CHAPTER NINETEEN

19

Controls to Establish an Effective IT Security Environment

CONCERNS REGARDING INFORMATION TECHNOLOGY (IT) security are perhaps the most major issue impacting IT auditors. Other chapters have talked about the importance of establishing effective internal controls, following Sarbanes-Oxley (SOx) rules, or using the Control objectives for information Technology (CobiT) framework, but IT security risks and incidents are the topics that create news headlines. This IT security risk is a greater concern in today's world of vast Internet connections and increasing reliance on cloud computing strategies. An enterprise's audit committee and senior management are often the parties that read about IT security breaches elsewhere and often question the chief audit executive (CAE) and IT auditors about enterprise IT security.

To gain this assurance about having effective IT security, an enterprise needs to establish and build an effective IT security environment. This task is the responsibility of IT operations and enterprise management at all levels. IT auditors can assist in this process by using their knowledge of effective internal controls to both review existing IT security controls and to act as internal consultants to help improve them. They can assist an enterprise in establishing an effective security environment.

This chapter will focus on building an effective IT security environment from three perspectives. We will introduce the generally accepted systems security principles (GASSP) that have been promoted by the Information Systems Audit and Control Association (ISACA) and others. They can be a major aid in establishing an effective IT security environment. As a second topic, we will explore ways to build effective IT perimeter security. While the locked computer operations center from the mainframe days is less of a risk today, security risks are much greater in today's Internet-based

e-commerce environments where network controls define the security perimeter. The chapter will discuss some IT perimeter security controls that IT auditors should consider when reviewing internal controls in these areas.

As a third topic for this chapter, we will discuss the importance of establishing an effective, enterprise-wide security strategy. Just as an employee code of conduct sets some high level rules for all enterprise stakeholders, an effective IT security strategy establishes some IT security-related rules. A well designed and well implemented IT security strategy can improve many aspects of enterprise operations. IT auditors should be aware of effective best or good practices in these areas and should use these to make effective IT security recommendations in their audit reviews.

GENERALLY ACCEPTED SECURITY STANDARDS

Either through their own work, contacts with fellow financial internal auditors or their external auditors, many IT auditors are aware of what are called generally accepted accounting principles and auditing standards (GAAP and GAAS, respectively). While GAAP is being replaced with international accounting standards today, these are the informal rules that external auditors use to assess enterprise accounting practices and then to perform audits of financial statements. They are not point-by-point specific rules but sets of general good practices that external auditors have used over the years.

With an approach similar to GAAP and GAAS, IT auditors and enterprise IT management have GSSP as a set of best practices for developing effective IT security practices and standards. GASSP is a consensus set of IT security-related principles, standards, conventions, and mechanisms that IT security practitioners should employ, that information processing products should provide, and that information owners should acknowledge to ensure the security of their information and IT systems. GASSP relates to physical, technical, and administrative information security and encompasses pervasive, broad functional, and detailed security principles. Its nomenclature defines a series rules, procedures, and practices that relate to the implementation of effective IT security practices in an enterprise. With ongoing rapid changes in IT technology, GASSP is expected to evolve accordingly.

GASSPs origins go back to 1990 when the U.S. National Research Council published *Computers at Risk* (CAR),[1] in what became a landmark book that emphasized the urgent need for the United States to better focus attention on information security. The GASSP document is a direct result of a key recommendation from that CAR report calling for the development of a comprehensive set of Generally Accepted System Security Principles that would provide a clear definition of IT security's essential features, assurances, and practices. The CAR report proposed using GAAP as a model for GASSP and also cited building codes and standards by the Underwriter's Laboratory[2] as examples of GASSP in other fields.

The International Information Security Foundation (I^2SF), a unit of the International Information Systems Security Certification Consortium $(ISC)^2$ that also sponsors the CISSP certification discussed in Chapter 30, launched a professional committee to develop GASSP. They along with ISACA published the description of GASSP, with its

current version 2.0 released in 1999.[3] As its name implies, these principles are generally accepted, that is, they represent concepts commonly being used at the present time to secure IT resources. The principles in that GASSP study are not new to the security profession. They are based on the premise that (almost) everyone should apply them when developing or maintaining an IT security system.

GASSP Principles

GASSP is based on eight high-level principles that management, IT security specialists, and IT auditors can use as an anchor on which to build and their IT security programs. These principles are intended to be a security guide when creating new systems, practices, or policies. They are not designed to produce specific answers, and should be applied as a whole, pragmatically and reasonably. Each of these eight principles is expressed as a one-line section heading and explained in the following list:

1. **IT security supports the mission of the enterprise.** The purpose of IT security is to protect an enterprise's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the enterprise's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Unfortunately, security is sometimes viewed as thwarting the mission of the enterprise by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. As a result, IT auditors should be aware that well-chosen security rules and procedures do not exist for their own sake—they are put in place to protect important assets and support the overall organizational mission.

   Security, therefore, is a means to an end and not an end in itself. For example, an enterprise's security good practices are usually secondary to their need to make a profit. Security, then, *ought to* increase the firm's ability to make a profit. In a public-sector agency, security is usually secondary to that agency's providing services to citizens. Security, then, *ought to* help improve these public services. Thus, managers and security specialists need to understand both their overall enterprise mission and how each IT system supports that mission. After these system roles have been defined, these security requirements can then be explicitly stated in terms of the enterprise's mission.
2. **IT Security is an integral element of sound management.** IT systems are often critical assets that support the mission of an enterprise. Protecting these assets can be as important as protecting other resources, such as cash, physical assets, or employees. However, including security considerations in the management of information and IT systems do not completely eliminate the possibility that these assets will be harmed. Ultimately, management must decide what level of risk they are willing to accept, taking into account the cost of security controls.

   As with other resources, the management of information and IT systems may transcend organizational boundaries. When an enterprise's information and IT systems are linked with external systems, management's responsibilities extend beyond the enterprise and both management and IT audit should know what general levels or types of security are employed on those external systems and

should seek assurances that the external system provides adequate security for their enterprise's needs.

3. **IT security should be cost-effective.** The costs and benefits of security should be carefully examined *in both monetary and nonmonetary terms* to ensure that the cost of controls does not exceed expected benefits. Security should be appropriate and proportionate to the value of and degree of reliance on the IT systems and to the severity, probability, and extent of potential harm. Requirements for security vary, depending on the particular IT system.

   In general, IT security is a smart business practice, and by appropriately investing in security measures, an enterprise can reduce the frequency and severity of IT security-related losses. For example, an enterprise may estimate that it is experiencing significant losses per year in inventory through the fraudulent manipulation of its IT inventory control system. Security measures, such as an improved access control system, may significantly reduce this loss. Moreover, a sound security program can thwart hackers and reduce the frequency of viruses.

   Security benefits have both direct and indirect costs. Direct costs include purchasing, installing, and administering security measures, such as access control software or fire suppression systems. Additionally, security measures can sometimes affect system performance, employee morale, or even retraining requirements. All of these should be considered in addition to the basic cost of an IT security control itself. In many cases, such as in the costs of administering an access control package, these additional costs may well exceed the initial cost of the control. Solutions to security problems should not be chosen if they cost more, in monetary or non monetary terms, directly or indirectly, rather than simply tolerating the problem.

4. **Systems owners have security responsibilities outside of their own organization.** If a system has external users, its owners have a responsibility to share appropriate knowledge about the existence and general extent of security measures so that other users can be *confident* that their system is adequately secure. This does not imply that all systems must meet any minimum level of security, but does imply that system owners should inform their clients or users about the nature of the security.

   The difference between responsibility and accountability for IT security is not always clear. In general, *responsibility* is a broader term, defining obligations and expected behaviors. The term implies a proactive stance on the part of the responsible party and a causal relationship between the responsible party and a given outcome. The term *accountability* generally refers to the *ability to hold* people responsible for their actions. Therefore, people could be responsible for their actions but may not be held accountable. For example, an anonymous user on a system is responsible for behaving according to accepted norms but cannot be held accountable if a compromise occurs since the action cannot be traced to an individual.

   This principle implicitly states that people and organizations have a shared responsibility and accountability for their IT systems which may be shared. In addition to sharing information about security, enterprise managers should act in a timely, coordinated manner to prevent and to respond to breaches of security to

help prevent damage to others. However, taking such action should *not* jeopardize the security of systems.

5. **IT security responsibilities and accountabilities should be made explicit.** The security-related responsibility and accountability of owners, providers, and users of IT systems and other parties concerned with IT systems security should be explicit. These responsibilities may be internal to an enterprise or may extend across enterprise boundaries. Even a smaller enterprise should prepare documentation that state an enterprise's security policies and explicit IT security responsibilities. However, this element does *not* mean that individual accountabilities must be provided for on all systems. For example, many information dissemination systems do not require user identification or use other technical means of user identification and, therefore, cannot hold users accountable.
6. **IT security requires a comprehensive and integrated approach.** Providing effective IT security requires a comprehensive approach that considers a variety of areas both within and outside of the IT security field and extending throughout the entire information life cycle. To work effectively, security controls often depend on the proper functioning of other controls. Many such interdependencies exist. If appropriately chosen, managerial, operational, and technical controls can work together synergistically. However, without a firm understanding of the interdependencies of security controls, they can actually undermine one another. For example, without proper training on how and when to use a virus-detection package, users may apply the package incorrectly and, therefore, ineffectively. As a result, users may mistakenly believe that if their system has been checked once, it will always be virus-free and may inadvertently spread a virus. In reality, these interdependencies are usually more complicated and difficult to ascertain.

   The effectiveness of security controls also depends on such factors as system management, legal issues, quality assurance, and internal and management controls. IT security also needs to work with traditional security disciplines including physical and personnel security. Many other important interdependencies exist that are often unique to the enterprise or system environment. Managers should recognize how IT security relates to other areas of systems and enterprise management.
7. **IT security should be periodically reassessed.** IT systems and the environments in which they operate are dynamic. System technology and users, data and information in the systems, risks associated with the system, and security requirements are ever-changing. Many types of changes affect system security including: technological developments, changes in the value or use of information; or the emergence of a new threat. In addition, security is untested and *never* perfect when a new system is implemented, and system users and operators discover new ways to intentionally or unintentionally bypass or subvert security. Changes in an IT system or its environment can create new vulnerabilities. Strict adherence to security procedures is rare, and procedures become outdated over time making it necessary to periodically reassess IT systems security.
8. **IT security is constrained by societal factors.** The ability of security to support the mission of an enterprise may be limited by such factors, as social issues where security and workplace privacy can be in conflict. For example, security is often

implemented on an IT system by identifying users and tracking their actions. However, expectations of privacy vary and can be violated by some security measures. In addition, security controls may be mandated by law in some cases. Although privacy is an extremely important societal issue, it is not the only one. The flow of information, especially between a government and its citizens, is another situation where security may need to be modified to support a societal goal. In addition, some authentication measures may be considered invasive in some environments and cultures.

Security measures should be selected and implemented with a recognition of the rights and legitimate interests of others. This may involve balancing the security needs of information owners and users with societal goals. However, rules and expectations change with regard to the appropriate use of security controls. These changes may either increase or decrease security. The relationship between security and societal norms is not necessarily antagonistic. Security can enhance the access and flow of data and information by providing more accurate and reliable information and greater availability of systems. Security can also increase the privacy afforded to an individual or help achieve other goals set by society.

As an IT auditor can observe, these eight GASSP principles are not definitive but outline a general framework that should be the basis for many aspects of good IT security. An IT auditor cannot use them to make an audit point saying that an auditee, for example, is in violation of "GASSP Principle 3." Rather, these eight principles should be used to form a basis to assess the strengths and weaknesses of any IT security system or environment being reviewed.

GASSP is strongly promoted through ISACA materials and referenced as an outside resource through the Institute of Internal Auditors' Web site. IT auditors may see a greater use and acceptance of GASSP in future years. These principles should help an IT auditor to better assess security in many environments. GASSP can provide the basis for an effective IT security environment in an enterprise.

Role of GASSP in the IT Organization

Moving beyond the previous eight GASSP principles, an enterprise, its IT security function, and certainly IT audit will have to rethink and reorganize some practices in order to embrace GASSP. Exhibit 19.1 shows the high-level role of GASSP in an enterprise, with consideration given to its installed technology products and other factors. While there are many ways to implement GASSP, the IT auditor should not lose track that GASSP is based on some broad and strong IT security principles. These pervasive principles address the properties of IT security information confidentiality, integrity, and availability. They provide general guidance to establish and maintain the security of information.

We will go around the points in this exhibit to briefly describe some to the key elements of GASSP and how they relate to one another and to an overall IT security environment. Each of these areas may differ, based on the enterprise, its size, and domicile. We start at the center of this exhibit with the security standards and other

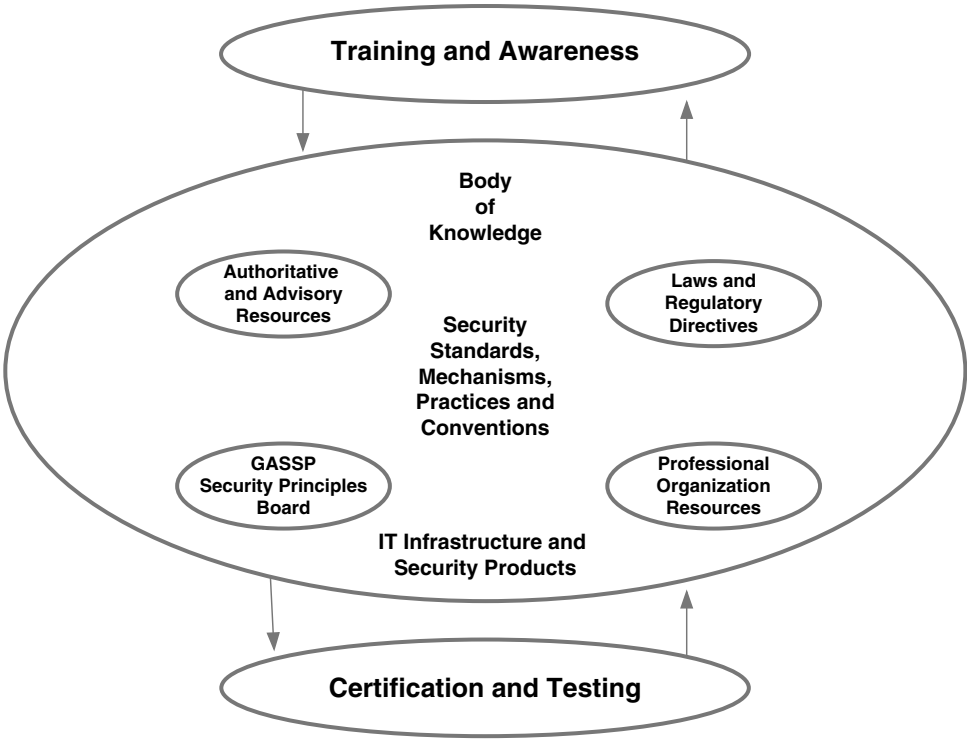

EXHIBIT 19.1 Role of GASSP in the Enterprise

mechanisms, move up to the body of knowledge, and then clockwise around to the other factors necessary to form an effective security environment using GASSP.

- **Security Standards, Mechanisms, Practices, and Conventions.** The core of any effective security environment is a set of strong enterprise-specific security standards, mechanisms, practices, and conventions. These are the types of issues that an IT auditor should have reviewed and hopefully found effective in an IT general controls review.
- **Body of Knowledge.** We have summarized GASSPs principles here, but a wide variety of persons in an enterprise should understand these broad principles and have expressed a commitment to understand and implement them on a regular basis. The idea is that if there is a question about some IT security practice, the enterprise should go back to these broad principles to interpret and resolve any issues.
- **Laws and Regulatory Directives.** Every enterprise is subject to a variety and often differing set of laws and regulations. A good example here can be found in personal privacy laws that differ greatly from one country to another. GASSP must always be interpreted based on these different and sometimes often changing rules.
- **Professional Organization Resources.** Professional organizations such as ISACA or the IIA regularly issue guidelines and standards that add new requirements to IT security approaches or change approaches. An enterprise must be aware of these matters and make changes to its IT security environment accordingly.

- **IT Infrastructure and Security Products.** There are a wide variety of IT application and infrastructure products that may help direct or modify approaches to IT security. While an enterprise should not install products that are deficient in these security principles, it is always necessary to be aware of any unique characteristics of any such installed produce and to make appropriate adjustment to other IT security practices.
- **GASSP Security Principles Board.** When an enterprise embraces GASSP, it needs to install some authoritative persons in an enterprise to properly interpret its applications of GASSP. Someone from the IT security function, the quality assurance group, or a representative from IT audit may be an appropriate resource here. While no one in the enterprise may be an ''expert'' on GASSP, the idea is to appoint a reasonable person who understands GASSP principles, can interpret them based on any questions raised, and can be an umpire or referee when needed.
- **Authoritative and Advisory Resources.** Although they do not typically sell consulting services, an enterprise should be closely tied with ISACA or (ISC)[2] publications and resources for any updates and other interpretive materials about GASSP.
- **Training and Awareness.** GASSP is of little value to an enterprise unless key stakeholders are trained on its principles. System developers, in particular, should be aware of the GASSP principles and use it when launching secure, effective applications for the enterprise. Similarly, IT auditors should learn and use the GASSP framework in their internal controls.
- **Certification and Testing.** There are no GASSP certifications or testing programs in place at present, but such efforts will be updated if there are any significant updates or changes to GASSP in the future.

GASSP principles have been released for some years but they still have not received a wide level of acceptance by enterprises in the United States to date. However, with our ever-changing and technologically advancing world today as well as ever-growing IT security concerns, GASSP provides an effective basis or framework for looking at and assessing IT security.

EFFECTIVE IT PERIMETER SECURITY

IT perimeter security once referred to little more than locks on the computer room door and a building entrance guard back in the days of mainframe centralized computer systems. The walls and door to that mainframe computer center of old represented the perimeter or an enterprise's IT operations. Today, that perimeter boundary has really changed with such things as connections to wireless virtual local area networks (LANs), the Internet and worldwide telecommunications networks, and connections to cloud computing services using Software as a Service (SaaS) processing strategies. The concept of a security perimeter surrounding an enterprise's IT resources has certainly changed, but there is still a need—even a greater need—for effective IT perimeter in today's environments.

IT auditors should understand and focus both their general and applications controls reviews on this concept of IT perimeter security.

ESTABLISHING AN EFFECTIVE, ENTERPRISE-WIDE SECURITY STRATEGY

Perimeter security in today's IT-centric and wireless communications world involves complex architectures and continually emerging and evolving technologies. To ensure an enterprise has a secure external IT systems perimeter, all appropriate technologies must be evaluated. By following the basic fundamental design concepts, such as using a top-down security model to identify and evaluate security assets, applying the connection trust model to external connections and implementing a multiple trust zone architecture appropriate to the organization, a sound perimeter architecture should result. A top-down security approach is where more senior management understands the seriousness and initiates a process, such as IT security, which is then systematically percolated down to through the ranks and to the lower level operations staff. This differs from a bottom-up approach, in which the less-senior operational staff initiates the process and then propagates their findings upward to management as proposed policy recommendations. As management has no information on what associated threat is and its implications—ideas on resource allocations, possible returns, and methods to implement security—this approach has at times almost sparked a fiasco. IT audit can often take the lead in initiating such a top-down approach by securing an initial buy-in from the audit committee through their audit recommendations.

Perimeter security requires implementing an architecture that utilizes existing IT components, based on a defense-in-depth approach to the security of the external network perimeter, to help ensure the perimeter security of any network will be well protected. Before undertaking the design or implementation of an enterprise network and its components, a comprehensive security architecture should be developed.

The reality, however, is that many enterprises, while recognizing the need for security, often neglect or reduce significant IT perimeter security concerns. An enterprise should design and implement a top-down security infrastructure strategy and approach to support an enterprise's communication needs and allow it to transact business securely in today's electronic world. Exhibit 19.2 shows this top-down security

EXHIBIT 19.2 Top-Down IT Security Model

model, and the paragraphs following will discuss its elements in greater detail. The security infrastructure should apply equally to pre-existing connections and to new initiative connections, and an organization's network should be protected based on the risk it represents to the enterprise.

The top level of the Exhibit 19.2 model calls for effective security policies. Although it sometimes seems almost too obvious, an IT auditor reviewing controls in an IT security environment should initially develop an understanding of existing IT security policies for the enterprise. Although usually only at a high level, any such set of policies should cover all aspects of IT security. It may be sufficient to state that the enterprise's IT security polices will be based on the principles of ISO27002, as discussed in Chapter 18, as well as CobiT from Chapter 2.

These strategies should be supported by detailed security standards that cover performing system monitoring, configuring a system as an application or web server, or configuring a firewall to segregate systems into designated zones. The standards should be application- and operating-system-specific, and detailed enough to enable a knowledgeable user to perform the activities highlighted in a standard or configure the system or application. Finally, the standards should specify the steps to be taken, such as sign-offs, if a breach of these standards is required.

IT security operations and an IT auditor should think of perimeter security in terms of a series of trust zones. That is, IT operations should identify and classify all current connections and systems into logical security-related zones. A key element of this security classification is access to the Internet and other network connections such as vendor support systems. The following are four potential classifications for interconnected systems:

1. **Trusted Systems and Processes.** These are systems are directly under the control of the IT organization. Trusted users and systems potentially require full access to internal systems.
2. **Semi Trusted Systems and Processes.** These are often vendor support and some business partner systems that require authenticated access to protect exposed systems that are not publicly accessible.
3. **Untrusted Systems and Processes.** Customer-related systems and processes often require authenticated access rights to specific information resources on exposed systems that are publicly accessible. However, these systems are not fully secure and untrusted.
4. **Hostile Systems and Process Threats.** Very restricted access should be allowed for these types of systems, and unauthorized access attempts should be detectable in real time.

Following these classifications, connections such as support vendors, customers, subsidiaries, and business partners, should be reviewed and allocated to a level of trust based on the level of control that can be maintained. However, identifying each connection in a large organization can be difficult at best. An effective method to launch such a classification is to conduct a workshop with a broad range of knowledgeable staff members who understand the associated concepts and who are familiar

with other projects within the enterprise and its IT operations. Although it is unlikely that a single workshop will identify all connections, this type of exercise may help to identify the majority of connections and other staff members within an enterprise that may be responsible for identifying these and other connections.

These connections and their network connections protocols should be documented and used to develop detailed controls to allow accesses to and from appropriate destinations. As a result, the enterprise should segregate different parts of its network into multiple trust zones.

The segregation and classification of systems and processes provides for the separation of systems based on the defined trust categories. An enterprise's internal IT network always should have its own network segment, including web, mail, domain name, and other servers, that should be classified into appropriate trust zones and partitioned or segmented appropriately. This may result in each of these services being segmented on separate zones or may result in a number of these services being implemented into a single zone. The final design of a perimeter security architecture will be dependent on the classification of systems and services, but the design of these security zones and classifications is a critical component of IT perimeter security.

BEST PRACTICES FOR IT AUDIT AND SECURITY

To summarize our comments about the importance of an effective IT perimeter security strategy, as well as comments in related chapters, we were impressed by the benchmark study findings of the IT Policy Governance Group,[4] an IT study group with a membership including the IIA, ISACA, companies such as Oracle and many others. This study benchmarked more than 100 practices for information security and IT audit in such areas as managing the IT architecture; managing information and data; managing IT operations; ensuring systems security; monitoring and evaluating; managing quality; managing risks and governance. Some of the key findings from this benchmarking study were:

- About 1 in 10 of the organizations surveyed (12%) experience the best outcomes for information security and IT audit with the lowest levels of data loss or theft, least business disruption, and fewest problems with audit. This says that IT audit has been viewed as effective for a minority of enterprises today, and there is much need for improvements.
- A majority of organizations reviewed, nearly 7 in 10 (69%) are experiencing higher rates of data loss or theft, higher levels of business disruptions from IT failures, and more difficulty with passing regulatory audits in IT. This says that enterprises continue to experience data loses and other security risks and have trouble complying with regulatory audits.
- Almost 2 in 10 organizations (19%) experience the worst outcomes with the highest rates of data loss or theft, the highest levels of business downtime, and the most difficulties passing audits in IT.

This really says that many enterprises continue to experience IT security threats but have problems with their current IT audit processes.

The study goes on to emphasize the importance of using CobiT, as discussed in Chapter 2, ITIL from Chapter 7, and ISO security standards, as introduced in Chapters 18 and 25. Based on a recent benchmarking study across a wide range of enterprises and conducted by a series of well-known IT professional organizations and vendors, this IT policy study has information supportive of many themes in this book, with an emphasis in particular on IT security. The interested IT auditor may consider these issues further by exploring the IT Policy Institute at www.itpolicycompliance.com.

NOTES

1. Marjory Blumenthal, *Computers at Risk: Safe Computing in the Information Age*, National Research Council, System Security Study Committee, DEC, 1990.
2. www.ul.com/global/eng/pages/.
3. Generally Accepted System Security Principles (GASSP), Version 2.0, June 1999, www.isaca.org.
4. Guidance for Best Practices in Information Security and IT Audit, 2009, www.itpolicycompliance.com.