Office of Inspector General

Executive Summary

Independent Evaluation of the FDIC's Information Security Program—2010

Report No. AUD-11-001
November 2010

Why We Did The Audit

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies, including the FDIC, to have an annual independent evaluation by agency Inspectors General of their information security program and practices and to report the results of the evaluation to the Office of Management and Budget (OMB). The FDIC Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to perform an audit to fulfill the requirements for the 2010 independent evaluation. The objective of the audit was to evaluate 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. KPMG reviewed a sample of information systems, including three designated by the FDIC as major applications.

We will separately issue our responses to specific questions raised by OMB in its April 21, 2010 memorandum, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* through the OMB automated collection tool. Our responses to the OMB questions, together with this report, satisfy our 2010 FISMA reporting requirements.

Background

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

FISMA directs the National Institute of Standards and Technology (NIST) to develop information security standards and guidelines. NIST has published Federal Information Processing Standards and Special Publications to fulfill this requirement. The NIST documentation includes risk management guidelines that provide a flexible framework for ensuring the adequacy and effectiveness of information security controls over information resources that support federal operations and assets. The standards and guidelines published by NIST are not legally binding on the FDIC, but the FDIC's policy is to voluntarily comply with those standards.

Audit Results

KPMG concluded that the FDIC information security program had a risk management framework that generally meets FISMA requirements and NIST security guidance. KPMG also concluded that the effectiveness of certain internal control activities within five of the seven phases of the risk management framework needed improvement.

KPMG determined that internal controls related to the phases *Creating and Maintaining an Inventory* and *Selecting Security Requirements* complied with the risk management framework described in NIST standards and guidance, was consistent with FISMA, and demonstrated effectiveness. However, KPMG also determined that certain internal controls in the phases *Categorizing Information Systems*, *Implementing Security Controls*, *Assessing Security Controls*, *Authorizing Information Systems*, and *Monitoring Security Controls* needed improvement. Importantly, the FDIC needed to improve its

processes for categorizing information systems that input, store, process, or output information assigned a high-potential-impact level by the FDIC; addressing common security controls that are relied upon by multiple systems; ensuring the timeliness and support for system authorization decisions; and continuously monitoring security controls.

KPMG also evaluated whether the FDIC had completed corrective actions in response to the security deficiencies identified during the 2009 FISMA performance audit. KPMG concluded that while the FDIC had completed corrective action on 12 of 18 prior-year issues, 6 prior-year issues required additional action. Of particular note, the FDIC had not implemented an enterprise-wide approach for reviewing audit logs of the FDIC's inventory of information systems. A similar deficiency was also reported during the previous two annual FISMA audits.

Recommendations and Management Comments

The FDIC can strengthen its information security program by implementing KPMG's 12 recommendations that address internal control deficiencies identified in the 5 risk management phases. On November 5, 2010, the Chief Information Officer (CIO) and Director, Division of Information Technology, provided a written response to a draft of this report. The CIO generally agreed with KPMG's recommendations or provided alternative actions that meet the intent of the recommendations. Therefore, all of the recommendations are resolved but remain open until corrective actions are completed and determined to be responsive. In response to the recommendations, the CIO stated that planned actions include issuing guidance on processes for categorizing information and systems, implementing an approach for addressing common security control requirements, and completing and implementing a tactical plan for the FDIC's continuous monitoring of security requirements.