does not exist one magic bullet product or system to implement an effective and certifiable ISMS. Beware of vendors who claim their products will do so. The specific environment and culture of each organization must be taken into account individually to create an effective ISMS.

- Ongoing evaluation and modification. Once an ISMS is launched, processes must be in place to continuously evaluate the effectiveness and feasibility of all components of the ISMS. When weaknesses, inefficiencies, or security gaps are discovered, the ISMS needs to be modified accordingly.

ISMS Certification Facts

According to the International Register of ISMS Accredited Certificates (http://www.iso27001certificates.com/) there were 2017 actual ISMS certified organizations as of the end of December 2005. The ten countries with the most certifications at the end of 2005 were:

1. Japan: 1187
2. UK: 219
3. India: 139
4. Taiwan: 66
5. Germany: 49
6. Italy: 40
7. Korea (note, "South" or "North" was not indicated): 35
8. USA: 31
9. Hungary: 23
10. Netherlands: 22

Certified ISMS Auditors

The International Register of Certified Auditors (IRCA—http://www.irca.org/) manages the certification for ISMS auditors. There are six types of auditor certifications:

- ISMS Auditors
- ISMS Internal Auditor
- ISMS Lead Auditor
- ISMS Principal Auditor
- ISMS Provisional Auditor
- ISMS Provisonal Internal Auditor

IRCA evaluates certification applicants against requirements that reflect the key skills, knowledge, and experience that define competence and which the ISMS auditor needs to demonstrate during audits. The evaluation criteria include education, work experience, auditor training, and auditing experience for each of the types of auditor certifications. The details of all certified auditors are included within a register, which is published and made publicly available by IRCA.

It is interesting to note the number of IRCA ISMS-certified auditors within each of the countries that have a preponderance of ISMS certified businesses. According to IRCA, there were the following combined numbers of certified ISMS auditors as of January 2006 in each of the indicated countries:

- Japan: 12
- UK: 16
- India: 1
- Taiwan: 6
- Germany: 1
- Italy: 14
- South Korea: 3
- USA: 6
- Hungary: 1
- Netherlands: 0
- Canada: 4

It is important to keep in mind that although the number of certified ISMS auditors appears to be small, each of the at least 51 worldwide ISMS registrars (certification bodies) may have their own certifications available to allow consultants and auditors to participate within the ISMS certification process. For example, BSI Global (http://www.bsi-global.com) provides training programs for individuals who are on their way to becoming IRCA certified, which allows the individuals to participate within ISMS audits. There are likely hundreds more individuals worldwide who have some sort of registrar-specific certification or qualifications.

ISMS Certification Trends

It is apparent from the previous statistics that United States' businesses have been slow to seek ISMS certified programs. Why? Ray Kaplan, a United States-based BSI Qualified BS7799 Auditor, Implementer, and Instructor points out an error many organizations make is considering that BS7799:2002 and ISO/IEC 27001 can be used as a checklist approach for grading their existing information security programs. "To use ISMS standards as mere checklists completely misses the main thrust of this important fabric: an ISMS is a process management system. The developing fabric of the ISO 27000 family of ISMS standards carries on the developing traditions of many process management systems. Some previous BS7799 certifications were conducted poorly, giving rise to the mistaken idea that ISMS certification was a sham. Some BS7799 certifications were issued on the flimsiest of grounds. However, as the fabric of national authorities square up to enforce rigor in formal certification to the developing ISO 27000 family of standards, rigor is becoming the rule. For instance, registrars are now requiring real, internationally recognized ISMS audit credentials for their auditors."

I anticipate that the growing number of security incidents coupled with the growing number of worldwide laws and regulations for protecting information will result in an increase in the number of organizations who establish formal ISMSs and subsequently seek ISMS certification; particularly as organizations begin to understand ISMS scope and certification processes.

Resources

The following list highlights a few good resources for you to check when considering ISMS implementation and certification:

- http://27000.macassistant.com/
- http://dmoz.org/Science/Reference/Standards/Individual_Standards/ISO_17799
- http://hotskills-inc.com/services_iso_17799.shtml
- http://www.17799.com/index.php
- http://www.irca.org
- http://www.iso27001certificates.com
- http://www.iso27001security.com
- http://www.standardsmark.com/Products/InfomationSecurity.htm
- http://www.xisec.co

About the Author

Rebecca Herold has more than 16 years of experience in information security, privacy and compliance. Rebecca is an independent consultant, author and instructor and assists organizations of all sizes with their information privacy, security and regulatory compliance programs.

Rebecca has a B.S. in Math and Computer Science and an M.A. in Computer Science and Education. Rebecca is a Certified Information Systems Security Professional (CISSP), a Certified Information Systems Auditor (CISA), a Certified Information Systems Manager (CISM), and a Fellow of the Life Management Institute (FLMI). Rebecca has been a member of the Information Systems Audit and Control Association (ISACA) since 1990 and has held all board positions throughout her membership in the Iowa chapter. She was Vice President, Privacy Services and Chief Privacy Officer at DelCreo, Inc., Chief Privacy Officer and Senior Security Architect for QinetiQ Trusted Information Management, Inc., and Senior Systems Security Consultant at Principal Financial Group. Rebecca was instrumental in building the information security and privacy program while at Principal Financial Group which was awarded the CSI Outstanding Security Program of the Year Award in 1997. Rebecca is also an adjunct professor for the Norwich University Master of Science in Information Assurance (MSIA) program.

Rebecca authored The Privacy Papers (Auerbach) in 2001, The Practical Guide to HIPAA Privacy and Security Compliance (Auerbach) in 2003, The Business Executive Practical Guides to Compliance and Security Risks book series (Realtime Publishers) in 2004, Managing an Information Security and Privacy Awareness and Training Program (Auerbach) in 2005, The Definitive Guide to Security Inside the Perimeter (Realtime Publishers) in 2005 and The Privacy Management Toolkit (Information Shield) in 2006. Rebecca lives in the country near Des Moines, Iowa. She is the community leader at http://www.realtime-itcompliance.com, and she can be reached at rebeccaherold@rebeccaherold.com.

About NetIQ Corporation

NetIQ is a leading provider of integrated systems and security management solutions that empower IT organizations with the knowledge and ability necessary to assure IT service. NetIQ's Knowledge-Based Service Assurance products and solutions include embedded knowledge and tools to implement industry best practices and to better ensure operational integrity, manage service levels and risk and ensure policy compliance. NetIQ's modular, best-of-breed solutions for Performance & Availability Management, Security Management, Configuration & Vulnerability Management, and Operational Change Control integrate through an open, service-oriented architecture allowing for common reporting, analytics and dashboards. We empower IT organizations with the knowledge of their IT service levels through automated assessment, understanding and real-time management of current configurations, known vulnerabilities and risk. With NetIQ you know your IT service is assured.

Headquartered in San Jose, Calif., with offices and development facilities in 16 countries worldwide, NetIQ employs 900 people and has more than 3,000 enterprise customers. For more information, please visit the company's web site at www.netiq.com or call (888) 323-6768.