

Stephen Tonn, Managing Partner
Compass Consulting Group

Federal Financial Regulators Release New Information Security Booklet

Earlier this year, the Federal Financial Institutions Examination Council (FFIEC) 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/ffiecinfobase/html_pages/it_01.html

Last month we provided a list of key risk assessment practices. This month's article provides definitions and concepts related to information security testing. The new guidelines state:

Financial institutions should gain assurance of the adequacy of their risk mitigation strategy and implementation by

- ***Basing their testing plan, test selection, and test frequency on the risk posed by potentially non-functioning controls;***
- ***Establishing controls to mitigate the risks posed to systems from testing; and***
- ***Using test results to evaluate whether security objectives are met.***

Testing Definitions

Information security is an integrated process that reduces information security risks to acceptable levels. The entire process, including testing, is driven by an assessment of risks. The greater the risk, the greater the need for the assurance and validation provided by effective information security testing.

In general, risk increases with system accessibility and the sensitivity of data and processes. For example, a high-risk system is one that is remotely accessible and allows direct access to funds, fund transfer mechanisms, or sensitive customer data. Information-only Web sites that are not connected to any internal institution system or transaction-capable service are lower-risk systems. Information systems that exhibit high risks should be subject to more frequent and rigorous testing than low-risk systems. Because tests only measure the security posture at a point in time, frequent testing provides increased assurance that the processes that are in place to maintain security over time are functioning.

A wide range of tests exists. Some address only discrete controls, such as password strength. Others address only technical configuration, or may consist of audits against standards. Some tests are overt studies to locate vulnerabilities. Other tests can be designed to mimic the actions of attackers. In many situations, management may decide to perform a range of tests to give a complete picture of the effectiveness of the institution's security processes. Management is responsible for selecting and designing tests so that the test results, in total, support conclusions about whether the security control objectives are being met.

Testing Concepts and Application

Testing Risks to Data Integrity, Confidentiality, and Availability - Management is responsible for carefully controlling information security tests to limit the risks to data integrity, confidentiality, and system availability. Because testing may uncover nonpublic customer information, appropriate safeguards to protect the information must be in place. Contracts with third parties to provide testing services should require that the third parties implement appropriate measures to meet the objectives of section 501(b) of the GLBA. Management also is responsible for ensuring that employee and contract personnel who perform the tests or have access to the test results have passed appropriate background checks, and that contract personnel are appropriately bonded. Because certain tests may pose more risk to system availability than other tests, management is responsible for considering whether to require the personnel performing those tests to maintain logs of their testing actions. Those logs can be helpful should the systems react in an unexpected manner.

Confidentiality of Test Plans and Data - Since knowledge of test planning and results may facilitate a security breach, institutions should carefully limit the distribution of their testing information. Management is responsible for clearly identifying the individuals responsible for protecting the data and providing guidance for that protection, while making the results available in a useable form to those who are responsible for following up on the tests. Management also should consider requiring contractors to sign nondisclosure agreements and to return to the institution information they obtained in their testing.

Measurement and Interpretation of Test Results - Institutions should design tests to produce results that are logical and objective. Results that are reduced to metrics are potentially more precise and less subject to confusion, as well as being more readily tracked over time. The interpretation and significance of test results are most useful when tied to threat scenarios.

Tractability - Test results that indicate an unacceptable risk in an institution's security should be traceable to actions subsequently taken to reduce the risk to an acceptable level.

Thoroughness - Institutions should perform tests sufficient to provide a high degree of assurance that their security plan, strategy and implementation is effective in meeting the security objectives. Institutions should design their test program to draw conclusions about the operation of all critical controls. The scope of testing should encompass all systems in the institution's production environment and contingency plans and those systems within the institution that provide access to the production environment.

Frequency - Test frequency should be based on the risk that critical controls are no longer functioning. Factors to consider include the nature, extent, and results of prior tests, the value and sensitivity of data and systems, and changes to systems, policies and procedures, personnel, and contractors. For example, network vulnerability scanning on high-risk systems can occur at least as frequently as significant changes are made to the network.

Next Month – Information Security Testing: Independent Diagnostic Tests, Key Factors and Outsourced Systems

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.

