

## **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. We have been running a special series of articles in Vision Views that summarize and discuss important portions of the new guidelines. The new documentation is available on the Internet through the FFIEC's InfoBase application at:

[http://www.ffiec.gov/ffiecinfbase/html\\_pages/it\\_01.html](http://www.ffiec.gov/ffiecinfbase/html_pages/it_01.html)

Last month we looked at an overview of **information security risk assessment and discussed the key steps for an effective risk assessment process**. This month's article will provide a list of **Key Risk Assessment Practices**. The new guidelines state:

**Financial institutions must maintain an ongoing information security risk assessment program that effectively**

- **Gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements;**
- **Analyzes the probability and impact associated with the known threats and vulnerabilities to its assets; and**
- **Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and testing necessary for effective mitigation.**

### **Key Risk Assessment Practices**

The new FFIEC information security guidelines state that a risk assessment is the key driver of the information security process. The guidelines also list the following areas as key practices that are directly related to effective performance of information security risk assessment:

- ◆ *Multidisciplinary and Knowledge-based Approach*—A consensus evaluation of the risks and risk mitigation practices followed by the institution requires the involvement of a broad range of users, with a range of expertise and business knowledge. Not all users may have the same opinion of the severity of various attacks, the importance of various controls, and the importance of various data elements and information system components. Management should apply a sufficient level of expertise to the assessment.
- ◆ *Systematic and Central Control*—Defined procedures and central control and coordination help to ensure standardization, consistency, and completeness of risk assessment policies and procedures, as well as coordination in planning and performance. Central control and coordination will also facilitate an organizational view of risks and lessons learned from the risk assessment process.
- ◆ *Integrated Process*—A risk assessment provides a foundation for the remainder of the security process by guiding the selection and implementation of security controls and the timing and nature of testing those controls. Testing results, in turn, provide evidence to the risk assessment process that the controls selected and implemented are achieving their intended purpose. Testing can also validate the basis for accepting risks.
- ◆ *Accountable Activities*—The responsibility for performing risk assessments should reside primarily with members of management in the best position to determine the scope of the assessment, and the effectiveness of risk reduction techniques. For a mid-sized or large

institution, that organization will likely be the business unit. The information security officer(s) are responsible for overseeing the performance of each risk assessment and the integration of the risk assessments into a cohesive whole. Senior management is accountable for abiding by the board of directors' guidance for risk acceptance and mitigation decisions.

- ◆ *Documentation*—Documentation of the risk assessment process and procedures assists in ensuring consistency and completeness, as well as accountability. Documentation of the analysis and results provides a useful starting point for subsequent assessments, potentially reducing the effort required in those assessments. Documentation of risks accepted and risk mitigation decisions are fundamental to achieving accountability for risk decisions.
- ◆ *Enhanced Knowledge*—Risk assessment increases management's knowledge of the institution's mechanisms for storing, processing, and communicating information, as well as the importance of those mechanisms to the achievement of the institution's objectives. Increased knowledge allows management to respond more rapidly to changes in the environment. Those changes can range from new technologies and threats to regulatory requirements.
- ◆ *Regular Updates*—Risk assessments should be updated as new information affecting information security risks are identified (e.g., a new threat, vulnerability, adverse test result, hardware change, software change or configuration change). At least once a year, senior management should review the entire risk assessment to ensure relevant information is appropriately considered.

#### **Next Month – Information Security Testing: Definitions, Concepts and Application**

Stephen Tonn is the Managing Director 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](mailto:stonn@thecompassgrp.net).

