Office of Audits

OIG

Federal Deposit Insurance Corporation

Report No. AUD-09-007 **March 2009**

Control Improvements Undertaken by the Division of Information Technology to Ensure the Confidentiality of Sensitive Email Communications

Why We Did The Audit

On October 6, 2008, the Director of the FDIC's Division of Information Technology (DIT) issued a memorandum to the FDIC Chairman (referred to herein as the DIT Memorandum), summarizing the status of control improvements intended to address five specific email security issues. The Director, DIT, requested the FDIC Office of Inspector General (OIG) to assess DIT's actions to address the five issues. The Director, DIT, also separately requested that the OIG assess DIT's efforts to use content filtering technology for corporate email communications. In response to these requests, the OIG contracted with KPMG LLP (KPMG) to audit these areas.

The audit objectives were to (1) determine whether the control improvements described in the DIT Memorandum were adequate, fully implemented, and operating as intended and (2) assess DIT's efforts to leverage content filtering technology on corporate email to mitigate the loss of sensitive business data. As part of the audit, KPMG assessed the status of DIT's ongoing security control improvements and the OIG-recommended control enhancements described in the OIG's August 2008 report, entitled *Controls for Protecting the Confidentiality of Sensitive Email Communications* (OIG Report No. AUD-08-013).

Background

The FDIC uses email extensively to exchange business information internally and externally. The National Institute of Standards and Technology recommends that organizations consider the use of email content filtering technology to mitigate the risk of loss of sensitive business data.

DIT has overall responsibility for providing email service to the Corporation and for maintaining the FDIC's email infrastructure.

Audit Results

As reflected in the table below, the control improvements described in the DIT Memorandum were adequate, fully implemented, and generally operating as intended.

Issues in the DIT Memorandum	Control Improvement is Adequate	Control Improvement is Fully Implemented	Control Improvement is Operating as Intended
Issue #1 – Too many contractors have administrator rights in the email environment.	✓	✓	*
Issue #2 – Monitoring and logging of contractor administrator's access to email accounts need improvement.	✓	✓	✓
Issue #3 – The process for encrypting sensitive email communications can be cumbersome.	✓	✓	✓
Issue #4 – Contractors have administrator rights, which could allow unauthorized access to email communications on desktops, laptops, and the "U:" drive.	✓	✓	✓
Issue #5 – Roles and responsibilities of contractor staff operating the Enterprise Vault need further review.	✓	✓	✓

✓ Completed.
* Although DIT implemented appropriate control improvements to address Issue #1, we were unable to fully assess whether these control improvements operate as intended because they were recently implemented. The OIG may assess whether these control improvements operate as intended as part of its planned security evaluation required by the Federal Information Security Management Act of 2002.

Although KPMG's work identified the need for additional control improvements to fully address the five email security issues contained in the DIT Memorandum, DIT took prompt action to implement these additional control improvements prior to the close of the audit.

DIT completed a pilot implementation of email content filtering technology. However, DIT temporarily discontinued the use of the email content filtering prior to the start of the audit. Based on concerns KPMG raised during the audit, DIT developed a formal policy and configuration management plan to govern email content filtering at the FDIC.

KPMG's report summarizes the status of DIT's ongoing security control improvements and the OIG-recommended control enhancements described in OIG Report No. AUD-08-013.

Recommendation and Management Response

KPMG recommended that the Director, DIT, implement content filtering technology on corporate email to mitigate the risk of loss of sensitive business data consistent with NIST-recommended practices and the FDIC's policies and procedures. Management concurred with our recommendation and plans to take responsive actions, subject to the concurrence of the FDIC Chairman.

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