ISO 17799:
Standard for Security

Organizations can use ISO 17799 as a model for creating information security policies and procedures, assigning roles and responsibilities, documenting operational procedures, preparing for incident and business continuity management, and complying with legal requirements and audit controls.

Ellie Myler, CRM, and George Broadbent

Pretexting. Zero Day Attacks. SQL Injections. Bots and Botnets. Insider Infractions. Click Fraud. Database Hacking. Identity Theft. Lost Laptops and Handhelds. According to Ted Humphreys, in a recent International Organization for Standardization (ISO) press release, "It is estimated that intentional attacks on information systems are costing businesses worldwide around $15 billion each year and the cost is rising."

Today's information professionals need to address an ever-increasing number of internal and external threats to their systems' stability and security, while maintaining access to critical information systems. As the e-commerce space continues to grow and new tools allow organizations to conduct more business online, they must have controls in place to curtail cyber crimes' malicious mayhem, tampering, and wrongdoing.

Organizations need to address information security from legal, operational, and compliance perspectives. The risk of improper use and inadequate documentation abounds, and the penalties are greater than ever. By combining best practices outlined in the international standard *ISO/IEC 17799 Information Technology – Security Techniques – Code of Practice for Information Security Management (ISO 17799)* with electronic records management processes and principles, organizations can address their legal and compliance objectives. This article explores the opportunity to bridge the

At the Core

This article

- ▶ Describes the components of ISO 17799 and provides a step-by-step method for using it as the framework for an information security program

- ▶ Tells how organizations can use ISO 17799 in conjunction with their electronic records management processes and principles to address legal and compliance objectives

- ▶ Discusses data loss reporting issues

gaps and bring together information security, intellectual property rights, protection and classification of organizational records, and audit controls.

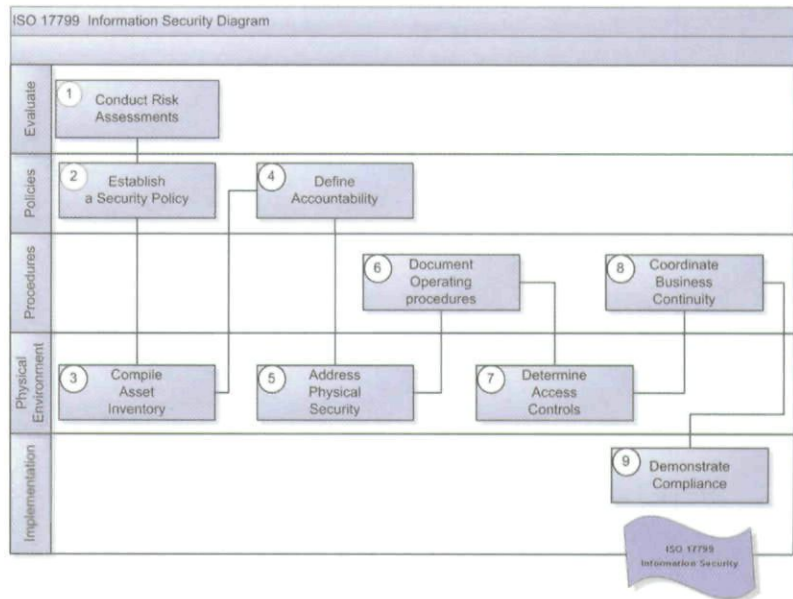## ISO 17799 Components, Applications, Implications

ISO 17799 provides a framework to establish risk assessment methods; policies, controls, and countermeasures; and program documentation. The standard is an excellent model for organizations that need to:

- Create information security policies and procedures

- Assign roles and responsibilities

- Provide consistent asset management

- Establish human and physical security mechanisms

- Document communications and operational procedures

- Determine access control and associated systems

- Prepare for incident and business continuity management

- Comply with legal requirements and audit controls

Information security can be defined as a program that allows an organization to protect a continuously interconnected environment from emerging weaknesses, vulnerabilities, attacks, threats, and incidents. The program must address tangibles and intangibles. Information assets are captured in multiple and diverse formats, and policies, processes, and procedures must be created accordingly.

Organizations can use this standard not only to set up an information security program but also to establish distinct guidelines for certification, compliance, and audit purposes. The standard provides various terms and definitions that can be adopted as well as the rationale, the importance, and the reasons for establishing programs to protect an organization's information

assets and resources. Figure 1 depicts the suggested steps and tasks associated with establishing and implementing an information security program.

This ISO framework is methodically organized into 11 security control clauses. Each clause contains 39 main security categories, each with a control objective and one or more controls to achieve that objective. The control descriptions have the definitions, implementation guidance, and other information to enable an organization to set up its program objectives according to the standard methodology.

Step 1: Conduct Risk Assessments

This component of the standard applies to activities that should be completed before security policies and procedures are formulated.

Risk is defined as anything that causes exposure to possible loss or injury. *Risk analysis* is defined as a process of identifying the risks to an organization and often involves an evaluation of the probabilities of a particular event or an assessment of potential hazards. Loss potentials should be understood to determine an organization's vulnerability to such loss potentials.

Risk categories are both internal

and external and can include:

- Natural: Significant weather events such as hurricanes, flooding, and blizzards

- Human: Fire, chemical spills, vandalism, power outages, and virus/hackers

- Political: Terrorist attacks, bomb threats, strikes, and riots

Conduct risk assessments to understand, analyze, evaluate, and determine what risks organizations feel are likely to occur in their environment. Risk assessment activities involve information technology (IT) and information processing facilities, facilities management and building security, human resources (HR), records management (RM) and vital records protection, and compliance and risk management groups. These groups must collectively determine what the risks are, the level of acceptance or non-acceptance of that risk, and the controls selected to counteract or minimize these risks.

Risk analysis is conducted to isolate specific and typical events that would likely affect an organization; considering its geography and the nature of its business activities will help to identify risks. Loss potential from any of these

events can result in prohibited access, disrupted power supplies, fires from gas or electricity interruptions, water damage, mildew or mold to paper collections, smoke damage, chemical damage, and total loss (with the destruction of the entire building).

Regularly monitor emerging threats and evaluate their impacts, as this is a constant, moving target. For example, according to an *IMlogic* article, "IM [instant messaging] worms are the most prevalent form of IM malware, representing 90 percent of all unique attacks in 2005. These attacks frequently utilized social engineering techniques to lure end users into clicking on suspicious links embedded inside IM messages, enabling the activation of malicious code that compromised the security of host operating systems or applications."

Although threats are increasingly sophisticated in the virtual sphere, the simple occurrence of employees stealing company information on paper is still very real and prevalent in today's work space.

Step 2: Establish a Security Policy

These components of the standard provide the content that should be included as well as implementation guidance to set the foundation and authorization of the program.

To set its precedence, an information security policy should be developed, authorized by management, published, and communicated. It should apply to all information assets and must demonstrate management's commitment to the program. Explain implications on work processes and associated responsibilities and outline them in employee job descriptions.

The security policy should be administered, documented, and periodically evaluated and updated to reflect organizational goals and lines of business. This is captured under clause 6.0 for organizing information security. It reflects administrative and management activities to implement the security pol-

Employees are part of the overall information security landscape and often they are the closest and best able to prevent certain incidents from occurring.

icy. All activities must identify authorities, responsibilities, agreements, and external security requirements. This has an impact on information processing facilities, external parties, access issues, and problem resolution measures. Keep a record of all policy administration activities to create historical relevance for the information security program.

Step 3: Compile an Asset Inventory

This component of the standard addresses asset management, controls, and the protection thereof. It applies to all assets in tangible and intangible form.

Identify the organization's intellectual property (IP), tools to create and manage IP, and physical assets with a

detailed inventory so the organization knows what type of resources it has, where they are located, and who has responsibility for them. Identifying how assets are to be used, classified, labeled, and handled is necessary to establish an asset management inventory.

This inventory should also distinguish the types, formats, and ownership control issues. Implement associated rules for the use of assets including e-mail, Internet usage, and mobile devices. Classifying assets and establishing procedures for labeling and handling according to the classification scheme are also important. Documents in electronic form will lend themselves to being identified through metadata and document properties completion. However, these processes must all be completed by resources. Although automation of these processes is a possibility, an organization still faces extensive costs and resource coordination to address this piece.

Step 4: Define Accountability

This component of the standard addresses the human aspect of security; it applies to the level of accountability that employees, contractors, and third-party users have to use to protect an organization's information assets.

An information security program will not be implemented unless roles and responsibilities are clearly articulated and understood by those having ownership in the program. Ideally, these roles and responsibilities should be outlined in job descriptions and documented in terms and conditions of employment.

Employees are part of the overall information security landscape and often they are the closest and best able to prevent certain incidents from occurring. HR is typically in charge of these issues, but they must collaborate with IT and RM to ensure that all information assets are addressed accordingly.

Define roles and responsibilities during pre-employment and screening processes, and perform background

checks to support the hiring process. If the job mandates working with highly sensitive information, an organization must be on guard to hire the most qualified person to perform these tasks. These employees must possess a great deal of integrity, pay attention to detail, and take their responsibilities seriously.

Information security awareness, education, and training must be a routine activity to keep employees informed, to communicate expectations, and to provide updates on their responsibilities. Standardize a disciplinary process for security breaches.

When employees leave or change jobs, it is essential that HR, in collaboration with other stakeholders, follows through with a return of assets process and removal of access rights, which can be captured in HR exit processes and procedures. This often is not a coordinated process, which allows employees to walk off with information or leave behind on servers and in physical work spaces masses of orphaned and unidentified information. Redesign the HR exit interview to ensure that information return or transfer is a coordinated process.

Step 5: Address Physical Security

This component of the standard outlines all the requirements for physical security perimeters and authorized entry controls; measures for protecting against external and environmental threats; equipment security, utilities, and cabling considerations; and secure disposal or removal of storage equipment media.

An organization's building and premises, equipment, and information-processing facilities must be fail proof to prevent unauthorized intrusions and access, and possible theft issues. This applies mostly to facilities management and IT, although risk management should also participate to provide environmental risk protection measures.

Include guidelines for physical security perimeters, entry controls, environmental threats, and access pat-

> An organization's building and premises, equipment, and information-processing facilities must be fail proof to prevent unauthorized intrusions and access, and possible theft issues.

terns in this section. Also address supporting utilities, power, and telecommunication networks. Finally, secure the disposal and removal of equipment that holds information so that information is truly deleted or "wiped" clean from the slate.

Step 6: Document Operating Procedures

Procedures for system activities, change management controls, and segregation of duties are included in this component.

Any organizational program will be more established when program administration, policies, procedures, and related processes are formally documented.

This component sets out to define operating procedures, instructions for the detailed execution thereof, and the management of audit trail and system log information. It applies to all facets of an information security program.

Formally documenting program activities will allow an organization to keep track of the development, implementation, and associated documentation for the program. Keep in mind that documentation does not magically appear through word processing programs. It takes resources, good writing skills, and an ability to change documentation when necessary.

Address the separation of development, test, and operational facilities to reduce the risk of unauthorized actions. Monitor and review third-party service delivery requirements to ensure that actions are carried out as mandated. Plan for, monitor, and update system resources, capacity management, and acceptance criteria, as necessary.

Constantly monitor and prepare to protect against malicious and mobile code to guard the integrity of system software and information. This especially pertains to intelligent cyber-crime activities such as structured query language injections and application to mobile devices, which are increasingly becoming more sophisticated. This should also focus on incoming e-mails and downloadable attachments, as well as a review of webpages.

Backup and restoration procedures must provide for the replication of information and methods for dispersal and testing, meeting business continuity requirements. This should also address retention periods for archival information or those with long-term retention requirements. Address media preservation issues to ensure the longevity of media that have long-term retention requirements.

Address network infrastructure through network controls and management. This includes:

- Remote equipment and connections

- Public and wireless networks

- Authentication and encryption controls

- Firewalls and intrusion detection systems

- Media handling and transit methods

- Information classification, retention, and distribution policies and procedures

Although mobile devices have helped organizations stay better connected, employees must use more discretion when using them. Alert employees to proper etiquette for relaying information so they will not be overheard in elevators, airports, or on other public transportation.

Address electronic data interchange, e-commerce, online transactions, electronic signatures, electronic publishing systems, and electronic communication methods such as e-mail and IM. Their secure use and associated procedures must demonstrate accuracy, integrity, and reliability. For organizations using e-commerce, this is not an option, as current regulations are pushing this into the forefront of IT agendas. Organizations should also monitor their systems and record security events through audit logs. Also address records retention policies for archival or evidence requirements.

Step 7: Determine Access Controls

This component of the standard includes guidelines for establishing policies and rules for information and system access.

Practice standard methods for all users and system administrators to control access to and distribution of information. Policies should apply to users, equipment, and network services. Newer technologies, such as those that have passwords connected to fingerprint digital touch pads, come at a cost, but they should be evaluated as a password management tool.

Figure 2: California SB 1386 Excerpts, Source and Language Summary

Source	Language
California 2002 Legislative Service, Chapter 915, S.B. 1386, Confidential or Privileged Information – Computers – Data	Any person or business that owns or licenses computerized data that includes personal information, to disclose in specified ways, any breach of the security of data.
California 2002 Legislative Service, Chapter 1054, A.B. No. 700, Telecommunications – Personal Identification Information – Disclosure, CA Civil Code 1798.82(g)	"Notice" may be provided by one of the following methods: (1) Written Notice (2) Electronic Notice Substitute notice consisting of e-mail notice, conspicuous posting on website page, and notification to major statewide media.
California 2002 Legislative Service, Chapter 1054, A.B. No. 700, Telecommunications – Personal Identification Information – Disclosure, CA Civil Code 1798.84(a)	Any customer injured by a violation of this title may institute a civil action to recover damages.
California 2002 Legislative Service, Chapter 1054, A.B. No. 700, Telecommunications – Personal Identification Information – Disclosure, CA Civil Code 1798.84(b)	Any business that violates, proposes to violate, or have violated this title may be enjoined.

Access control measures should include:

- Setting up user registration and deregistration procedures

- Allocating privileges and passwords

- Implementing a "clear desk and clear screen policy"

- Managing:
  - Unattended equipment
  - Virtual private network solutions
  - Wireless networks and authentications
  - Network service issues such as routing and connections
  - Telecommuting virtual spaces and intellectual property rights
  - Cryptographic keys and procedures
  - Software development, testing, and production environments
  - Program source code and libraries
  - Change control procedures and documentation
  - Patches, updates, and service packs

Any information system that an organization procures or develops must also include security requirements for valid data input, internal processing controls, and encryption protection methods. Document the integrity, authenticity, and completeness of transactions through checks and balances. Retain and archive system documentation for configurations, implementations, audits, and older versions. This is further detailed in clause 12 of the standard.

Step 8: Coordinate Business Continuity

This component of the standard includes reporting requirements, response and escalation procedures, and business continuity management.

As organizations increasingly come under attack and suffer security breaches, they must have some formalized manner of responding to these events.

Business continuity management addresses unexpected interruptions in business activities or counters those events that impede an organization's critical business functions. This process should include:

- Identifying risks and possible occurrences
- Conducting business impact analyses
- Prioritizing critical business functions
- Developing countermeasures to mitigate and minimize the impact of occurrences
- Compiling business continuity plans and setting up regular testing methods for plan evaluation and update

A business continuity management framework also includes emergency or crisis management tasks, resumption plans, recovery and restoration procedures, and training programs. Testing the plan is an absolute must to determine its validity. Tests can include a variety of methods to simulate and rehearse real-life situations. Develop calling trees, hot- and cold-site configurations, and third-party contractors, depending on the organization's priority of critical business functions.

Report information security incidents or breaches as soon as possible to ensure that all relevant information can be remembered. This requires having feedback processes in place as well as establishing a list of contacts that are available around the clock to manage this process. Procedures should be consistent and effective to ensure orderly

Figure 3: ISO Clauses

Clause	Description
10.5	Backup and document restoration procedures
10.8.1	Retention and disposal guidelines for information exchange policies and procedures
10.10.3	Audit log information evidence requirements
11.3.3	User responsibilities for a "Clear Desk and Clear Screen Policy"
12.3.1	Transborder flow and encryption information issues
12.4.1	Maintenance of system documentation and change control procedures
15.1.2	Maintenance of IP registers, licenses, copyrights, trademarks, and documentation
15.1.3	Records safeguarding and handling guidelines, classification, and retention schedules and inventories of key information

responses to not only manage the immediate process but also to collect evidence for legal proceedings.

Step 9: Demonstrate Compliance

This component of the standard provides standards for intellectual property rights, RM requirements, and compliance measures. These apply to everything from an organization's information processing systems to the granular data and transactional records contained within those systems.

There is an increased scrutiny on organizations to demonstrate compliance with applicable laws, regulations, and legislative requirements for all aspects of their business transactions. Adherence to rules and regulations are an integral part of the information security program and will contribute to demonstrating corporate accountability.

Address identification, categorization, retention, and stability of media for long-term retention requirements according to business and regulatory requirements. Document retention periods and associated storage media as

part of managing the organization's records. Address privacy and personal data requirements, which can vary from one country to the next. Address transborder data flow and movement, and associated encryption methods as related to import and export issues depending on federal laws and regulations.

Follow up on and evaluate compliance with established policies and procedures to determine implementation effectiveness and possible shortcomings. Clearly delineate audit controls and tools to determine areas for improvement. Again, it is critical to take time to document all information related to the development and establishment of compliance and audit, including decisions made, resources involved, and other source documentation cited.

Data Breach Reporting Issues

New information security requirements are emerging as a result of organizations' negligence to protect sensitive data and impose adequate controls on employees using mobile technology to house such data. Information security

issues are constantly in the media, as with the recent case when the U.S. Department of Veterans Affairs (VA) lost control of the personal information of 28 million veterans when a laptop containing the information was stolen from an employee's home. The VA was criticized for its delay in disclosing the loss and notifying those affected.

California Senate Bill (SB) 1386 is setting the precedent for reporting and disclosing data security breaches and declarations for privacy and financial security. (See Figure 2 "California SB 1386 Excerpts, Source and Language Summary.") Other states are now adopting laws allowing consumers to "freeze" their credit files, even if they have not been a victim of identity theft. If passed, pending bills in the U.S. Congress, including S.1408: Identity Theft Protec-tion Act and H.R. 4127: The Data Accountability and Trust Act, would also force organizations to be more accountable for the vast amount of personal information that they may have.

Organizations should take heed of these legislative efforts and proactively plan for them by updating their information security practices. Any organization that uses e-commerce in its business practices must align its systems and databases for the protection of information content. Organizations that are subject to these laws should structure their reporting measures according to the following components of the ISO 17799 standard:

- Clause 10.9 establishes electronic commerce countermeasures and cryptographic controls to protect sensitive customer information and all associated electronic records databases.

- Clause 13.1 provides a methodology for reporting incidents supported by timely procedures with appropriate behavior mechanisms and disciplinary processes.

Establish, fund, and monitor training, support, and compliance to ensure that employees receive appropriate training before turning them loose with the tools.

Information Security Objectives and Records Management Components

Although information security is now in the limelight and is being brought to the attention of the executive-level audience, RM is still the basic foundation that branches out into all the various new compliance areas. Records managers need to work with IT to ensure that retention and vital records requirements are addressed and are part of the many inventories that the ISO standard suggests. They must also update their programs to be in line with an information security program's objectives as outlined in the controls and implementation guidance of the ISO 17799 standard.

Maintenance, retention, and protec-

tion requirements of data, information, and IP are addressed in the ISO clauses in Figure 3.

Vital records are those records that are needed to resume and continue business operations after a disaster and are necessary to recreate an organization's legal and financial position in preserving the rights of an organization's employees, customers, and stockholders. If vital records protection methods exist before an information security program is established, they should be integrated or referred to as part of the larger information security scheme. IP and the management and protection thereof have long been addressed by organizations through a vital records program. When electronic records were not prevalent, vital records protection methods included the same premises, such as:

- Appraisal and identification of those records that are deemed vital

- Duplication and dispersal processes

These methods can apply to any electronic environment but the inventories of such records must include not only the paper versions but also their electronic counterparts captured in other media or systems within the organization.

The objective to protect electronic vital records must focus on:

- Newly created records

- Work in progress

- Other information that is not stored on servers and is typically found on users' desktops

Although it can be argued that many electronic records are captured in enterprise resource planning systems, routine backups of this data may be re-circulated so that long-term retention and protection requirements are not addressed.

Initially, allowing employees to transport laptops and other devices with large amounts of data away from the corporate environment was seen as a way to

increase productivity. That is still the case, but controls in the form of policies as to what can and cannot be taken must be established and consistently enforced. As technology offers more ways to compact large amounts of data on very small devices, it is crucial to monitor and correct employees to prevent their actions from compromising the organization's responsibilities for keeping information safe. Establish, fund, and monitor training, support, and compliance to ensure that employees receive appropriate training before turning them loose with the tools.

Compliance also applies to information systems and their audit considerations. Administrators running an organization's information systems must be just as closely scrutinized as the employees within the organization and in virtual spaces.

Stay Ahead of the Curve to Stay Secure

While information security is the newest flavor of the month, chances are that many organizations have no program in place and, therefore, no control over how their employees manage information.

Organizations cannot continue to practice their business in an irresponsible manner. Using the ISO standard to structure their programs is the foundation, but they must also stay ahead of the curve, outguessing and outsmarting potential incidents and occurrences. Websites for information security are pervasive and provide both written materials and podcasts to help keep information professionals informed. Records managers and IT professionals can also help each other achieve a best practices program for information security.

However, any program that an organization initiates will need management support and resources to accomplish it. Collaboration by all parties, including senior management, is essential to achieve compliance in the space of information security. ∎

Ellie Myler is a Certified Records Manager and Certified Business Continuity Professional and a 17-year veteran of the records management industry. A Senior Records Management Analyst with Entium Technology Partners LLC, Myler has previously served as a consultant to Fortune 500 companies in a wide spectrum of industries. She designs and customizes corporate governance programs for records management and business continuity program initiatives and writes and lectures frequently on information management and technology topics. She may be reached at emyler@entium.com.

George Broadbent has more than 17 years of diversified system architecture, network design and implementation, and application development experience, including network management of Novell NetWare and Microsoft Windows 2000/2003 networks. He has designed and built local and wide area networks (LANs/WANs) that include the use of high-availability systems, real-time data replication and hierarchical storage solutions for large multi-site organizations. He has performed the architecture, design, implementation, deployment, and/or support of enterprise electronic mail systems with integrated electronic archiving solutions for Microsoft Exchange-based systems. He can be reached at gbroadbent@entium.com.

References

ARMA International. "VA IG Slams Top Officials in VA Data Theft Incident." *Washington Policy Brief*, July 2006. Available at *www.arma.org/news/policybrief/index.cfm?BriefID=1335* (accessed 26 September 2006).

Bartholomew, Doug. "Responding to Risk: Invisible Enemies." *Industry Week*, 1 March 2006. Available at *www.industryweek.com/ReadArticle.aspx?ArticleID=11440* (accessed 26 September 2006).

Greenemeier, Larry. "The Next Data Breach Could Mean Your IT Job." *Information Week*, 17 July 2006. Available at *www.informationweek.com/security/showArticle.jhtml?articleID=190400266.* (accessed 26 September 2006).

IMlogic. *IMlogic Threat Center – 2005 Real-Time Communication Security: The Year in Review.* Accessed 12 July, 2006 at *www.imlogic.com/pdf/2005ThreatCenter_report.pdg.* No longer available.

International Organization for Standardization. *ISO/IEC 17799: 2005, Information Technology – Security Techniques – Code of Practice for Information Security Management.* Geneva, Switzerland: International Organization for Standardization, 2005.

—————. *ISO/IEC 18043:2006, Information Technology – Security Techniques – Selection, Deployment and Operations of Intrusion Detection System.* Geneva, Switzerland: International Organization for Standardization, 2006.

—————. "New ISO/IEC Standard to Help Detect IT Intruders." Available at *www.iso.org/iso/en/commcentre/pressreleases/2006/Ref1017.html* (accessed 26 September 2006).

U.S. House. *Data Accountability and Trust Act*, 109th Congress, H.R. 4127. Available at *www.govtrack.us/congress/bill.xpd?bill=h109-4127* (accessed 26 September 2006).

U.S. Senate. *Identity Theft Protection Act*, 109th Congress, S.1408. Available at *www.govtrack.us/congress/bill.xpd?bill=s109-1408* (accessed 26 September 2006).