

## **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](http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html)

Last month we looked at the security process and roles and responsibilities for information security. This month's article will provide an overview of **information security risk assessment and will discuss the key steps for an effective risk assessment process**. 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.**

### **OVERVIEW**

The quality of security controls can significantly influence all categories of risk. Traditionally, examiners and bankers recognize the direct impact on operational/transaction risk from incidents related to fraud, theft, or accidental damage. Many security weaknesses, however, can directly increase exposure in other risk areas. For example, the GLBA introduced additional legal/compliance risk due to the potential for regulatory noncompliance in safeguarding customer information. The potential for legal liability related to customer privacy breaches may present additional risk in the future. Effective application access controls can reduce credit and market risk by imposing risk limits on loan officers or traders. If a trader were to exceed the intended trade authority, the institution may unknowingly assume additional market risk exposure.

A strong security program reduces levels of reputation and strategic risk by limiting the institution's vulnerability to intrusion attempts and maintaining customer confidence and trust in the institution. Security concerns can quickly erode customer confidence and potentially decrease the adoption rate and rate of return on investment for strategically important products or services. Examiners and risk managers should incorporate security issues into their risk assessment process for each risk category. Financial institutions should ensure that security risk assessments adequately consider potential risk in all business lines and risk categories.

Information security risk assessment is the process used to identify and understand risks to the confidentiality, integrity, and availability of information and information systems. An adequate assessment identifies the value and sensitivity of information and system components and then balances that knowledge with the exposure from threats and vulnerabilities. A risk assessment is a necessary prerequisite to the formation of strategies that guide the institution as it develops, implements, tests, and maintains its information systems security posture. An initial risk

assessment may involve a significant onetime effort, but the risk assessment process should be an ongoing part of the information security program.

## KEY STEPS

Common elements of risk assessment approaches involve three phases: information gathering, analysis, and prioritizing responses. Vendor concerns add additional elements to the process.

### Information Gathering

Identifying and understanding risk requires the analysis of a wide range of information relevant to the particular institution's risk environment. Once gathered, the information can be catalogued to facilitate later analysis. Information gathering generally includes the following actions:

- ◆ Obtaining listings of information system assets (e.g., data, software, and hardware). Inventories on a device-by-device basis can be helpful in risk assessment as well as risk mitigation. Inventories should consider whether data resides in house or at a technology service provider (TSP).
- ◆ Determining threats to those assets, resulting from people with malicious intent, employees and others who accidentally cause damage, and environmental problems that are outside the control of the organization (e.g., natural disasters, failures of interdependent infrastructures such as power, telecommunications, etc.).
- ◆ Identifying organizational vulnerabilities (e.g., weak senior management support, ineffective training, inadequate expertise or resource allocation, and inadequate policies, standards, or procedures).
- ◆ Identifying technical vulnerabilities (e.g., vulnerabilities in hardware and software, configurations of hosts, networks, workstations, and remote access).
- ◆ Documenting current controls and security processes, including both information technology and physical security.
- ◆ Identifying security requirements and considerations (e.g., GLBA).
- ◆ Maintaining the risk assessment process requires institutions to review and update their risk assessment at least once a year, or more frequently in response to material changes in any of the six actions above.

### Analyze Information

The information gathered is used to characterize the system, to identify and measure threats to the system and the data it contains and transmits, and to estimate the likelihood that a threat will take action against the system or data.

System characterization articulates the understanding of the system, including the boundaries of the system being assessed, the system's hardware and software, and the information that is stored, processed, and transmitted. Since operational systems may have changed since they were last documented, a current review of the system should be performed. Developmental systems, on the other hand, should be analyzed to determine their key security rules and attributes. Those rules and attributes should be documented as part of the systems development lifecycle process. System characterization also requires the cross-referencing of vulnerabilities to current controls to identify those that mitigate specific threats, and to assist in highlighting the control areas that should be improved.

Threats are identified and measured through the creation and analysis of threat scenarios. Threat scenarios should be comprehensive in their scope (e.g., they should consider reasonably foreseeable threats and possible attacks against information and systems that may affect the institution's condition and operations or may cause data disclosures that could result in

substantial harm or inconvenience to customers). They should consider the potential effect and likelihood for failure within the control environment due to non-malicious or malicious events. They should also be coordinated with business continuity planning to include attacks performed when those plans are implemented. Non-malicious scenarios typically involve accidents related to inadequate access controls and natural disasters. Malicious scenarios, either general or specific, typically involve a motivated attacker (i.e., threat) exploiting a vulnerability to gain access to an asset to create an outcome that has an impact.

The risk from any given scenario is a function of the probability of the event occurring and the impact on the institution. The probability and impact are directly influenced by the financial institution's business profile, the effectiveness of the financial institution's controls, and the relative strength of controls when compared to other industry targets.

The probability of an event occurring is reflected in one of two ways. If reliable and timely probability data is available, institutions can use it. Since probability data is often limited, institutions can assign a qualitative probability, such as frequent, occasional, remote, and improbable.

Frequently, technology service providers (TSPs) perform some or all of the institution's information processing and storage. Reliance on a third party for hosting systems or processing does not remove the institution's responsibility for securing the information. It does change how the financial institution will fulfill its role. Accordingly, risk assessments should evaluate the sensitivity of information accessible to or processed by TSPs, the importance of the processing conducted by TSPs, communications between the TSPs' systems and the institution, contractually required controls, and the testing of those controls.

### **Prioritize Responses**

This phase ranks the risk (outcomes and probabilities) presented by various scenarios produced in the analysis phase to prioritize management's response. Management may decide that since some risks do not meet the threshold set in their security requirement, they will accept those risks and not proceed with a mitigation strategy. Other risks may require immediate corrective action. Still others may require mitigation, either fully or partially, over time. Risks that warrant action are addressed in the information security strategy. In some borderline instances, or if planned controls cannot fully mitigate the risk, management may need to review the risk assessment and risk ranking with the board of directors or a delegated committee. The board should then document its acceptance of the risk or authorize other risk mitigation measures.

### **Next Month – Key Risk Assessment Practices**

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).

