Office of Audits

Federal Deposit Insurance Corporation

Report No. AUD-08-013 August 2008

Controls for Protecting the Confidentiality of Sensitive Email Communications

Why We Did The Audit

The FDIC Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to audit and report on the FDIC's controls over the confidentiality of sensitive email communications. The results of this audit will support the OIG in fulfilling its evaluation and reporting responsibilities under the Federal Information Security Management Act of 2002.

The objective of the audit was to assess the FDIC's controls for protecting the confidentiality of sensitive email communications and to identify opportunities for mitigating risk where appropriate.

Background

The FDIC uses email extensively, internally and externally, to exchange business information such as open bank data, contract negotiations, personnel data, and legal matters. Protecting the confidentiality of sensitive email communications requires a comprehensive set of security controls and sustained vigilance to address current and emerging security threats.

The FDIC's Division of Information Technology (DIT) has overall responsibility for providing email service to the Corporation and for maintaining the FDIC's email infrastructure. The FDIC's email infrastructure requires administrators (trusted individuals) to perform necessary maintenance. Because of the nature of their duties, administrators have the ability to access the unencrypted email communications of others.

Audit Results

KPMG found that the FDIC had a number of key controls in place to protect the confidentiality of sensitive email communications. Such controls include, for example, a corporate policy governing the encryption of sensitive email communications; an enterprise-wide email encryption solution; background checks and confidentiality agreements for administrators supporting the email infrastructure; and a security awareness and training program addressing, among other things, the protection of sensitive email communications. DIT was also working to implement a number of additional email security control improvements during the audit.

While such actions were positive, controls over administrator access to the email infrastructure needed to be strengthened. In addition, KPMG identified several potential control enhancements intended to further mitigate the risk of email exposure at the FDIC that DIT should assess for implementation.

Recommendations and Management Response

KPMG recommended that the Director, DIT, strengthen controls over administrator access to the email infrastructure and assess potential controls enhancements identified during the audit. The FDIC concurred with both recommendations, and its planned actions are responsive to the recommendations.

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