

ISO 2700X: A cornerstone of true security

By Jonathan Gossels & Richard Mackey, Jr.

A brief look at ISO 27001 and ISO 27002, addressing the thorny issue of certification versus compliance – most organizations will find compliance with ISO 27002 rather than certification to ISO 27001 to be the preferred approach.

For years, organizations have been searching for an objective benchmark to measure the security of potential business partners and to distinguish the security of their own services. While not perfect, ISO 17799 emerged as the standard of choice because it overcame many of the critical deficiencies of SAS 70. Specifically, it provided a comprehensive set of security-related topics and an objective means for measuring compliance.

Following the same approach it used with the ISO 900X Quality Assurance standards, the International Organization for Standardization (ISO) has allocated the 27000 numbering range for a series of Information Security Standards. The initial standards are:

- ISO 27000 contains technical definitions used throughout the 2700X series.
- ISO 27001 is a specification for an Information Security Management System (ISMS). ISO 27001:2005 is a re-labeling of BS 7799 Part 2. This is the formal standard used for *certifying* Information Security Management Systems. Its focus is evaluating process rather than content.
- ISO 27002 is a re-labeling of ISO 17799, which was originally BS 7799 Part 1. This standard contains a *Code of Practice* consisting of a comprehensive set of information security control objectives and a menu of best practice security controls.

Let's look briefly at ISO 27001 and ISO 27002 and then address the thorny issue of *certification* versus *compliance*; most organizations will find compliance with ISO 27002 rather than certification to ISO 27001 to be the preferred approach.

ISO 27001

ISO 27001 is formally entitled, *Information Security Management - Specification with Guidance for Use*. Its purpose is to serve as the foundation for third party audits. Not surprisingly, it is process-oriented.

The standard contains an Introduction and seven chapters as shown below:

- Scope
- Normative References

- Terms and Definitions
- Information Security Management System
- Management Responsibility
- Management Review of the ISMS
- ISMS Improvement

The standard also describes a six-stage certification process consisting of the following steps:

- Define an information security policy
- Define scope of the information security management system
- Perform a security risk assessment
- Manage the identified risk
- Select controls to be implemented and applied
- Prepare a Statement of Applicability

It further describes a recursive PDCA lifecycle management approach consisting of: Plan (establish the Information Security Management System), Do (operate the ISMS), Check (monitor and review the ISMS), and Act (maintain and improve the ISMS).

To achieve *certification*, an organization's ISMS must be audited by an assessor who works for a Certification Body. A Certification Body must be accredited by the National Accreditation Body for the relevant geography.

The certification process requires clear *segregation of duties* in that the organization performing the certification must not have been involved in providing either consulting or training.

ISO 17799/27002

ISO 17799/27002 defines an overarching security framework consisting of 133 specific controls organized around 39 control objectives. This balanced framework serves as the basis for both measuring an organization's effectiveness in addressing risk and structuring an organization's overall security program. Because ISO 17799/27002's requirements are largely a superset of other major regulations, achieving ISO 17799/27002 compliance positions most organizations to be well on their way to meeting the requirements of Sarbanes

Oxley, Gramm-Leach-Bliley, HIPAA, and other pertinent regulations. Each of the 11 topical areas of the standard is described briefly below.

Risk assessment and treatment

This section requires organizations to adopt a systematic risk assessment approach. This ensures that the security program that emerges from ISO 17779/27002 addresses real business risks and priorities.

Security policy

This section requires a written security policy and an ongoing process for its review and evaluation.

Organization of information security

The most important topics within the Organization of Information Security section include management commitment to information security, allocation of security responsibilities, and security of external parties.

Asset classification and control

The Asset Classification and Control section forms the basis of understanding and assessing risk in the environment under review. It requires that organizations catalog and classify by sensitivity both physical and information assets. Furthermore, it requires that organizations define owners, custodians, and users of information to formalize the process of granting access to and tracking the use of information. The processes described in this section help organizations ensure that information assets receive an appropriate level of protection. It also addresses physical asset inventory and labeling.

Human resources security

The behavior of people is an essential element of any security environment. The Human Resources Security section deals with security issues across the employment lifecycle from pre-employment through termination. Organizations must ensure that their employees are trustworthy and well informed. The section also covers areas like employee background checks, required sign-off on appropriate behavior policies, and training to educate employees regarding their responsibility for the security of the organization and its assets.

Physical and environmental security

The Physical and Environmental Security section addresses secure areas, equipment security, and general controls. This section outlines the processes associated with ensuring the safety of employees and assets, the location and physical security of offices, the security of cabling, and operation of collocation facilities.

Communications and operations management

The Communications and Operations Management section is a major part of the standard. Topics within it include:

- Operational procedures and responsibilities
- Third party service delivery management
- System planning and acceptance
- Protection against malicious software
- Backup
- Network security management

- Media handling
- Exchanges of information
- Electronic commerce services
- Monitoring

Access control

The Access Control section contains almost all the aspects of computer security that are covered in typical security reviews. In other words, while much of the standard deals with processes that organizations should follow, Access Control delves into the mechanisms and practices that have a direct impact on the effective security of the applications, networks, and systems in an enterprise. It covers the design of applications and networks, configuration of firewalls, login and password controls, security logging and monitoring, and the use of VPN technology for remote access.

Information systems acquisition, development, and maintenance

The Information Systems Acquisition, Development, and Maintenance section is intended to ensure that security is an integral part of information systems, that correct processing occurs, that confidentiality is protected, that file systems are secure, that the development process is properly controlled, and that technical vulnerabilities are managed.

Information security incident management

The objective of the Information Security Incident Management section is to ensure that information security events and weaknesses associated with information systems are communicated in a timely manner allowing time for corrective action to be taken.

Business continuity management

The Business Continuity Management section identifies measures to mitigate potential disruption of business activities and critical business processes caused by major failures or disasters.

Compliance

The Compliance section places the technical requirements of the standard in the full legal, regulatory, and business context. Its objective is to avoid breaches of any law, statute, regulation, or contractual obligation. This section requires organizations to understand all their legal requirements, including those specified by governments, regulatory agencies, partners, and even the organizations' own policies.

Broad use of the standards

History has shown that far more organizations used ISO 17799 as a framework for conducting comprehensive security assessments to improve the security and controls of their IT infrastructure rather than for the specific purpose of certification. It is important to recognize that the ISO standards have significant value beyond certification.

Compliance vs. certification

The decision to certify or comply is more than one of cost. The ISO 27001 and 27002 standards serve different purposes. ISO 27001 assesses whether an organization follows a coarse-grained set of pro-

cesses that are integral to maintaining the security of an enterprise. Certification assumes that if these processes are in place then effective security automatically follows. In contrast, 27002 describes a comprehensive set of concrete and fine-grained practices with which an enterprise can be compared.

Unless there is a clear business reason – such as customers or partners demanding certification to do business – most organizations would be better served thinking in terms of compliance with ISO 27002 rather than certification to ISO 27001. Because of the expense, without a clear business driver, there is little incremental value in spending those formal certification dollars. In most cases, having a reputable security firm attest that an organization is “substantially compliant” is sufficient.

Just as with ISO 9000, the marketplace is not homogenous. Certain vertical markets such as aerospace or certain supply chains may latch on to the ISO 27001 certification as a required fact of life.

Where most organizations fall short

After conducting numerous ISO 17799/27002 assessments, it is clear that many organizations fall short in the same areas and those deficiencies can cause a cascade of non-compliance of other required controls. For example, few organizations have an up to date inventory of their information assets. When information asset catalogs exist, they frequently do not contain information about data owners, business risk, and information sensitivity. Without this information, it is impossible to develop meaningful information handling policies and procedures.

Similarly, few organizations have implemented a comprehensive risk management approach. This means that they have no consistent way of determining the business risk associated with the various elements in their environment and, consequently, cannot know if they have appropriately protected those resources.

IT departments have traditionally operated on the *heroic actions* of individual employees; people that know exactly how the environment is put together and do whatever it takes to keep the systems running. While seemingly efficient, the problem with that model is that the organization suffers if that key person is suddenly out of the picture for some reason. Few organizations have formally docu-

mented operating procedures that enable critical functions to be performed consistently by multiple people.

Perhaps most importantly, the standard recognizes that security must be a *corporate commitment*, not the responsibility of a specialty group within IT. This requires the creation of a cross-functional security management team. Few organizations currently have such a security management team in place. On the other hand, the ones that do are making remarkable progress.

Last word

The ISO 27001 and ISO 27002 standards have gained attention for being a practical mechanism for both assessing and asserting good security practices. ISO 17799/27002, in particular, helps companies build comprehensive and cost-effective enterprise security programs, ensuring that security resources are applied wisely and efforts are focused on activities that reduce real business risk. Investment in ISO 17799/27002 compliance promises a high return because the requirements are largely a superset of other major regulations. Achieving ISO 17799/27002 compliance positions most organizations to be well on their way to meeting the requirements of Sarbanes Oxley, Gramm-Leach-Bliley, HIPAA, and other relevant regulations.

About the Authors

Jonathan G. Gossels, ISACA, CISM, is President & CEO of SystemExperts Corporation, advising clients in compliance, technology strategies, managing complex programs, and resolving issues related to security initiatives. He can be reached at jon.gossels@systemexperts.com.

Richard E. “Dick” Mackey, ISACA, CISM, VP of Consulting of SystemExperts Corporation, is regarded as one of the industry’s foremost authorities on distributed computing infrastructure, compliance, and security. He has advised leading Wall Street firms on overall security architecture, virtual private networks, enterprise-wide authentication, and intrusion detection and analysis and has unmatched expertise in the Open Software Foundation Distributed Computing Environment. He can be reached at dick.mackey@systemexperts.com.