

A prevalent misconception about information security is that an organization can achieve conformance and improve information security via checklists and technology-focused standards alone. Creating an information security management system extends beyond the IT department and requires a thoughtful, customized approach for every business.

Fiction: One-Size-Fits-All

There is no checklist that can replace the guidance of senior management and the organization's strategic business objectives in implementing a defensible and sustainable information security program.

A checklist or template is an excellent way to harden a server, desktop or router by providing documented security best practices and a way to consistently apply controls to multiple systems. But this bottom-up model falls apart when an attempt is made to rely on a checklist methodology to implement an enterprise-wide information security strategy. In the same way investment wisdom dictates that one should "buy low and sell high," or that writing a software program is "just typing," the checklist model misses the underlying complexity of the processes and variable requirements of an organization's strategic business objectives for information security. The checklist model lacks the structure for appropriate planning, governance and flexibility for reasonable implementation and continual improvement of information security management.

"There is no simple off-the-shelf solution that is a substitute for a holistic, corporate-sponsored information security initiative."

Requirements for Auditors

With the publication of ISO 27006:2007, the "requirements for bodies providing audit and certification of information security management systems (ISMS)", the International Standards Organization has raised the bar on the requirements for auditors.

It is no longer acceptable for a quality auditor to read the standard (ISO 27001:2005), and execute a certification audit. In addition to the existing ethical and legal requirements for auditors in general, auditor skills and competence have moved front and center in the effort to enhance credibility of certification and provide added benefit to the certifying organizations. ISO 27006 requires that a certification body supply auditors whose *"skills and collective competence is appropriate to the activities to be audited and the related information security issues."*

ISO 27006 specifies levels of education, years of experience in information technology, information security experience, currency of knowledge and experience, knowledge of legislative and regulatory requirements, knowledge of information security threats and trends, understanding of client-specific threats and vulnerabilities, ability to assess effectiveness of controls, experience with incident management and risk management for auditors competent to do ISO 27001 certification audits. ■

continued on page 2

Information Security and IT - In an increasingly complex environment nearly every business in the United States must respond to legal and regulatory requirements that affect their use of information assets to meet business objectives. Organizations operating in the global marketplace face even more numerous and demanding requirements. In such a complex legal and regulatory environment, many organizations are deferring decisions about information security to their IT personnel that should first be addressed by the company's senior management, general counsel or privacy officer. In the vacuum of coordinated management planning and guidance, the checklist model becomes an attractive recourse for IT. As a result, decisions are made that may make sense from a tactical perspective but may not be in the best strategic business interests of the organization or the shareholders. In the worst-case scenario, such decisions can unnecessarily expose the organization to a multitude of legal, regulatory, contractual and compliance issues.

Comprehensive Solution - Information Security is a process, not simply a template. Implementing a sound and effective information security program requires a top-down approach. Goals and objectives of the program must be defined in the context of strategic business objectives. Implementation of the program should reflect these goals and objectives and reasonably address identifiable risks the organization may encounter. Once implemented, the program must be monitored and continually improved. Changes in the business environment must be assessed for risk, and corrective or preventative actions taken.

Proven Objective – It is the myth of “certification in a box” that the checklist methodology is comprehensive. Effective and sustainable information security is not, however, the product of a checklist. Implementation of tactical controls must be guided by documented, defensible direction provided by senior management, and aligned with the strategic business objectives of the organization. Only through effective governance can an organization hope to implement a security program that reasonably and appropriately manages risk.

John B. Weaver, president and CEO of JBW Group International, advises executive management and board directors to take an active interest in their organization's information security posture. Ultimately, it is the board's fiduciary responsibility and avoidance of the inherent complexities of information security is not a very defensible position if a breach occurs. ■

Fact: ISO 27001 is the standard

Organizations should use this standard as a tool for building a holistic and complete information security management program.

Whether an organization intends to formally certify their information security management system (ISMS) or not, the comprehensive framework of ISO 27001 is an exceptional tool for implementing an information security program. An internationally recognized, business focused, process driven and continuously improving information security program will reduce risk and bring value to the organization on multiple levels.

In the rush to implement controls, many organizations immediately go to the 11 general areas, 39 control objectives and 133 specific controls contained in Annex A of the standard as the path to compliance. The real power of the standard is contained in clauses four through eight of the general requirements. These general requirements outline, implicitly and explicitly the role of management and of corporate governance in the identification and treatment of risk to the organization. ■

FOR MORE INFORMATION...

JBW Group International

P.O. Box 19373

Minneapolis,

Minnesota 55419 USA

www.jbwgroup.com

Email: info@jbwgroup.com

1.877.97.27001