Office of Audits

Report No. AUD-08-001
October 2007

FDIC's IT Disaster Recovery Capability

Background and Objective of the Audit

The Office of Management and Budget has issued policy requiring federal agencies to establish and periodically test their ability to recover from information technology (IT) service interruptions. In addition, the National Institute of Standards and Technology (NIST) has developed security standards and guidelines to assist agencies in restoring their information systems following a disruption or failure. Further, organizations can consider adopting a number of industry-accepted practices related to IT disaster recovery.

Key to achieving the FDIC's business goals and objectives is having a reliable recovery capability for the Corporation's critical IT systems and applications.

The objective of the audit was to determine whether the FDIC has established and implemented an IT disaster recovery capability consistent with federal standards and guidelines and industry-accepted practices.

Results of Audit

The FDIC has established and implemented an IT disaster recovery capability that is consistent with federal standards and guidelines and industry-accepted practices. Among other things, the FDIC has established an alternate processing site and developed written plans to recover its general support systems and mission-critical applications following a disaster. In April 2007, the FDIC's Division of Information Technology (DIT) conducted a test of its IT disaster recovery capability and successfully recovered its general support systems and mission-critical applications. DIT issued a report on the results of its IT disaster recovery testing, including the issues it identified during the testing and associated solutions, to improve future recovery responsiveness and reliability.

These accomplishments are positive. However, our audit identified the following areas needing enhancements to further assure that information security controls are in place in the event of a disaster.

- The FDIC's corporate contingency planning policy does not reflect the FDIC's current IT disaster recovery practices or recent NIST guidance.
- Security patches were not installed on certain servers in the FDIC's alternative processing site.
- DIT had not documented or tested its strategy for recovering key security services designed to protect the FDIC's alternate processing capability during a disaster.

Our report also identifies opportunities for DIT to enhance its IT disaster recovery performance metrics. We discussed these opportunities with DIT officials during our audit.

Recommendations and Management Response

We recommended that FDIC management (1) update the FDIC's corporate contingency policy; (2) take steps to ensure that security patches are installed on disaster recovery servers in a timely manner; and (3) document and test, as appropriate, DIT's strategy for recovering key security services. In general, management concurred with our recommendations and is taking responsive corrective action.

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