

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. Over the past few months, 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 discussed definitions and concepts related to information security testing. This month's article continues the discussion of information security testing and provides details on types of testing, key factors of independent testing, and testing needed for outsourced systems. 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.***

Types of Testing

Independent diagnostic tests include penetration tests, audits, and assessments. Independence provides credibility to the test results. To be considered independent, testing personnel should not be responsible for the design, installation, maintenance, and operation of the tested system, as well as the policies and procedures that guide its operation. The reports generated from the tests should be prepared by individuals who also are independent of the design, installation, maintenance, and operation of the tested system.

Penetration tests, audits, and assessments can use the same set of tools in their methodologies. The nature of the tests, however, is decidedly different. Additionally, the definitions of penetration test and assessment, in particular, are not universally held and have changed over time.

Penetration Tests - A penetration test subjects a system to the real-world attacks selected and conducted by the testing personnel. The benefit of a penetration test is to identify the extent to which a system can be compromised before the attack is identified and assess the response mechanism's effectiveness. Penetration tests generally are not a comprehensive test of the system's security and should be combined with other independent diagnostic tests to validate the effectiveness of the security process.

Audits - Auditing compares current practices against a set of standards. Industry groups or institution management may create those standards. Institution management is responsible for demonstrating that the standards they adopt are appropriate for their institution.

Assessments - An assessment is a study to locate security vulnerabilities and identify corrective actions. An assessment differs from an audit by not having a set of standards

to test against. It differs from a penetration test by providing the tester with full access to the systems being tested. Assessments may be focused on the security process or the information system. They may also focus on different aspects of the information system, such as one or more hosts or networks.

Key Factors

Management is responsible for considering the following key factors in developing and implementing independent diagnostic tests:

Personnel - Technical testing is frequently only as good as the personnel performing and supervising the test. Management is responsible for reviewing the qualifications of the testing personnel to satisfy themselves that the capabilities of the testing personnel are adequate to support the test objectives.

Scope - The tests and methods utilized should be sufficient to validate the effectiveness of the security process in identifying and appropriately controlling security risks.

Notifications - Management is responsible for considering whom to inform within the institution about the timing and nature of the tests. The need for protection of institution systems and the potential for disruptive false alarms must be balanced against the need to test personnel reactions to unexpected activities.

Controls Over Testing - Certain testing can adversely affect data integrity, confidentiality, and availability. Management is expected to limit those risks by appropriately crafting test protocols. Examples of issues to address include the specific systems to be tested, threats to be simulated, testing times, the extent of security compromise allowed, situations in which testing will be suspended, and the logging of test activity. Management is responsible for exercising oversight commensurate with the risk posed by the testing.

Frequency - The frequency of testing should be determined by the institution's risk assessment. High-risk systems should be subject to an independent diagnostic test at least once a year. Additionally, firewall policies and other policies addressing access control between the financial institution's network and other networks should be audited and verified at least quarterly. Factors that may increase the frequency of testing include the extent of changes to network configuration, significant changes in potential attacker profiles and techniques, and the results of other testing.

Proxy Testing - Independent diagnostic testing of a proxy system is generally not effective in validating the effectiveness of a security process. Proxy testing, by its nature, does not test the operational system's policies and procedures, or its integration with other systems. It also does not test the reaction of personnel to unusual events. Proxy testing may be the best choice, however, when management is unable to test the operational system without creating excessive risk.

Outsourced Systems

Management is responsible for ensuring institution and customer data is protected, even when that data is transmitted, processed, or stored by a service provider. Service providers should have appropriate security testing based on the risk to their organization, their customer institutions, and the institution's customers. Accordingly, management and auditors evaluating technology service providers (TSPs) should use the above testing guidance in performing initial due diligence, constructing contracts, and exercising ongoing oversight or audit responsibilities. Where indicated by the institution's risk assessment, management is responsible for monitoring the testing performed at the service provider through review of timely audits and test results or other equivalent evaluations.

Next Month - This is our final article in the Information Security Focus series. We would like to thank Precision Computer Systems for providing us with the opportunity to summarize and discuss information security regulatory requirements, and we sincerely hope that you have found the articles informative and helpful. Reprints of any or all of the articles may be obtained by contacting Compass Consulting Group.

Two new FFIEC booklets have been published since the Information Security Booklet was released – Business Continuity Planning (BCP) and Supervision of Technology Service Providers (TSP). Our next series of articles will provide highlights and discussion of key points from the BCP Booklet.

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.

