

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 *Information Security Booklet* is the first in a series of updates to the 1996 FFIEC Information Systems Examination Handbook. These updates will address significant changes in technology that have occurred since 1996, and will incorporate a risk-based examination approach. 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

Inside the new guidelines you will find descriptions of how institutions should protect and secure the systems and facilities used to process and maintain information. The booklet calls for financial institutions and technology service providers to maintain effective security programs, tailored to the complexity of their operations. For example...

Security Objectives

Information security enables a financial institution to meet its business objectives by implementing business systems with due consideration of information technology-related risks to the organization, business and trading partners, technology service providers, and customers. Organizations meet this goal by striving to accomplish the following objectives:

- *Availability*—The ongoing availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information and/or systems.
- *Integrity of Data or Systems*—System and data integrity relate to the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.
- *Confidentiality of Data or Systems*—Confidentiality covers the processes, policies, and controls employed to protect information of customers and the institution against unauthorized access or use.
- *Accountability*—Clear accountability involves the processes, policies, and controls necessary to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, intrusion detection, recovery, and legal admissibility of records.
- *Assurance*—Assurance addresses the processes, policies, and controls used to develop confidence that technical and operational security measures work as intended.

Assurance levels are part of the system design and include availability, integrity, confidentiality, and accountability. Assurance highlights the notion that secure systems provide the intended functionality while preventing undesired actions.

Regulatory Guidance, Resources and Standards

Financial institutions developing or reviewing their information security controls, policies, procedures, or processes have a variety of sources to draw upon. First, federal laws and regulations address security, and regulators have issued numerous security related guidance documents. Institutions also have a number of third-party or security industry resources to draw upon for guidance, including outside auditors, consulting firms, insurance companies, and information security professional organizations. In addition, many national and international standard-setting organizations are working to define information security standards and best practices for electronic commerce. While no formal industry accepted security standards exist, these various standards provide benchmarks that both financial institutions and their regulators can draw upon for the development of industry expectations and security practices.

Next Month – presentation of the **Information Security Process** including **Roles and Responsibilities**.

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.

