Office of Audits

OIG

Federal Deposit Insurance Corporation

Why We Did The Audit

The FDIC Office of Inspector General (OIG) contracted with KPMG, LLP (KPMG) to conduct an independent evaluation of the FDIC's information security program and practices pursuant to the Federal Information Security Management Act of 2002 (FISMA). FISMA requires federal agencies, including the FDIC, to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluation to the Office of Management and Budget.

The objective of the evaluation was to determine the effectiveness of the FDIC's information security program and practices, including the FDIC's compliance with FISMA and related information security policies, procedures, standards and guidelines.

Background

Key to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system is safeguarding the sensitive information it collects and manages in its roles as federal deposit insurer of banks and savings associations and as receiver for failed institutions. Ensuring the integrity, availability, and confidentiality of this information in an environment of increasingly sophisticated security threats requires a strong, enterprise-wide information security program.

Report No. AUD-08-020 **September 2008**

Independent Evaluation of the FDIC's Information Security Program-2008

Audit Results

In general, with respect to the information technology systems and common controls reviewed, KPMG found that the related program and operational controls demonstrated effectiveness while management and technical controls warranted management attention. The FDIC continues to build upon its past success in addressing the information security provisions of FISMA and standards and guidelines of the National Institute of Standards and Technology. Importantly, the FDIC had established policies and procedures in substantially all of the security control areas KPMG evaluated. The FDIC had also implemented a number of important security control improvements in response to KPMG's 2007 evaluation, such as enhancing its encryption capabilities and strengthening its corporate privacy program. Additional control improvements were also underway at the close of the audit.

The above accomplishments were positive. However, KPMG identified a number of information security control deficiencies warranting management attention. Of particular note, KPMG identified access control deficiencies within the FDIC's internal network that presented a high risk of unauthorized disclosure of sensitive information or compromise of IT resources. While the FDIC was taking prompt action to address these access control deficiencies, increased management attention in this area is warranted. The table below presents KPMG's security program assessment results. The report identifies eight steps that the Corporation can take to improve the effectiveness of its information security program controls in the areas of *Risk Assessment; Planning; Certification, Accreditation, and Security Assessments; Media Protection; Awareness and Training; Identification and Authentication; Access Control;* and *Audit and Accountability*. In many cases, the FDIC was already working to improve security controls in these areas during KPMG's audit.

Because this report addresses issues associated with information security, we do not intend to make public release of the specific contents of the report.

KPMG's Assessment of the FDIC's Security Program Controls

Control Class	Control Families Tested that Demonstrated Effectiveness	Control Families Tested that Warrant Management Attention
Program	• Information Security Governance • Enterprise Architecture	
Management		• Risk Assessment • Planning • Certification, Accreditation, and Security Assessments
Operational	• Maintenance • System and Information Integrity • Incident Response • Awareness and Training	• Media Protection
Technical		• Identification and Authentication • Access Control • Audit and Accountability

Source: KPMG's 2008 audit of the FDIC's information security program. KPMG did not evaluate the following control families: System & Services Acquisition, Contingency Planning, Configuration Management, System and Communication Protection, Personnel Security, and Physical and Environmental Protection.