

Research Bulletin

Date: November 6, 2006,
Title: Achieving Effectiveness in Information Protection

Written by Karen Worstell

Introduction

Since the effort toward definition of information security practice began in the early 1990s, the issues and approaches have been continuously evolving. The ability to demonstrate effectiveness in information security is no longer an option, but an imperative in the interconnected ecosystem that enables business. The update to BS 7799 recently released by ISO/IEC provides an excellent foundation toward defining an Information Security Management System (ISMS). An understanding of the standard's recommendations for demonstrating effectiveness of the ISMS is essential to realize the full potential of this definition and standardization of information security practice across businesses. The benefits of implementing measurement-based ISMS will only increase as demands for assurance of sound information management practices intensify. Companies will be well-served to start now with an ISO/IEC 27001 based ISMS implementation.

In particular, the ISO/IEC 27001 **(ISO/IEC 27001:2005(E))** standard defines an excellent set of processes that should form the basis of a well-rounded security practice for any agency or enterprise. In addition, it establishes expectations for accountability and evidence of control appropriateness and control effectiveness. These three areas, process, accountability and evidence, are critical to any security program's success and are discussed in more depth in this research note, along with some suggestions for implementation.

Why Use a Standards Approach?

Many organizations express frustration with the multitude of guideline regulations and statutes today. Many of them require documented compliance (i.e., evidence) in the areas of privacy, security, business continuity, disaster readiness, E-Discovery and data integrity. The application of a standard that is descriptive of the general processes, management accountability and requirement for evidence of controls, provides a foundation for streamlining compliance, thus saving money on the compliance process over what would be spent without this organizing approach. Adherence to standards accepted as best practice, along with evidence of implementation, will provide a basis for demonstration of good faith efforts, establish a foundation for continuous process improvement and reduction of cost, and will assist with building a culture of cross-functional/cross-organizational communication that may help organizations avoid legal sanctions and penalties caused by compliance deficiencies resulting from poor communications among stakeholders. ISO/IEC 27001 will also improve inter-enterprise communication regarding established practice for information protection, integrity, confidentiality and availability, providing a common language for trust in the interconnected business community.

Background on ISO/IEC 27001

The reader will benefit from an independent reading of ISO/IEC 27001, as a detailed treatment of the standard within this research note is redundant to the standard itself. Readers will find the standard well-organized and very worthwhile to purchase and examine.

The ISO/IEC 27001 establishes a model for an Information Security Management System. Rather than being a technical approach to network security, this standard sets the bar for the business processes associated with a tailored programmatic approach to securing information assets. It extends the OECD Guidelines for the Security of Information Systems and Networks¹ with guidance that, as it becomes widely adopted, will help information security achieve its place as an attribute of business that is as well-

¹ OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org.

accepted as quality and safety. In the near term, this standard establishes a baseline by which interested parties can have confidence in the security controls of their business partners.

The model uses a well-known Plan-Do-Check-Act (PDCA) top level process lifecycle and further defines the top level process to include “establishing, implementing, operating, monitoring, reviewing and improving” the Information Security Management System. Each of these areas has functional responsibilities that are defined in detail, along with the *de rigueur* glossary of terms. Challenges in ISO/IEC 27001 exist in the details and consulting support may be in order for many organizations who desire to make this management system part of their “organizational DNA”, particularly in the discipline of demonstrating control design and effectiveness through proper measurement, testing and reporting.

Opportunities Using ISO/IEC 27001 for Outstanding Information Security Programs

Organizations wishing to evaluate functional responsibilities in an overall company information security program will find in ISO/IEC 27001 an excellent taxonomy of information security functional areas, particularly for security in a service-oriented environment. Certainly an enterprise may have in-house functions related to security that are not an exact fit, but as an effort to focus on core responsibilities, process flow, and security in a service delivery model, this standard delineates a comprehensive set of responsibilities that can be used to evaluate organizational structure. In a process-oriented firm, aligning a security organization with a “PDCA” approach and the “establish ► implement ► operate ► monitor ► review ► improve” methodology may provide an effective means to ensure that internal clients of the security organization have a clear way to interface with the organization. An additional benefit is that an organization with internal processes that are well-defined and assigned has the opportunity to measure service delivery and improvements in service levels, not only in operational security functions (firewall and VPN management, account services) but also in more “lumpy” services such as security consulting. Given the omnipresent need to account for return on security investment, or activity-based accounting, a process based approach founded on the ISMS described in ISO/IEC 27001 will likely appeal to systems-savvy

organizations that value operational efficiency and superb service delivery and product quality.

Opportunities to improve on the ISO/IEC 27001 foundation

The standard sets expectations for accountability, but leaves the description of roles and responsibilities to the implementing organization. Using terms such as “the organization” as a catch-all for everything from the entity level to the departmental level, champions of ISO 27001 will need to define a structured Responsibility-Accountability-Consult-Inform (RACI) model to accompany implementation of 27001. There should be an articulation of accountability beyond “management” to levels such as “executive”, “manager”, “employee” and “contractor/consultant”. Issues such as segregation of duties, monitoring independence, and third-party validation are also left to the implementer. For organizations experienced in security system structure and implementation, this will not be an obstacle. Implementers should be aware, however, that the standard does not provide a “turn key” definition of an ISMS and that successful execution will require additional levels of planning, perhaps with the support of a consulting group, if in-house staff would benefit from supplemental expertise.

As described within the standard, ISO 27001 also leaves implementing organizations to interpret the proper means to:

- Assess (identify and analyze) risk (ISO/IEC 27001:2005(E) ' 4.2.1.e)
- Set control objectives (' 4.2.1.g) to take into account not only security requirements and risk treatment, but also “legal, regulatory and contractual requirements”
- “Enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected” (' 4.2.3.a.(3))
- “Measure effectiveness of controls to verify that security requirements have been met” (' 4.2.3.c)

Organizations have historically struggled with how to realize these four critical elements of “establish” and “monitor” effectively. The reasons for this are varied, but notably, being accountable for measuring both the control design and effectiveness of

information security is a relatively recently required skill for non-audit professionals, thanks to the Sarbanes-Oxley Act for Financial Accountability of 2002. Security organizations would do well to team closely with internal IT Auditors to ensure that the approach to 27001 implementation provides adequate training to the information security team as well as the IT organization in terms of control design and effectiveness. Organizations who use Six Sigma or other forms of process improvement, such as lean manufacturing, will find that measurement techniques and the DMAIC (Define-Measure-Analyze-Improve-Control) methodology will assist in implementation of 27001. For any organization that wishes to claim conformity to 27001, acceptable fulfillment of these challenging areas (as well as others) is mandatory. This illustrates again that in-house project teams or consulting support for ISO/IEC 27001 will bring needed expertise to the table for facilitation, measurement systems, control design, and control test plans and evaluation.

Conclusion

ISO/IEC 27001 is a viable description of a process-oriented approach to achieve excellent execution of information security practices, assurance that the program is working as intended, and a basis for establishing trust between business partners who share digital assets or network connectivity. In the long term, this standard (along with other information security guidance in FFIEC for financial institutions, NIST 800 for US federal agencies, ISO/IEC 17799:2005, CobiT and ITIL) will enable organizations who desire a competitive advantage for trusted business to claim conformance to an internationally recognized set of well-structured rules to improve process, policy and technology.

Karen Worstell is Co-Founder and Director, Waters Edge Consulting