Office of Audits

Federal Deposit Insurance Corporation

Report No. AUD-09-020 August 2009

Audit of Information Technology Controls in Support of the FDIC Funds' 2008 and 2007 Financial Statements Audit

Why We Did The Audit

The FDIC Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct an audit of the FDIC's Information Technology (IT) controls over key financial systems and data that support financial management and the generation of financial statements for the Deposit Insurance Fund (DIF) and the Federal Savings and Loan Insurance Corporation Resolution Fund (FRF) (hereafter, the Funds). The results of this audit support the Government Accountability Office (GAO) in assessing the effectiveness of the FDIC's internal control over financial reporting for the Funds' 2008 and 2007 financial statements audit.

The objective of the audit was to assess (1) the progress the FDIC has made in mitigating previously reported IT security control deficiencies pertaining to financial systems and information and (2) the effectiveness of the FDIC's controls in protecting the confidentiality, integrity, and availability of its financial systems and information. The scope of KPMG's work was limited to assessing (1) the FDIC's remedial actions pertaining to 15 IT security control deficiencies reported by the GAO during the prior-year financial statements audit of the Funds and (2) selected access and separation of duties controls within the Accounts Payable and General Ledger modules of the PeopleSoft Enterprise Financials Management application (PeopleSoft financials).

Background

The FDIC relies extensively on automated information systems to support the preparation of financial statements for the Funds. The FDIC's principal financial system is the New Financial Environment (NFE), which includes the PeopleSoft financials.

KPMG used the GAO's January 1999 *Federal Information System Controls Audit Manual* methodology to conduct the audit. KPMG also used security standards and guidelines issued by the National Institute of Standards and Technology as its principal criteria.

Audit Results

KPMG found that the FDIC had taken action to mitigate 14 of the 15 previously reported IT security control deficiencies pertaining to the FDIC's financial systems and information. Such actions included updating the FDIC's risk assessment for the NFE, segregating incompatible system-related duties for key individuals supporting the NFE, and performing software configuration audits of the NFE. With respect to the remaining control deficiency concerning maintenance of requirements baselines, the FDIC had not yet fully implemented corrective actions by the close of KPMG's field work. Accordingly, the OIG plans to assess the sufficiency of the FDIC's actions to address this control deficiency in future audit work.

KPMG also found that, with respect to the control areas assessed, the FDIC had established and implemented a number of effective controls that were designed to protect the confidentiality, integrity, and availability of financial systems and information. Of particular note, the FDIC had implemented a major restructuring of the NFE's security controls in July 2008 that included, among other things, limiting user access to system functionality and data consistent with business needs and improving security monitoring controls.

The above actions were positive. However, KPMG identified two security control deficiencies, neither of which the GAO considered to be significant deficiencies in the context of the Funds' 2008 and 2007 financial statements audit. Specifically, KPMG found that sensitive financial information, including personally identifiable information (PII), and program files were not adequately protected from unauthorized disclosure or modification. This deficiency increased the risk of an unauthorized disclosure or compromise of PII, which could have led to identity theft or other consumer fraud. The deficiency also increased the risk that a knowledgeable internal user could have accessed or modified financial program files for unauthorized purposes. KPMG immediately notified the FDIC of this control deficiency and subsequently confirmed that action had been taken to protect the sensitive information and files.

KPMG also found that the FDIC had not followed its software configuration management processes when installing software updates to a key NFE-interfacing application. Specifically, the FDIC installed copies of software updates that had not been subject to proper quality assurance testing and analysis. No system problems appear to have occurred as a result of this control deficiency. In addition, FDIC officials described various compensating controls that would help to reduce the risk associated with this deficiency. However, the deviations from the FDIC's configuration management processes presented a risk that errors or unauthorized software modifications could have been introduced into the NFE production computing environment.

Recommendations and Management Response

KPMG made three recommendations to strengthen IT controls by reducing the risk of unauthorized modification or disclosure of sensitive financial information and program files and ensuring that software installed in the production computing environment is subject to proper quality assurance testing and analysis. The FDIC concurred with the recommendations, and its actions and planned actions are responsive.

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