

Federal Financial Regulators Release New Information Security Booklet

The Federal Financial Institutions Examination Council (FFIEC) recently issued revised guidance for examiners and financial institutions to use in identifying information security risks and evaluating the adequacy of controls and applicable risk management practices of financial institutions. Over the next few months a special series of articles in *Vision Views* will summarize and discuss portions of the new guidelines. The new documentation is available on the Internet through the FFIEC's InfoBase application at:

http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html

Last month we looked at security objectives and regulatory guidance, resources and standards. This month's article will discuss the **Information Security Process** including **Roles and Responsibilities**. The new guidelines state:

Financial institutions should implement an ongoing security process, and assign clear and appropriate roles and responsibilities to the board of directors, management, and employees.

THE SECURITY PROCESS

The security process is the method an organization uses to implement and achieve its security objectives. The process is designed to identify, measure, manage, and control the risks to system and data availability, integrity, and confidentiality, and to ensure accountability for system actions. The process includes five areas that serve as the information security framework:

- ◆ **Information Security Risk Assessment**—A process to identify threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes.
- ◆ **Information Security Strategy**—A plan to mitigate risk that integrates technology, policies, procedures and training. The plan should be reviewed and approved by the board of directors.
- ◆ **Security Controls Implementation**—The acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and assurance that management and staff understand their responsibilities and have the knowledge, skills, and motivation necessary to fulfill their duties.
- ◆ **Security Testing**—The use of various methodologies to gain assurance that risks are appropriately assessed and mitigated. These testing methodologies should verify that significant controls are effective and performing as intended.
- ◆ **Monitoring and Updating**—The process of continuously gathering and analyzing information regarding new threats and vulnerabilities, actual attacks on the institution or others combined with the effectiveness of the existing security controls. This information is used to update the risk assessment, strategy, and controls. Monitoring and updating makes the process continuous instead of a one-time event.

Security risk variables include threats, vulnerabilities, attack techniques, the expected frequency of attacks, financial institution operations and technology, and the financial institution's defensive posture. All of these variables change constantly. Therefore, an institution's management of the risks requires an ongoing process.

ROLES AND RESPONSIBILITIES

Information security is the responsibility of everyone at the institution, as well as the institution's service providers and contractors. The board, management, and employees all have different roles in developing and implementing an effective security process.

The board of directors is responsible for overseeing the development, implementation, and maintenance of the institution's information security program. Oversight requires the board to provide management with guidance and receive reports on the effectiveness of management's response. The board should approve written information security policies and the information security program at least annually. The board should provide management with its expectations and requirements for:

- ◆ Central oversight and coordination,
- ◆ Areas of responsibility,
- ◆ Risk measurement,
- ◆ Monitoring and testing,
- ◆ Reporting, and
- ◆ Acceptable residual risk.

Senior management's attitude towards security affects the entire organization's commitment to security. For example, the failure of a financial institution president to comply with security policies could undermine the entire organization's commitment to security. Management also should consider the roles and responsibilities of external parties. Technology service providers (TSPs), contractors, customers, and others who have access to the institution's systems and data should have their security responsibilities clearly delineated and documented in contracts.

Senior management should designate one or more individuals as information security officers. Security officers should be responsible and accountable for security administration. At a minimum, they should directly manage or oversee risk assessment, development of policies, standards, and procedures, testing, and security reporting processes. Security officers should have the authority to respond to a security event by ordering emergency actions to protect the financial institution and its customers from an imminent loss of information or value. They should have sufficient knowledge, background, and training, as well as an organizational position, to enable them to perform their assigned tasks.

Employees should know, understand, and be held accountable for fulfilling their security responsibilities. Institutions should define these responsibilities in their security policy. Job descriptions or contracts should specify any additional security responsibilities beyond the general policies. Financial institutions can achieve effective employee awareness and understanding through security training, employee certifications of compliance, self-assessments, audits, and monitoring.

Next Month – Risk Assessment Overview and Key Steps

Stephen Tonn is the Managing Partner of Compass Consulting Group, an independent Internal Audit & IT Security Solutions provider. You can reach him at (210) 601-9710 or by email at stonn@thecompassgrp.net.

