Information Security Management Best Practice Based on ISO/IEC 17799

The international information security standard provides a framework for ensuring business continuity, maintaining legal compliance, and achieving a competitive edge

René Saint-Germain

Security matters have become an integral part of daily life, and organizations need to ensure that they are adequately secured. While legislatures enact corporate governance laws, more and more businesses are seeking assurance that their vendors and partners are properly protecting information assets from security risks and are taking necessary measures to ensure business continuity. Security management certification provides just such a guarantee, thereby increasing client and partner confidence.

A number of best practice frameworks exist to help organizations assess their security risks, implement appropriate security controls, and comply with governance requirements as well as privacy and information security regulations. Of the various best practice frameworks available, the most comprehensive approach is based on the implementation of the international information security management standard, ISO/IEC 17799, and subsequent certification against the British standard for information security, BS 7799. This ISO 17799/BS 7799 frame work is the only one that allows organizations to undergo a third-party audit.

Organizations today must deal with a multitude of information security risks. Terrorist attacks, fires, floods, earthquakes, and other disasters can destroy information processing facilities and critical documents. Theft of trade secrets and the loss of information due to unexpected computer shutdowns can cause businesses to lose their commercial advantage. *The CGI/FBI Computer Crime and Security Survey* states that total losses in the United States in 2004 as a result of computer security breaches reached $141,496,560. Organizations often tackle security issues as part of their efforts to comply with a variety of regulatory requirements, such as the Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA). It is becoming increasingly clear, however, that to address all aspects of security, organizations need to implement a more comprehensive approach using a methodical compliance framework.

At the Core

This article

- Introduces various best practices for implementing security controls
- Lists the 10 security domains of ISO/IEC 17799
- Describes the benefits of implementing ISO/IEC 17799
- Talks about security trends

Compliance is not always straightforward. As META Group notes in its white paper, "Unraveling Security and Risk Regulation," legislation governing regulatory requirements often lacks the specificity organizations need to know how to comply. According to META Group, companies and institutions affected by such legislation must decide for themselves which security controls are appropriate for their organizations.

An increasing number of businesses, moreover, are seeking to obtain security certification from third-party organizations, given that certification guarantees that the controls implemented meet information security requirements. Certification enables organizations to comply with increasing demands from financial institutions and insurance companies for security audits. In addition, it builds trust in an organization's capacity to implement appropriate security controls to manage and protect confidential client and business information.

Some best practices that facilitate the implementation of security controls

include Control Objectives for Information and Related Technology (COBIT), ISO/IEC 17799/BS 7799, Information Technology Infrastructure Library (ITIL), and Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE). Focus on the ISO/IEC 17799 standard is warranted, given that it provides the most comprehensive approach to information security management. The other best practices focus more on IT governance, in general, or on the technical aspects of information security. (See Table 3.)Moreover, ISO 17799/BS 7799 is the only best practice framework that allows organizations to undergo a third-party audit and become certified. Implement-ing an overarching compliance framework using ISO/IEC 17799 and BS 7799 requires a methodical information security management system that facilitates the planning, implementation, and documentation of security controls and ensures a constant process review.

ISO/IEC 17799: An Information Security Management Standard

ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management defines information security as the preservation of information confidentiality, integrity, and availability. The goals of information security are to ensure business continuity, to maintain legal compliance, and to achieve competitive edge. For example, organizations with a committed client base and an established partner network need to demonstrate to their partners, shareholders, and clients that they have identified and measured their security risks and implemented a security policy and controls that will mitigate these risks. Such controls might include, for example, the use of digital certificates for electronic transactions, the drafting and testing of business continuity plans, the use of secure backup media and the implementation of appropriate access controls.

In drafting a security policy and implementing appropriate security controls, organizations comply with legal requirements and demonstrate their commitment to securing information assets and to protecting the confidentiality of personally identifiable customer information. They also provide their business partners and clients with greater confidence in their capacity to prevent and rapidly recover from any interruptions to production or service levels.

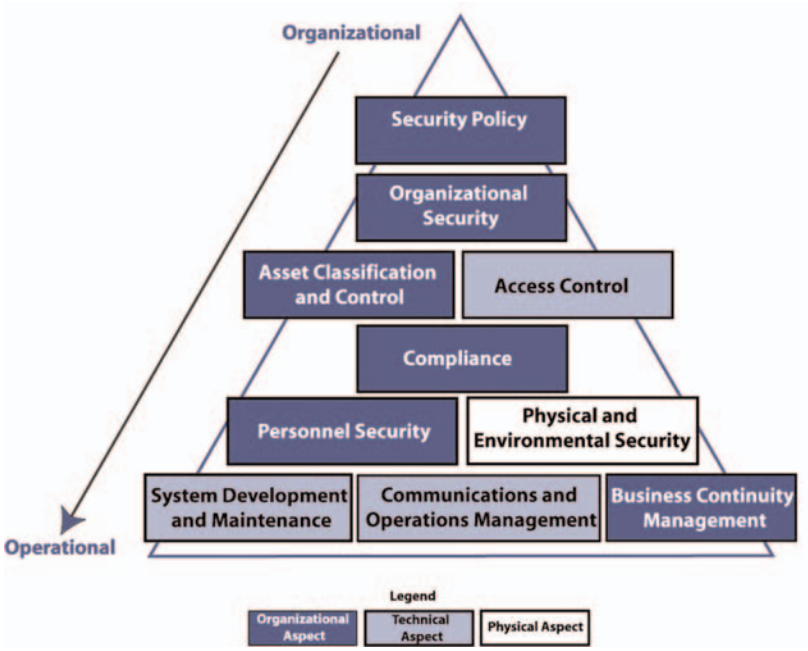


Figure 1: The Ten Domains of ISO/IEC 17799

Proper security ultimately results in minimizing business damage. Implementing ISO/IEC 17799 involves putting in place a cost-effective execution plan that includes appropriate security controls for mitigating identified risks and protecting the confidentiality, integrity, and availability of an organization's information assets. It also involves ongoing monitoring to ensure that these controls remain effective. In sum, ISO/IEC 17799 enables organizations to manage information security as a coherent and global business process that extends beyond the very narrow approach to security that focuses uniquely on technical aspects or computer infrastructure.

ISO/IEC 17799 comprises 10 security domains and seeks to address security compliance at all levels: managerial, organizational, legal, operational, and technical. It includes 36 control objectives, consisting of general statements of security goals for each of the 10 domains. The standard also includes 127 controls that identify specific means for meeting the control objectives. Organizations implement these controls to mitigate the risks they have identified. The ISO 17799/BS 7799 security domains are:

1. **Security Policy** – Demonstrate management commitment to, and support for, information security.
2. **Organizational Security** – Develop a management framework for the coordination and management of information security in the organization; allocate information security responsibility.
3. **Asset Classification and Control** – Maintain an appropriate level of protection for all critical or sensitive assets.
4. **Personnel Security** – Reduce the risk of error, theft, fraud, or misuse of computer resources by promoting user training and awareness regarding risks and threats to information.
5. **Physical and Environmental Security**

– Prevent unauthorized access to information processing facilities and prevent damage to information and to the organization's premises.

6. **Communications and Operations Management** – Reduce the risk of failure and its consequences by ensuring the proper and secure use of information processing facilities and by developing incident response procedures.
7. **Access Control** – Control access to information to ensure the protection of networked systems and the detection of unauthorized activities.
8. **Systems Development and Maintenance** – Prevent the loss, modification, or misuse of information in operating systems and application software.
9. **Business Continuity Management** – Develop the organization's capacity to react rapidly to the interruption of critical activities resulting from failures, incidents, natural disasters, or catastrophes.
10. **Compliance** – Ensure that all laws and regulations are respected and that existing policies comply with the security policy in order to ensure that the objectives laid out by senior management are met.

Figure 1 suggests a structure for the standard's 10 domains. This structure is driven from the top down, such that the impact is felt from the management or organizational level all the way to the operational level.

Implementation Considerations

ISO/IEC 17799 is highly flexible and can be used by a variety of organizations. Organizations should determine what their primary security objectives are and adapt their use of the standard to these objectives as they strive for information security governance. Table 1 provides an overview of ISO/IEC 17799 uses.

Organizations also must consider how to efficiently manage ISO/IEC 17799 standard implementation, given that this standard, although flexible, is quite complex and touches on a number of different security areas. The important documentation and accountability requirements of BS 7799 certification only add to this challenge. One solution is to use a governing tool that will guide the deployment team, enable collaboration across the organization, and automate the documentation process. A number of such solutions are currently available on the market and offer varying levels of functionality.

Certification Process

Organizations that base information security management systems (ISMS) on BS 7799 specifications can apply to become certified. An organization that obtains certification is said to be ISO/IEC 17799 compliant and BS 7799 certified.

Development, implementation, maintenance, and continual improvement of a documented ISMS are fundamental to certification. To guide organizations through this process, BS 7799 uses the Plan-Do-Check-Act (PDCA) model that is common to other management systems. Table 2 provides an overview of PDCA cycle phases as they relate to an ISMS.

Once an organization has developed, implemented, and documented its ISMS, an accredited certification body carries out a third-party audit. The BS 7799 audit includes both a documentation audit and an implementation audit. Security auditors assess whether an organization's ISMS scope covers all aspects of operations. They also ensure that the risk assessment reflects the organization's business activities and that the assessment's results are reflected in the risk treatment plan. Finally, the implementation audit verifies that the organization has effectively implemented its security policies and controls and that processes have been set in place to ensure the ISMS's review and improvement.

A number of critical factors can affect success or failure in the certification process. Key success factors include adopting an implementation approach that is consistent with the organization's culture,

Type of Company	Size	Primary Objective	Use of the Standard
Small Enterprise or Organization	Fewer than 200 employees	Raise the awareness of the management regarding information security	ISO 17799 contains the security topics that should be dealt with as a foundation for information security management.
Medium Enterprise (centralized or decentralized)	Fewer than 2,000 employees	Create a corporate culture of compliance	The standard contains the practices required to put together an information security policy.
Large Enterprise	More than 2,000 employees	Obtain security certification at the end of the process	Use BS 7799-2 to implement, maintain review, and improve an information security management system (ISMS)

Table 1: Uses of the ISO/IEC 17799 Standard

PDCA Phase	Description
Plan (establish the ISMS)	• Define the ISMS scope and the organization's security policies • Identify and assess risks • Select control objectives and controls that will help manage these risks • Prepare the Statement of Applicability (SoA) documenting the controls selected and justifying any decisions not to implement, or to only partially implement, certain controls
Do (implement and operate the ISMS)	• Formulate and implement a risk mitigation plan • Implement the previously selected controls to meet the control objectives
Check (monitor and review the ISMS)	• Conduct periodic reviews to verify the effectiveness of the ISMS • Review the levels of acceptable and residual risk • Periodically conduct internal ISMS audits
Act (maintain and improve the ISMS)	• Implement identified ISMS improvements • Take appropriate corrective and preventative action • Maintain communication with all stakeholders • Validate improvements

Table 2: Information Security Management Systems and the PDCA Model

ensuring that the security policy reflects business objectives, and providing proper training for employees. Another key success factor is the use of a governing system that ensures the timely update of security policies as well as organization-wide collaboration and knowledge-sharing. However, the single most important success factor in obtaining BS 7799 certification is management commitment to, and support of, an ongoing, organization-wide information security management process. Indeed, without management commitment, certification cannot succeed. Other obstacles to obtaining certification include insufficient knowledge of the approach adopted and poor understanding of security requirements, risk assessment, and risk management processes.

Once certification is achieved, organizations can expect to undergo periodic monitoring audits and must reapply for certification every three years. It is important that organizations use a governing system to automate the BS 7799 compliance and certification process, given the documentation and accountability requirements.

Benefits of Implementing the ISO/IEC 17799/BS 7799 Framework

ISO/IEC 17799 compliance and BS 7799 certification provide important advantages on many levels. BS 7799 certification serves as a public statement of an organization's ability to manage information security. It demonstrates to partners and clients that the organization has implemented adequate information security and business continuity controls. It also demonstrates the organization's commitment to ensuring that its information security management system and security policies continue to evolve and adapt to changing risk exposures. Certification is a mark of distinction that sets organizations apart from their competition and provides partners, shareholders, and clients with greater confidence.

Furthermore, given the reduced level of risk to which ISO/IEC 17799 compliant organizations are exposed, these organizations will spend less money recovering from security incidents, which may also translate into lower insurance premiums. Finally, an indication of the importance of ISO/IEC 17799 compliance is the fact that international invitations to tender are beginning to require that organizations be ISO/IEC 17799 compliant.

Security Compliance Trends

The approach to compliance is evolving from one focused on technical elements to an understanding of compliance as a coherent business process (not a project) that intimately involves all aspects of an organization. This new perspective, where compliance is managed and measured as a business process, is leading some larger organizations to appoint a chief security officer or a chief risk officer to ensure that security compliance is dealt with on a organization-wide and ongoing basis.

Al Passori of META Group, in his article "CIO Primer for Three Standard Deviations," predicts that by 2009/10, 35 percent of the Global 2000, i.e., the 2,000 largest companies worldwide, will have adopted at least one international security framework.

The increasing interest in security frameworks is due to new governance legislation, to a growing awareness of the importance of information security, and to security audit demands by financial institutions and insurance companies.

Initially implemented primarily in Europe and Asia, ISO/IEC 17799 has been adopted as a national standard in many countries, including Australia, Brazil, the Czech Republic, Finland, Iceland, Ireland, Japan, the Netherlands, New Zealand, Norway, Spain, and Sweden.

Continually striving toward fuller maturity, ISO/IEC 17799 is already one of the most widely referenced information security frameworks. As the editor of *Information Security Magazine*, Lawrence Walsh, notes, "Even as the ISO undertakes

Best Practices and Compliance Frameworks	Description/Scope	Offers Certification?	Comparison with ISO/IEC 17799
CERT Security Practices	A set of recommended best practices for improving the security of computer network systems	No	ISO/IEC 17799 addresses a more comprehensive set of information security issues.
Common Criteria for Information Technology Security Evaluation (ISO 15408)	A technical standard that certifies the levels of defense conferred by the security measures implemented in information systems	Yes	ISO/IEC 17799 focuses on the organizational and administrative aspects of security whereas ISO 15408 focuses on the technical aspects of information systems. Therefore, they are complementary.
Control Objectives for Information and (Related) Technology (COBIT)	COBIT is an international standard for IT governance that seeks to bring together business control models and IT control models.	No	COBIT and ISO/IEC 17799 are mutually complementary, with COBIT providing a broader coverage of IT governance in general and ISO/IEC 17799 focusing more specifically on security and providing certification.
Guidelines for the Management of IT Security (GMITS) (ISO 13335)	GMIS is an international standard that lays out guidelines for information security management and consists of a number of technical reports covering information security management concepts and models, techniques, IT security management and planning, and selection of safeguards.	No	The two standards are complementary. While GMITS describes high level concepts for IT security management, ISO/IEC 17799 specifies controls that can be used to develop and implement an information security management system (ISMS).
Information Technology Infrastructure Library (ITIL)	A supplement to Committee of Sponsoring Organizations of the Treadway Commission (COSO) and COBIT that proposes best practices for IT service management	No	ITIL and ISO/IEC 17799 are complementary and can be used together. ITIL can be used to improve general IT processes and controls and ISO/IEC 17799 can be used to improve security controls and processes.
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)	An assessment and planning framework for security that enables companies to identify and analyze risks and develop a plan to mitigate those risks. The OCTAVE approach can be implemented using two assessment methods: one for large companies (OCTAVE Method) and one for small businesses (OCTAVE-S).	No	OCTAVE is an evaluation activity, not a continuous process. BS 7799, on the other hand, implements a continuous process for risk management and compliance based on the PDCA model. As such, an OCTAVE method could be created and incorporated into the planning segment of the PDCA cycle used in BS 7799.
System Security Engineering Capability Maturity Model (SSE-CMM)	A model for assessing the security maturity level of an organization. Five security levels exist, from 1 (performed informally) to 5 (continuously improving). SSE-CMM does not describe a way of doing things but rather reports widespread practice.	No	BS 7799 provides a process for the continuous improvement of information security. As such, SSE-CMM and BS 7799 complement each other and BS 7799-certified organizations may seek to be recognized as SSE-CMM Level 5 organizations.

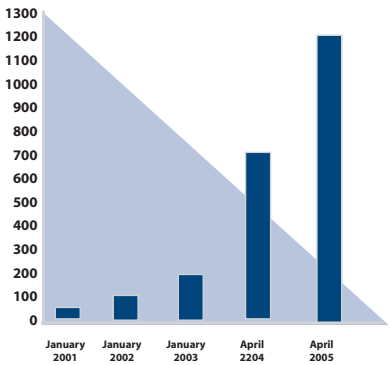
Table 3: Quick Comparison of Security Best Practices

a major review of the standard, ISO 17799 – and its British Standards Institution (BSI) cousin -– are rapidly becoming the canon for information security management." Michael Rasmussen, of the Giga Information Group, adds that "ISO 17799 has become the de facto standard for defining (at a high level) an information security program/architecture."

A revised version of BS 7799 was expected to be published at the end of June 2005. Originally, the name of this revised standard was going to be ISO 24743. However, during the early part of 2005 it was determined that it would be called BS ISO/IEC 17799 (BS 7799-1). The revised standard was designed to be more user-friendly and incorporates changes in technology, technical upgrades, and compatibility issues. The standard also provides additional controls as well as enhancing and revising existing controls. With the release of this new version, an increase in the adoption of this standard worldwide, especially in North America, can be expected. (See Figure 2.)

In the current context of increased information security, privacy, and governance regulations, organizations are required to assess their risks, adopt appropriate controls, and document their efforts to demonstrate compliance. Lack of security compliance can result in business loss, as well as severe civil and criminal penalties, including fines and prison sentences. Moreover, a growing demand also exists for security certification to increase confidence in the security of information held by companies and institutions.

A comprehensive, flexible framework for implementing cost-effective compliance, deployed via a governing system that maintains security policies and controls, is essential for organizations falling into several regulatory realms. The ISO/IEC 17799/BS 7799 best practice framework provides a set of best practices and controls that address the essential issues of information confidentiality, availability, and integrity existing at the heart of regulatory efforts. This comprehensive approach to information security management enables organizations to build client and partner trust in their capacity to secure their information assets and ensure business continuity.



Source: International ISMS/BS 7799 Certification Newsletters July 2003, April 2004, August 2004 (Acknowledgements to Xisec) Certificate Registrar: *www.xisec.com*

Figure 2: Trends in the Global Uptake of BS 7799

René Saint-Germain *is the president of Callio Technologies (*www.callio.com*), the software provider of a process framework for deploying and maintaining security compliance certification. He is an expert in risk assessment and contingency planning, with broad experience with Fortune 500 companies and government agencies at all levels. Mr. Saint-Germain is a frequent speaker at security-related conferences. Contact him at* rstg@callio.com.

References

Alberts, Christopher et. al., "Introduction to the OCTAVE Approach." CERT Coordination Center. Available at *www.cert.org/octave/approach_intro.pdf* (Accessed 3 June 2005).

BSI. "Information and Communication Technology: Frequently Asked Questions." Available at www.bsi-global.com/ICT/Security/faqs.xalter (Accessed 3 June 2005).

BSI. Information security management systems—specification with guidance for use. 2002.

Computer Security Institute. "2004 CSI/FBI Computer Crime and Security Survey." Available at *www.gocsi.com* (Accessed 3 June 2005).

Information Systems Audit and Control Association (ISACA). "COBIT Mapping: Mapping ISO/IEC 17799: 2000 With COBIT." Available at *www.isaca.org/Template.cfm?Section=Research2&Template=/ContentManagement/ContentDisplay.cfm&ContentID=15056#cobitiso* (Accessed 3 June 2005).

ISO/IEC. ISO/IEC 17799: Information Technology–Code of Practice for Information Security Management. 2000.

META Group. "Unraveling Security and Risk Regulation," white paper. January 2005.

National Institute of Standards and Technology (NIST). "International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management – Frequently Asked Questions." November 2002. Available at *csrc.nist.gov/publications/secpubs/otherpubs/revisofaq.pdf* (Accessed 3 June 2005).

Passori, Al. META Group. "CIO Primer for Three Standard Deviations," 6 January 2005. Available at *www.metagroup.com/us/resCenter/displayResourceCenter.do?areaPrefix=ITLVM* (Accessed 3 June 2005).

Rasmussen, Michael. Giga Information Group, Inc. "IT Trends 2003: Information Security Standards, Regulations and Legislation." 5 December 2002. Available at *images.telos.com/files/external/Giga_IT_Trends_2003.pdf* (Accessed 3 June 2005).