Office of Inspector General

February 2006
Report No. 06-007

Audit of the FDIC's Security Certification and Accreditation Program

AUDIT REPORT

Office of Audits

OIG

Federal Deposit Insurance Corporation
801 17th Street NW, Washington, DC 20434

Office of Audits
Office of Inspector General

DATE: February 15, 2006

MEMORANDUM TO: Michael E. Bartell, CIO and Director
Division of Information Technology

FROM: Russell A. Rau[Electronically produced version; original signed by Russell A. Rau]
Assistant Inspector General for Audits

SUBJECT: *Audit of the FDIC's Security Certification and Accreditation Program* (Report No. 06-007)

Attached is a copy of the subject report prepared by KPMG LLP under a contract with the Office of Inspector General. Please refer to the Executive Summary for the overall audit results. The firm's report is presented as Part I of this document.

A summary and evaluation of your response, the response in its entirety, and the status of the recommendation are contained in Part II of this report. The response adequately addressed the recommendation in the report. We consider the recommendation to be resolved, but it will remain open until we have determined that agreed-to-corrective actions have been completed and are effective.

If you have any questions concerning the report, please contact Stephen M. Beard, Deputy Assistant Inspector General for Audits, at (202) 416-4217, or Mark Mulholland, Director, Systems Management and Security Audits Directorate, at (202) 416-2944. We appreciate the courtesies extended to the audit staff.

Attachment

cc: James H. Angel, Jr., OERM
Rack Campbell, DIT

Office of Audits

OIG

Background and Purpose of Audit

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to audit and report on the FDIC's security certification and accreditation (C&A) program. The results of this audit support the FDIC OIG in fulfilling its evaluation and reporting responsibilities under the Federal Information Security Management Act (FISMA).

The Office of Management and Budget requires agencies to certify and accredit their information systems consistent with federal security policies, standards, and guidelines. Certification involves the evaluation of an information system's management, operational, and technical security controls. Accreditation involves a senior agency official's authorization of an information system to operate. The certification and accreditation of federal information systems is critical to securing the government's operations and assets.

The audit objective was to determine whether the FDIC's security C&A policies, procedures, and practices were satisfactory and consistent with federal standards and guidelines.

To view the full report, go to www.fdicig.gov/2006reports.asp

Report No. 06-007
February 2006

The FDIC's Security Certification and Accreditation Program

Results of Audit

The FDIC established and implemented C&A policies, procedures, and practices that were satisfactory and consistent with federal standards and guidelines. The FDIC continued to build its C&A program during 2005 in response to evolving National Institute of Standards and Technology guidance, and additional improvements were underway at the close of our field work. Further, the FDIC had undertaken action to address certain C&A-related matters previously identified in the OIG's September 2005 security evaluation report required by FISMA.

The FDIC can further strengthen its C&A program by:

- enhancing system sensitivity assessment guidance to describe how final security categorizations are determined;
- ensuring that application security plans adequately describe how common security controls and general support systems critical to the security of the application are considered in the application's C&A;
- ensuring the cost-benefit of alternative control solutions for reducing or eliminating vulnerabilities;
- enhancing written procedures for defining the nature and scope of testing, managing system-level plans of action and milestones, accepting risks associated with system security weaknesses, and issuing interim systems authorizations; and
- establishing formal milestone reviews at key points in the C&A process to ensure that critical documentation is current, accurate, and complete.

These program enhancements will provide FDIC management with greater assurance that system security risks are effectively managed and that C&A practices are consistently applied throughout the Corporation. We also performed benchmarking with other federal agencies and included the results in this report.

Recommendation

KPMG recommended that the FDIC's Chief Information Officer strengthen the FDIC's C&A policies, procedures, and guidelines by considering and addressing, as appropriate, the issues described in this report. The FDIC's comments were responsive to the recommendation.

Table of Contents

Part I

Report by KPMG LLP

Audit of the FDIC's Security Certification and Accreditation Program

Prepared for the
Federal Deposit Insurance Corporation
Office of Inspector General

Submitted by:
KPMG LLP
Risk and Advisory Services
2001 M. Street, NW
Washington, DC 20036-3389

Audit of the FDIC's Security Certification and Accreditation Program

Prepared by KPMG LLP

Introduction

- OIG contracted with KPMG LLP (KPMG) to audit and report on the FDIC's security certification and accreditation (C&A) program.
- KPMG conducted its work from April through November 2005 in accordance with generally accepted government auditing standards. KPMG performed certain follow-up procedures subsequent to field work to consider recent improvements in the FDIC's C&A program.

Introduction (Cont.)

- Certification involves the evaluation of an information system's management, operational, and technical security controls.
- Accreditation involves a senior agency official's authorization of an information system to operate.
- By accrediting an information system, the senior agency official accepts the risks associated with the system's operation.

Introduction (Cont.)

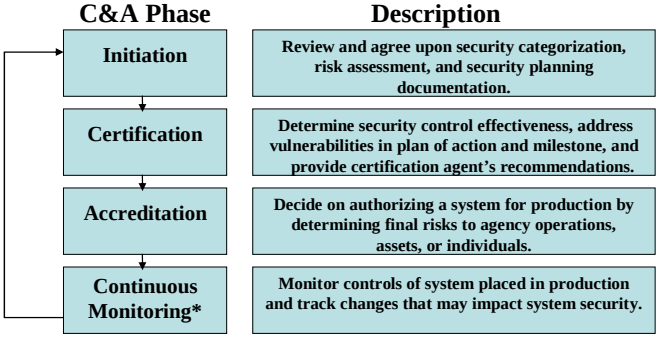
- Agencies are required by Office of Management and Budget (OMB) policy to certify and accredit their information systems consistent with federal standards and guidelines issued by the National Institute of Standards and Technology (NIST).
- In addition, federal Inspectors General are required by OMB policy to assess and report on agency C&A programs as part of their annual independent security evaluations mandated by the Federal Information Security Management Act (FISMA).
- The results of this audit support the OIG in fulfilling its evaluation and reporting responsibilities under FISMA.

Objective, Scope, and Methodology

- The objective was to determine whether the FDIC's C&A policies, procedures, and practices were satisfactory and consistent with federal standards and guidelines.
- The audit focused on the application of the FDIC's C&A program policies, procedures, and guidelines to major applications and general support systems.
- Key criteria included OMB policy and NIST standards and special publications (SP), as identified in Attachment III.

Objective, Scope, and Methodology (Cont.)

NIST SP 800-37 divides the C&A process into 4 phases. The audit results are structured around these 4 phases.



Source: KPMG analysis of NIST SP 800-37.

* KPMG did not fully evaluate the implementation of Continuous Monitoring due to the recent implementation of the applications selected for review. The OIG plans to perform more detailed work in this area in 2006.

Objective, Scope, and Methodology (Cont.)

- Key FDIC C&A policies, procedures, and guidelines reviewed:
  - Circular 1310.3, *Information Technology Security Risk Management Program*
  - Circular 1360.8, *Information Security Categorization*
  - Division of Information Technology (DIT) *Policy and Guidelines on Certification and Accreditation (C&A)*
  - DIT's *Risk Management Methodology*
- C&A packages for three major applications selected for detailed review:
  - New Financial Environment (NFE) Phase I
  - Legal Integrated Management System (LIMS)
  - Asset Servicing Technology Enhancement Project–Metavante

Objective, Scope, and Methodology (Cont.)

- The FDIC OIG surveyed seven federal Inspectors General to obtain certain information regarding their agencies' C&A programs.
- The audit results build upon information we provided to DIT throughout the audit:
  - April 2005 CIO briefing on the NFE Phase I C&A package
  - July 2005 DIT management briefing on the FDIC's C&A policies and procedures
  - September 2005 OIG FISMA report suggested improvements, such as (a) ensuring plans of action and milestones (POA&Ms) reflect all relevant security weaknesses (b) integrating processes for identifying mission-critical applications with processes for determining application availability for Federal Information Processing Standards (FIPS) Publication (PUB)199 purposes and (c) re-evaluating the 180-day duration for interim system authorizations.

Background

- Pursuant to its statutory responsibilities under FISMA, NIST continues to develop risk-based security standards and guidelines for securing federal information systems.
- NIST standards and guidelines are introducing significant changes in how federal agencies, including the FDIC, protect their information and systems.
- The President and OMB continue to place a high priority on fully certifying and accrediting federal information systems.
- The FDIC has focused its C&A efforts to date on major applications and general support systems. The FDIC plans to place priority attention on its sensitive non-major applications in 2006 to ensure that potential security risks associated with these systems are addressed.

Overall Results

- The FDIC's C&A policies, procedures, and practices were satisfactory and consistent with federal standards and guidelines.
- The FDIC continued to build its C&A program throughout 2005 in response to evolving NIST guidance, and additional improvements were underway at the close of our field work.
- The audit identified opportunities for the FDIC to further strengthen its C&A program policies, procedures, and guidelines. Generally, these opportunities existed because the FDIC's C&A program has been evolving in response to emerging NIST requirements and the Corporation's security management needs.
- Addressing the issues in this report will provide FDIC management greater assurance that system security risks are effectively managed and that C&A practices are consistently applied throughout the Corporation.

FDIC C&A Program Accomplishments

- Established and implemented policies, procedures, and/or guidelines to:
  - Classify information systems and data
  - Assess security risks
  - Plan for security
  - Test and evaluate system security controls
  - Develop POA&Ms
  - Ensure that system owners are actively engaged in C&A program activities
  - Standardize accreditation decisions
  - Monitor system security controls

FDIC C&A Program Accomplishments (Cont.)

- Implemented a risk-based approach to certify and accredit the information systems that pose the greatest risk to the FDIC (i.e., major applications and general support systems).
- Achieved process efficiencies by identifying and testing "common" security controls that cross system boundaries, such as personnel and physical security controls.

Initiation Phase - Areas That Can Be Strengthened

- Sensitivity Assessment Questionnaire (SAQ) guidance should be enhanced to:
  - Describe how the initial FIPS PUB 199 categorization (which is based on an analysis of system data sensitivity and categorizes the data into high, moderate, and low impact) can be modified by the responses to SAQ questions in determining an application's final FIPS PUB 199 categorization.
  - Address requirements for documenting management's rationale for maintaining or changing initial FIPS PUB 199 categorizations.

Initiation Phase - Areas That Can Be Strengthened (Cont.)

- Application security plans include a description of the IT environment in which the application operates. However, guidance for preparing application security plans should be enhanced to require that security plans describe how (a) common security controls and (b) system components critical to the security of the application (such as database management and server operating systems) are considered in the application's C&A.
  - Provides greater clarification of system boundaries for C&A purposes and greater assurance that all relevant risks are considered when accrediting applications.
  - Promotes efficiency because many relevant system components are covered in other security plans and common controls are covered in a separate Security Test and Evaluation (ST&E).

Initiation Phase - Areas That Can Be Strengthened (Cont.)

- Procedures for reducing or eliminating vulnerabilities identified from risk assessments should be enhanced to better describe when the cost-benefit of alternative control solutions should be considered. The consideration of cost-benefits could be as simple as a memorandum to the file and may accompany an implementation plan.
- Procedures should be enhanced to establish an independent milestone review before proceeding to the Certification Phase. Such a "check point" would provide additional assurance that system security categorizations, risk assessments, and security plans are current, accurate, and complete.
  - The Certification Agent plays a key role.
  - The level of rigor should be consistent with the FIPS PUB 199 impact.

Certification Phase - Areas That Can Be Strengthened

- Procedures for planning and conducting ST&E should:
  - Define the nature and scope of ST&E test case validations, including requirements for ensuring independence in the process.
  - Include requirements for gathering, reviewing, and reusing (where appropriate) previous assessments, audits, and evaluation results. Such assessments and audit work can also benefit Continuous Monitoring activities.

Certification Phase - Areas That Can Be Strengthened (Cont.)

- Procedures for preparing and managing POA&Ms should be enhanced to define the Certification Agent's role in providing recommendations to system owners to correct security control deficiencies identified during ST&E.
- Procedures for accepting moderate or high risk associated with known security vulnerabilities should be enhanced to ensure that:
  - Relevant federal standards and guidelines are considered in justifying decisions to accept risk.
  - A standard format for accepting risk is used, such as DIT's *Memorandum of Acceptance of Risk*, when circumstances warrant (such as when the risk is high or moderate).

Certification Phase- Areas That Can Be Strengthened (Cont.)

- Procedures should be enhanced to establish an independent milestone review by the Certification Agent before proceeding to the Accreditation Phase. Such a review would provide additional assurance that:
  - System owners fully describe corrective actions taken to close system-level weaknesses on POA&Ms.
  - All security weaknesses are fully addressed in system-level POA&Ms and included in the final certification package.
  - Justifications for accepting moderate or high risk are adequately documented, when circumstances warrant.
- Procedures should be enhanced to require that certification letters identify those security vulnerabilities that must be remediated in order to achieve full accreditation when recommending an Interim Authority to Operate (IATO).

Accreditation Phase - Areas That Can Be Strengthened

- IATO guidance should be enhanced to:
  - Describe how terms and conditions (i.e., limitations on system operations) should be defined and documented.
- As referenced in the Initiation Phase, guidance should be enhanced to better describe how common security controls and system components critical to the security of an application are to be considered and reported in the accreditation letter.

Continuous Monitoring Phase - Areas That Can Be Strengthened

- C&A guidelines should be enhanced to:
  - Describe how security controls will be selected and monitored following an IATO or full authorization to operate.
  - Describe the use of POA&Ms in the status reporting component of Continuous Monitoring.

Conclusion and Recommendation

The FDIC has made significant strides in developing its C&A program in response to emerging NIST requirements. This report identifies opportunities for the FDIC to further strengthen its C&A policies, procedures, and guidelines.

KPMG recommends that the Chief Information Officer strengthen the FDIC's C&A policies, procedures, and guidelines by considering and addressing, as appropriate, the issues described in this report.

Attachment I

Key Observations of IG Survey

We surveyed IGs of seven federal agencies that had a C&A program assessment rating of satisfactory or higher based on their 2004 FISMA evaluation. The results are as follows.

- Most OIGs reported that their agency had categorized all of their major applications and general support systems in accordance with FIPS PUB 199.
- Less than one half of the OIGs reported that their agency had identified "common" security controls. A lesser number of these same agencies had certified and accredited their common security controls.
- Most OIGs reported that their agency's system-level POA&Ms included all relevant IT security weaknesses, including OIG- and GAO-identified weaknesses.

Attachment I

Key Observations of IG Survey (Cont.)

- Some IGs reported that their agencies used the Automated Security Self-Evaluation and Remediation Tracking tool to centrally manage the remediation of security weaknesses.
- Almost all IGs reported that their agencies had certified and accredited their general support systems before certifying and accrediting any overlaying applications. One OIG recommended that the agency identify risks associated with unaccredited general support systems in major application C&A packages.
- Almost all IGs reported that their agencies had developed IATO policies or procedures.
- Some IGs reported that their agencies' C&A programs included a quality assurance component (a GAO-recommended practice).

Attachment II

Prior Audits, Performance Measures, and Fraud

- Relevant reports and correspondence include:
  - September 2005 OIG report entitled, *Independent Evaluation of the FDIC's Information Security* Program-2005 (Report No. 05-040)
  - September 2005 OIG report entitled, *Responses to Security-Related Questions Raised in OMB's Fiscal Year 2005 Reporting Instructions for FISMA and Agency Privacy Management* (Report No. 05-034)
  - OIG Memorandum entitled, *FDIC's Information Security Program*, dated November 8, 2005

Attachment II

Prior Audits, Performance Measures, and Fraud (Cont.)

- KPMG did not evaluate the FDIC's C&A program performance measures as part of the audit. Such procedures were performed as part of the OIG's annual information security evaluation required by FISMA.
- KPMG did not develop specific audit procedures to detect fraud and illegal acts because they were not considered material to the audit objective. However, throughout the audit, KPMG was sensitive to the potential of fraud, waste, abuse, and mismanagement.

Attachment III

Laws, Regulations, Standards, and Guidelines

Key statutes, regulations, standards, and guidelines:

- Federal Information Security Management Act of 2002
- OMB Circular No. A-130, *Management of Federal Information Resources* Appendix III, *Security of Federal Automated Information Resources*
- OMB Memorandum M-02-1, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
- NIST FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*
- NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*

Attachment IV

Acronyms

Acronym	Definition
C&A	Certification and Accreditation
CIO	Chief Information Officer
DIT	Division of Information Technology
FDIC	Federal Deposit Insurance Corporation
FIPS PUB	Federal Information Processing Standard Publication
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
IATO	Interim Authorization to Operate
LIMS	Legal Integrated Management System
NFE	New Financial Environment
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SAQ	Sensitivity Assessment Questionnaire
SP	Special Publication
ST&E	Security Test and Evaluation

Attachment V

Glossary

Term	Definition
Accreditation	Official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.
Accreditation Package	The evidence provided to the authorizing official to be used in the security accreditation decision process. Evidence includes, but is not limited to: (a) the system security plan; (b) the assessment results form the security certification; and (c) the plan of action and milestones.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation); agency assets; or individuals.
Certification Agent	The individual, group, or organization responsible for conducting a security certification.
Certification	Comprehensive assessment of the management, technical, and operational security controls in an information system, made in support of security accreditation to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.
Chief Information Officer	Agency official responsible for: • Providing advice and other assistance to the head of the executive agency and other senior management personnel to ensure that agency information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency. • Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency. • Promoting the effective and efficient design and operations of all major information resources management processes for the agency, including improvements to work processes of the agency.

Glossary (Cont.)

Term	Definition
Common Security Control	Security control that can be applied to one or more agency information systems and has the following properties: (a) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (b) the results from the assessment of the control can be used to support the security C&A processes of any agency information system where that control has been applied.
Federal Information System	An information system used or operated by an executive agency, a contractor of an executive agency, or another organization on behalf of an executive agency.
General Support System	An interconnected set of information resources under the same direct management control. This system normally includes hardware, software, information, data, applications, communications, and people.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information Systems Manager	Individual responsible to the senior agency information security officer, authorizing official, or information systems owner or ensuring the appropriate operational security posture is maintained for an information system or program.
Major Application	An application that requires special attention due to the risk and magnitude of the harm that would result in the loss, misuse, or unauthorized access to or modification of information in the application.

Attachment V

Glossary (Cont.)

Term	Definition
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
NIST	National Institute of Standards and Technology – a government agency charged with establishing guidance for IT security.
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact	Low: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Moderate: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. High: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Risk	The level of impact on agency operations (including mission, functions, image, or reputation); agency assets; or indviudal resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation); agency assets; or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. A risk assessment is part risk management, synonymous with risk analysis, and incorporates threat and vulnerabilty analysis.

Attachment V

Glossary (Cont.)

Term	Definition
Risk Management	The process of managing risks to agency operations (including mission, functions, image, or reputation); agency assets; or individuals resulting form the operation of an information system. IT includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate that system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
Security Category	The characterization of information or an information system based on an assessment of potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organization assets, or individuals.
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.
Sensitive Non-Major Application	An application that processes a lesser degree of sensitive information than a major application but still requires some extra attention to security risks and controls.
System Security Plan	Formal document that provides an overview of the security requirement for the information system and describes the security controls in place or planned for meeting those requirements.
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered.

Part II

Corporation Comments and OIG Evaluation

CORPORATION COMMENTS AND OIG EVALUATION

The report contains one recommendation for the CIO and Director of DIT. The CIO provided a written response to the draft report on February 1, 2006. This response is presented in its entirety on page II-2. DIT management concurred with the recommendation, which we consider resolved, but it will remain open for reporting purposes until we have determined that agreed-to corrective actions have been completed and are effective. DIT's response to the recommendation is summarized below, along with our evaluation of the response.

Recommendation 1: KPMG recommends that the Chief Information Officer strengthen the FDIC's C&A policies, procedures, and guidelines by considering and addressing, as appropriate, the issues described in this report.

DIT Response: DIT concurs with the recommendation. DIT has worked with the OIG audit team to begin assessing the observations made in the draft report. DIT has drafted a matrix that documents DIT's consideration of the observations. DIT reviewed the status of this effort with the OIG and Office of Enterprise Risk Management on January 18, 2006. It was agreed that the provision of the completed matrix would satisfy the recommendation and that the OIG would review DIT's actions regarding these issues in the 2006 Federal Information Security Management Act evaluation. DIT will complete the matrix and provide it to the OIG by April 5, 2006.

OIG Evaluation of Response: DIT's consideration of the observations and resulting matrix satisfies the intent of the recommendation. We consider the recommendation resolved**,** but it will remain open until we have determined that each observation was considered and addressed in the matrix.

CORPORATION COMMENTS

FDIC
Federal Deposit Insurance Corporation
550 17th St. NW Washington DC, 20429
Division of Information Technology

February 1, 2006

MEMORANDUM TO: Stephen M. Beard
Deputy Assistant Inspector General for Audits
Office of Inspector General

FROM: Michael E. Bartell, CIO and Director [Electronically produced version; original signed by Michael E. Bartell]
Division of Information Technology

SUBJECT: Response to the Draft Report Entitled, *Audit of FDIC's Security Certification and Accreditation Program*
(Assignment No. 2005-031)

The Division of Information Technology (DIT) is pleased to provide our comments to the Office of Inspector General's (OIG) draft report dated December 23, 2005, entitled *Audit of FDIC's Security Certification and Accreditation Program*.

Responses to the Recommendations:

1. KPMG recommends that the Chief Information Officer strengthen the FDIC's C&A policies, procedures and guidelines by considering and addressing, as appropriate, the issues described in this report.

Response: Concur

DIT has worked with the OIG audit team to begin assessing the observations made in the draft report. DIT has drafted a matrix that documents DIT's consideration of the observations. DIT reviewed the status of this effort with the OIG and the Office of Enterprise Risk Management on January 18, 2006. It was agreed that the provision of the completed matrix would satisfy the recommendation and that the OIG would review DIT's actions regarding these issues in the 2006 Federal Information Security Management Act evaluation. DIT will complete the matrix and provide it to the OIG by April 5, 2006.

If you have any questions concerning this response, please contact Rack Campbell, Chief, Audit and Internal Control Section on (703) 516-1422.

cc: James Angel, OERM
Ned Goldberg, DIT
Mark Brickman, DIT
Rack Campbell, DIT

MANAGEMENT RESPONSE TO RECOMMENDATION

This table presents the management response on the recommendation in our report and the status of the recommendation as of the date of report issuance.

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	DIT has begun assessing the observations made in the draft report. DIT will provide a matrix that documents DIT's consideration of the observations.	4/5/06	N/A	Yes	Open

[a] Resolved – (1) Management concurs with the recommendation, and the planned corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but planned alternative action is acceptable to the OIG.
(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Once the OIG determines that agreed-to-corrective actions have been completed and are effective, the recommendation can be closed.