The Information Security Management System (ISMS)

Summary

NUIT's Information and Systems Security/Compliance (ISS/C) adopted the ISO Standards for Security Management (27001) and Security Practice (27002) for implementation of information security practice at Northwestern University. ISS/C uses a "risk analysis" process, supported by interviews and a survey, to help identify and prioritize business technology issues. Aided by a plan developed by Ronald Gault Consulting LLC, and in response to identified risk, ISS/C selects and implements the applicable ISO policies and standards to help reduce information technology risk.

Background

Late in 2012, NUIT'S Information and Systems Security/Compliance (ISS/C) completed a review of several information security frameworks (e.g., COBIT, ITIL, NIST, etc.) before electing to adopt the International Standards Organization's (ISO) Information Security Management (27001) and Security Practice (27002) Standards.

ISS/C selected ISO 27001/2, based on a persistent theme: the ISO Standards were consistently identified as basic elements of the other frameworks. Further, the ISO Standards appear to map reasonably well to the operations of the University. Though ISO Standards support certification through a rigorous process of implementation, ISS/C's plans do not currently call for ISO certification, as not all ISO Standards are applicable to, or required of, University operations. Rather, ISS/C's approach is to adopt, adapt and apply ISO standards supported by the risk analysis process.

Planning

ISS/C engaged the services of Ronald Gault Consulting LLC to assist in the development of a security plan that complements the implementation activities required of the ISO Standards. The "Information Systems Security Plan/Practices" (ISSP/P) document summarizes the operational framework, provides expeditious access to policy statements, and helps identify and describe procedures for the appropriate use and protection of University data. ISS/C applies updates to the ISSP/P with new and revised policies as they are implemented.

ISO Basics

The ISO Standards provide a model for establishing, implementing, operating, monitoring, reviewing and improving information security practice; the collection of these activities constitute the Information Security Management System (ISMS). The ISMS emphasizes the importance of:

a) understanding an organization's information security requirements and the need to establish policy and objectives for information security;
b) implementing and operating controls to manage an organization's information security risks in the context of the organization's overall business risks;
c) monitoring and reviewing the performance and effectiveness of the implementation; and
d) continual improvement based on objective measurement.

The Information Security Management System (ISMS)

Northwestern’s ISMS is influenced by its business plans, needs and objectives, security and compliance requirements, and existing/anticipated operations; it is designed to be responsive and flexible, and accommodating of the University’s dynamic environment.

Risk Analysis

To achieve the “understanding” emphasized by the ISO Standards, ISS/C uses a “risk analysis” process to identify information technology issues as perceived by the technology leaders of the University’s business units. Central to this process is a survey document titled “Security Questionnaire”; ISS/C collects, evaluates, anonymizes and collates the survey responses. Based on analysis and the application of risk-weighting factors, ISS/C uses the survey results to establish priorities, identify the applicable ISO Standards, and drive the appropriate implementation, monitoring and measurement activities.

Structured Approach - PDCA

The ISO Standards employ a repeatable process titled “Plan-Do-Check-Act”:

- *Plan*: Establish policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall policies and objectives
- *Do*: Implement and operate the ISO Standards policy, controls, processes and procedures.
- *Check*: Assess and, where applicable, measure process performance against policy, objectives and practical experience and report the results to management for review.
- *Act*: Take corrective and preventive actions, based on results of the internal and management reviews or other relevant information, to achieve continual improvement.

Input to this process are information security requirements and expectations established through the risk analysis process and ongoing assessments; output of the process is managed information security.