FDIC's IT Security Risk Management Program – Overall Program Policies and Procedures and the Risk Assessment Process

(Report No. 04-028, July 30, 2004)

Summary

This report presents the results of an audit by International Business Machines (IBM) Business Consulting Services (hereafter referred to as IBM), an independent professional services firm engaged by the Office of Inspector General (OIG) to support its efforts to satisfy reporting requirements related to the Federal Information Security Management Act of 2002.

The objective of this audit was to determine whether the FDIC has an adequate information technology (IT) security risk management program. The scope of the audit focused on the adequacy of the FDIC's policies and procedures for the Information Technology Security Risk Management Program and the risk assessment process. IBM concluded that the FDIC had made progress since August 2003 in implementing the program. However, policies and procedures for the overall risk management program and the risk assessment process could be strengthened.

Recommendations

IBM made three recommendations to the Director, Division of Information Resources Management (DIRM), to improve the policies and procedures for managing IT risk.

Management Response

DIRM has agreed to take corrective actions for two recommendations, which are resolved but will remain undispositioned and open for reporting purposes until we have determined that agreed-to corrective actions have been completed and are effective. DIRM did not concur with a part of the third recommendation. Overall, this recommendation is not resolved.

This report addresses issues associated with information security. Accordingly, we have not made, nor do we intend to make, public release of the specific contents of the report.