Office of Inspector General

Executive Summary

Information Technology Security Controls over FDIC*connect*

Report No. AUD-10-002
December 2009

Why We Did The Audit

The FDIC Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct an audit of FDIC*connect*.

The objective of the performance audit was to assess the FDIC's information technology (IT) security controls over FDIC*connect* that are designed to ensure the confidentiality, integrity, and availability of the system. Specifically, the audit assessed selected IT security controls pertaining to the core functionality and selected business transactions of FDIC*connect*.

Background

FDIC*connect* is a Web-based application that allows FDIC-insured financial institutions to conduct business and exchange sensitive information (including privacy data) with the FDIC, other federal regulatory agencies, and state banking departments. FDIC*connect* is one of the most widely used Web-based applications at the FDIC.

KPMG used security standards and guidelines issued by the National Institute of Standards and Technology (NIST) as its principal criteria in performing the audit.

Audit Results

KPMG found that the FDIC had established and implemented a number of important information security controls over FDIC*connect* that are designed to ensure the confidentiality, integrity, and availability of the system. Such controls include written information security policies and procedures in substantially all of the areas that KPMG reviewed; key planning documents, such as an application security plan, contingency plan, and configuration management plan; and strong network perimeter security controls that include firewalls, an intrusion detection system, and monthly scanning of FDIC*connect* servers to detect missing security patches and other security vulnerabilities. Further, the Division of Information Technology (DIT) had certified and accredited FDIC*connect* using a methodology consistent with NIST security standards and guidelines.

The above accomplishments are notable. However, KPMG identified several security control deficiencies warranting management attention. Specifically, DIT needed to strengthen its configuration management controls for FDIC*connect* by ensuring that source code in the production computing environment and the FDIC's corporate software repository are consistent and properly documented. DIT also needed to review FDIC*connect* user accounts in the Microsoft Windows® Active Directory® and disable or delete accounts that are no longer

needed. Further, DIT needed to update the security plan and contingency plan for FDIC*connect* to address changes in the application's technology and functionality. KPMG's report contains five recommendations to address these security control deficiencies.

KPMG's report includes one additional recommendation intended to improve the FDIC's Risk Management methodology. Specifically, DIT should review and revise (where appropriate) its risk assessment methodology to help ensure that risks associated with electronic transactions involving the Internet are fully considered.

Management's Response

On December 4, 2009, the Director, Division of Information Technology (DIT), provided a written response to the draft report. DIT concurred with the recommendations, and its actions and planned actions are responsive.

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