# Office of Inspector General

June 15, 2004
Report No. 04-022

## FDIC's Information Technology Examination Program

AUDIT REPORT

## TABLE OF CONTENTS

FDIC
Federal Deposit Insurance Corporation
801 17th St. NW Washington DC. 20434

Office of Audits
Office of Inspector General

**DATE:** June 15, 2004

**MEMORANDUM TO:** Michael J. Zamorski, Director
Division of Supervision and Consumer Protection

[Electronically produced version; original signed by Russell Rau]

**FROM:** Russell A. Rau
Assistant Inspector General for Audits

**SUBJECT:** *FDIC's Information Technology Examination Program*
(Report No. 04-022)

This report presents the results of our audit of the Federal Deposit Insurance Corporation's (FDIC) information technology (IT) examination program. The FDIC is the primary federal regulator for approximately 5,300 state-chartered financial institutions throughout the United States and its territories.[1] These institutions had assets totaling approximately $1.7 trillion and insured deposits totaling more than $942 billion as of December 31, 2003.

The objective of this audit was to determine whether FDIC's IT examinations provide reasonable assurance that IT risks are being addressed by the risk management programs in FDIC-supervised financial institutions. To accomplish our objective, we reviewed the FDIC Division of Supervision and Consumer Protection (DSC) policies and procedures for performing IT examinations, the Federal Financial Institutions Examination Council's (FFIEC)[2] IT handbooks, and IT examinations completed in FDIC's Dallas and New York regions during 2003. We focused our work primarily on institutions having more than $1 billion in assets and generally more complex IT architectures. Appendix I of this report discusses our objective, scope, and methodology in detail. Appendix II contains a table summarizing our results.

[1] This includes a small number of banks in Puerto Rico, Guam, American Samoa, the Federated States of Micronesia, and the Virgin Islands. At the time this report was prepared, there were no FDIC-supervised banks in the District of Columbia.

[2] The FFIEC is a formal interagency body empowered (1) to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the FDIC, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision and (2) to make recommendations to promote uniformity in the supervision of financial institutions.

## BACKGROUND

According to the FDIC, no area of banking has changed as significantly during the past 10 years as the IT area.[3] Insured institutions increasingly have made banking services and data available to customers through automated teller machines and transactional World Wide Web sites. The complexity of maintaining a secure IT environment undoubtedly will increase as banks continue to enhance technological capabilities and delivery channels. Also, attacks on IT systems are increasing, and new vulnerabilities such as denial of service attacks[4] are reported daily, which actually or could cause substantial financial losses. Other risks include (1) threats to security; (2) loss of availability, integrity, and confidentiality of information; and (3) regulatory compliance with laws and regulations.

The FDIC's primary concern about the financial industry's use of IT is the potential risk of loss to deposit insurance funds from high-cost bank failures if risks are not adequately managed and controlled. The FDIC principally addresses its concern by participating in government-wide initiatives, issuing guidance, and conducting IT examinations.

### FDIC's Participation in Government-Wide Critical Infrastructure Protection Initiatives

FDIC has actively participated in government-wide efforts aimed at protecting the nation's cyber-based and physical infrastructures and key resources. The *December 17, 2003 Homeland Security Presidential Directive* (Hspd-7) on Critical Infrastructure Identification, Prioritization, and Protection established a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attacks. Recognizing that each infrastructure sector possesses its own unique characteristics and operating models, Hspd-7 designated the U.S. Department of the Treasury as the Sector-Specific Agency for banking and finance.

The U.S. Department of the Treasury, Assistant Secretary for Financial Institutions, chairs the committee designated as the primary coordinating body for critical infrastructure initiatives relating to the financial services industry and chairs the Financial and Banking Information Infrastructure Committee (FBIIC). The FBIIC's responsibilities include identifying the U.S. financial system's critical infrastructure assets, their locations, and potential vulnerabilities; prioritizing their importance; and assisting primary regulatory agencies in addressing vulnerabilities. The FBIIC is charged with coordinating federal and state financial regulatory efforts to improve the reliability and security of the U.S. financial system. The FDIC participates in FBIIC efforts to evaluate and protect the critical infrastructure of the U.S. banking and financial services industry and to assess the vulnerabilities and risks facing the industry.

---

[3] *FDIC Outlook*, fall 2003 edition, Chicago Regional Perspectives, "Improved Security Is Vital as Information Technology Grows More Complex," p.17. The *FDIC Outlook* is published quarterly by the FDIC's Division of Insurance and Research as an information resource on banking and economic issues for insured financial institutions and financial institution regulators.

[4] Denial of service attacks flood a computer network with data in order to deny access to legitimate users.

## FDIC Guidance to Institutions

The FDIC distributes a majority of its guidance to bankers through Financial Institution Letters (FIL). The FILs generally announce new regulations and policies, new FDIC publications, and a variety of other matters of principal interest to bank management. In some cases, the FILs explain specific examination procedures to be performed by FDIC IT examiners. For example, FIL-118-2002, *Information Technology Examination Procedures*, dated October 9, 2002, and effective November 1, 2002, announced new FDIC IT examination procedures for assessing information technology risk. The FDIC has also issued several FILs covering areas such as e-banking, IT audits, electronic fund transfers, business continuity planning, technology service providers, and risk management.

## FDIC IT Examinations and Related Policies and Procedures

Under section 10(d) of the Federal Deposit Insurance Act (FDI Act), all FDIC-insured institutions are required to undergo on-site safety and soundness examinations by a federal regulator[5] every 12 or 18 months[6] depending on asset size and CAMELS[7] ratings. Safety and soundness examinations are the primary means to identify weaknesses that may ultimately lead to institution failure. Although not required under the FDI Act, the FDIC also conducts IT examinations designed to assess an institution's IT risks. The FDIC normally conducts IT examinations concurrently with safety and soundness examinations.

### *FFIEC's Uniform Rating System for Information Technology*

The FFIEC's Task Force on Supervision has adopted the Uniform Rating System for Information Technology (URSIT).[8] The URSIT is an internal rating system used by federal and state regulators for assessing the safety and soundness of information technology in financial institutions and by service providers that furnish these services to financial institutions.

URSIT ratings consist of a composite rating and four component ratings based on a risk evaluation of four critical components: Audit, Management, Development and Acquisition, and Support and Delivery. The ratings are based on a scale of 1 through 5 in ascending order of supervisory concern with 1 representing the highest rating and least degree of concern, and 5 representing the lowest rating and highest degree of concern. The URSIT is explained in more detail in Appendix III.

---

[5] The four federal regulators are the FDIC, Federal Reserve Board, Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

[6] The FDI Act requires all FDIC-insured institutions to be examined on a 12-month cycle. The Act allows the examination cycle to be extended to 18 months for institutions with assets of $250 million or less if other factors are met – primarily that the institution is CAMELS rated 1 or 2 (see footnote 7), well managed, and well capitalized.

[7] CAMELS (**C**apital, **A**sset Quality, **M**anagement, **E**arnings, **L**iquidity, and **S**ensitivity to Market Risk are the rating factors used by federal regulators in examining the safety and soundness of FDIC-insured institutions. A rating of 1 through 5 is given, with 1 having the least regulatory concern and 5 having the greatest concern.

[8] The FFIEC recommended that the federal supervisory agencies implement the URSIT no later than April 1, 1999.

The primary purpose of the rating system is to identify those entities whose condition or performance of IT functions require special supervisory attention. This rating system assists examiners in making an assessment of risk and compiling examination findings. However, the rating system does not drive the scope of an examination. Examiners should use the rating system to help evaluate the entity's overall risk exposure and risk management performance and to determine the degree of supervisory attention believed necessary to ensure that weaknesses are addressed and that risk is properly managed.

### *FFIEC Examination Procedures*

In 1996, the FFIEC issued its *Information Systems (IS) Examination Handbook*, an interagency guide to assist regulatory examiners in examining information systems operations in financial institutions and independent service bureaus. The handbook contains an overview of information systems concepts, practices, examples of sound IS controls, and FFIEC examination work programs. The handbook also covers regulatory policies of FFIEC member agencies for use in the examination of information systems. The handbook is currently being updated and renamed the *FFIEC Information Technology (IT) Examination Handbook* and is being reissued in a series of booklets that either introduce new topics or replace chapters of the 1996 handbook. The first booklet on information security was issued January 29, 2003. Eventually, the 1996 handbook will be retired.

### *FDIC's Risk-Focused IT Examination Procedures*

On November 1, 2002, the FDIC launched a new program for assessing IT risk at FDIC-supervised financial institutions. The program incorporated a new philosophy for categorizing institutions' use of technology and exposure to technology risk and use of updated and more risk-focused IT examination procedures. The FDIC developed two new work programs to accomplish this:

- The IT-MERIT (Maximum Efficiency, Risk-focused, Institution Targeted) Procedures work program contains examination procedures used by examiners conducting technology risk reviews at FDIC-supervised financial institutions with the least technology risk.

- The IT General Work Program is used by examiners conducting technology risk reviews at FDIC-supervised financial institutions with low to moderate technology risk. The IT General Work Program consolidated several previously issued, technology-related work programs into a single work program and eliminated redundant review areas to improve examiner efficiency.

Examiners use the existing FFIEC work programs for all financial institutions with greater technology risk and for institutions with complex or sophisticated technology systems.

FDIC's new risk-focused approach to IT examinations begins with classifying the IT risk at financial institutions into one of four new IT examination categories. Table 1 shows the required work programs and IT examination report treatments for each category. The new categories describe an institution's technology risk profile to address the different levels of risk posed by financial institutions through their use of IT. These new technology profile categories are applied to financial institutions through a standard methodology called the Technology Profile Script. Details on the Technology Profile Script and scoring matrix and definitions of category types are in Appendix IV.

**Table 1: Required Work Program and IT Examination Report Treatment for Each Technology Profile Category**

| Technology Profile Matrix Score Range | Technology Profile Category | Required Work Program | Report Treatment Based on Technology Profile Category and URSIT Rating |
|---|---|---|---|
| 0-49 | Type I | IT-MERIT Procedures | Composite URSIT rating reported as part of the bank's safety and soundness report. |
| 0-49 | Type II | IT General Work Program | ▪ If composite URSIT rating is 1 or 2: only the composite rating is reported as part of the safety and soundness report.<br>▪ If composite or any component is 3, 4, or 5 rated: composite and all four component ratings are reported in a separate IT report of examination. |
| 50-79 | Type III | IT General Work Program supplemented by FFIEC work programs | |
| 80-130 | Type IV | FFIEC work programs | Composite and all four component ratings are reported in a separate IT report of examination. |

Source: FDIC Regional Directors Memorandum 2002-043 and FDIC Financial Institution Letter FIL-12-99.

The Technology Profile category and total assets of all FDIC-supervised institutions as of December 31, 2003 are shown in the following tables.

**Table 2: Technology Profile Category of FDIC-Supervised Banks, December 31, 2003**

| Region | Type I | Type II | Type III | Type IV | Total Banks |
|---|---|---|---|---|---|
| Atlanta | 370 | 60 | 236 | 22 | 688 (13%) |
| Chicago | 482 | 305 | 343 | 25 | 1,155 (22%) |
| Dallas (includes Memphis) | 319 | 155 | 482 | 61 | 1,017 (19%) |
| Kansas City | 668 | 174 | 534 | 37 | 1,413 (26%) |
| New York (includes Boston) | 98 | 128 | 366 | 41 | 633 (12%) |
| San Francisco | 198 | 26 | 162 | 31 | 417 ( 8%) |
| **Total** | **2,135** | **848** | **2,123** | **217** | **5,323** |
| **Percentage of Institutions** | **40%** | **16%** | **40%** | **4%** | **100%** |

Source: FDIC Division of Supervision and Consumer Protection, Information Systems Section.

**Table 3: Total Assets* of FDIC-Supervised Banks by Type, December 31, 2003**

| Region | Type I | Type II | Type III | Type IV | Total Assets |
|---|---|---|---|---|---|
| Atlanta | $ 76,730 | $ 5,977 | $ 55,909 | $ 93,241 | $ 231,857 (14%) |
| Chicago | 46,000 | 38,421 | 81,975 | 16,539 | 182,935 (11%) |
| Dallas (includes Memphis) | 28,961 | 12,228 | 81,198 | 54,492 | 176,879 (11%) |
| Kansas City | 35,688 | 8,893 | 69,717 | 14,300 | 128,598 ( 8%) |
| New York (includes Boston) | 38,285 | 62,577 | 279,952 | 239,595 | 620,409 (37%) |
| San Francisco | 32,210 | 1,644 | 113,215 | 175,492 | 322,561 (19%) |
| **Total** | **$257,874** | **$129,740** | **$681,966** | **$593,659** | **$1,663,239** |
| **Percentage of Total Assets** | **15%** | **8%** | **41%** | **36%** | **100%** |

Source: FDIC Division of Supervision and Consumer Protection, Information Systems Section.
*Dollars in millions.

## FDIC IT Examiner Workforce and Training

The FDIC uses specially trained IT examiners to conduct IT examinations. In 1997, the FDIC developed two programs to address IT: the Information Systems On-the-Job Training (IS-OJT) Program and the Electronic Bank Subject Matter Experts (E-banking SMEs) Program. Examiners completing the IS-OJT program become part of a cadre of IT examiners available to participate in IT examinations of large, complex data centers as well as perform other IS-related assignments. Examiners completing the E-banking SME program are responsible for examining technical aspects of e-banking activities of financial institutions that permit transactions over public networks. The examiners also conduct examinations of non-bank service providers that develop and support e-banking applications.

In December 2003, the IS-OJT program was revised to address increasingly complex networks, Internet connectivity, and emerging electronic banking activities such as Internet banking and electronic cash systems and was renamed the Information Technology On-the-Job Training (IT-OJT) Program. The IT-OJT program is tiered to focus training on the graduated skill sets needed to examine Type III and Type IV entities as well as other complex entities.

## RESULTS OF AUDIT

FDIC's IT examination program provides reasonable assurance that IT risks are being addressed by risk management programs in FDIC-supervised financial institutions. The program requires risk-focused IT examinations, which seek to identify and gain an understanding of the inherent risks present at each institution, evaluate the effectiveness of the bank's risk management and internal control structures, and recommend improvements. FDIC IT examiners focused their examination procedures on how well an institution manages and controls its high to moderate IT risks, with less attention focused on how well an institution manages and controls low IT risks. Consistent with the FDIC's goals to reduce the overall burden on the financial institution through the use of risk-focused examinations, not all control areas at the institution may be reviewed. Nevertheless, the examination procedures adequately cover those controls needed for institutions to implement an effective information security program.

We did identify opportunities for improving the quality of the IT examination process based on our review of 21 IT examinations of banks with complex or sophisticated technology systems. Specifically, the FDIC does not have a review process in place to determine whether appropriate examination procedures are applied and that findings and conclusions are adequately supported. Although the FDIC has a quality review process in place for its safety and soundness examinations, the FDIC has generally not conducted similar quality reviews for IT examinations. The FDIC can improve the quality, efficiency, and effectiveness of its IT examinations by instituting a standardized quality review of all phases of the IT examination process and supporting documentation prior to issuance of IT examination results.

## QUALITY REVIEW PROCESS COULD IMPROVE INFORMATION TECHNOLOGY EXAMINATIONS

Our review of IT examinations in 21 judgmentally selected institutions with complex or sophisticated technology systems found that more effective supervisory oversight would improve the quality of IT examinations. The sample consisted of 10 Type IV and 11 Type III financial institutions as shown in Appendix II.

Twelve of the IT examinations we reviewed were conducted in accordance with FDIC policies and procedures, and the corresponding reports of examination on each bank's information technology risk management program were adequately supported. Certain aspects of the remaining nine IT examinations, however, were not conducted in accordance with policy and procedures as discussed below:

- **Incorrect Type of Examination Performed:** For three institutions requiring Type IV examinations, examiners performed less thorough Type III examinations. FDIC's Technology Profile Script prepared by examiners prescribed a Type IV examination using more thorough FFIEC work programs for these three banks. However, examiners used FDIC's IT General Work Program, which provides for a more streamlined but less thorough examination.

- **Outdated Work Programs Used:** Five examinations were conducted using rescinded information security-related sections of 1996 FFIEC work programs instead of the December 2002 FFIEC Information Security work program. The changes had been implemented by the FDIC in January 2003, and all five examinations were conducted after that date.

- **Insufficient Support Provided:** Three IT reports of examination were not adequately supported. For one examination, most of the work program used to document IT security work was blank, indicating that the work was not performed. For another examination, only one page of the work program was retained in the examination work paper files. Examiners also used an incorrect work program for this examination as discussed above. Finally, for the remaining examination, the work program for physical and data security was missing from the work paper files. Examiners also used an outdated work program for this examination, as discussed above.

In addition, we noted that examination work papers that were not always properly labeled and signed or initialed by the preparer.

These conditions were primarily due to a lack of management oversight during the planning and field work phase of the IT examinations and a lack of supervisory review of the supporting IT work papers. Because IT examiners have broad discretion and must exercise considerable judgment in planning, conducting, and drawing conclusions about an institution's IT risk management program, periodic supervisory reviews during all phases of IT examinations by regional office IT specialists would be beneficial. Also, periodic quality assurance reviews would ensure that IT examiners apply appropriate IT examination procedures, consistently exercise sound judgment, obtain sufficient information to identify weaknesses in an institution's risk management program, and adequately document and support examination findings and conclusions.

**Type of Examination Performed**

In three Type IV institutions with extensive core processing, networking, and e-banking systems,[9] examiners performed Type III examinations which were less thorough examinations. Although the Technology Profile Script completed by examiners categorized all three institutions as Type IV institutions requiring Type IV examinations using FFIEC work programs, in each case, examiners performed Type III examinations using the FDIC's IT General Work Program.

According to FDIC's Regional Directors Memorandum (RD Memorandum) 2002-043, dated September 30, 2002, examiners are required to use FFIEC work programs for all Type IV institutions. Examiners scored all three institutions in the Technology Profile Scripts as Type IV

[9] Core processing includes loan, deposit, trust, or general ledger applications. Networking may be broadly defined as workstations, branches, servers, or other communications devices. Most institutions have some networking capabilities. E-banking includes both informational and transactional Web sites. Other examples include maintaining or developing internal systems with bank programming staff and providing data processing or Internet services for others.

institutions. Each bank scored 80 or more, resulting in a Type IV profile requiring IT examiners to use FFIEC IT examination procedures.

- In the case of one institution with $1.1 billion in assets, examiners indicated in the Pre-Examination Planning Memorandum that a Type III review would be conducted using the FDIC IT General Work Program. Performing a Type III review conflicts with guidelines in the Technology Profile Script. Examiners did not document on the Technology Profile Script the reason why a Type IV examination would not be performed.

- For two other Type IV banks, IT examiners also performed Type III examinations using the FDIC IT General Work Program. For one bank with $3.1 billion in assets, examiners noted in the pre-planning memorandum that, "The full FFIEC IS [information security Type IV] work program will be used since the Bank services others for ACH [automated clearing house]." Nevertheless, examiners used the FDIC IT General Work Program in conducting the examination. For the other bank with $1.4 billion in assets, no qualitative adjustments were recorded on the Technology Profile Script, and no pre-planning memorandum was in the examination files to support using the IT General Work Program rather than FFIEC work program.

According to RD Memorandum 2002-043, a Field Supervisor or Senior Examiner may make qualitative adjustments to the Technology Profile Script score to address significant risks not included in the scoring model. The scoring matrix has a column for documenting such qualitative adjustments. Qualitative adjustment factors may include all questions in the Script that were not directly scored as well as other areas not included in the Technology Profile Script. Once the Technology Profile Type is determined, additional risk characteristics, such as asset size, prior IT examination ratings, and prior examination scope should be considered before the final determination is made on the type of examination to be performed. While it is not clear from the RD Memorandum whether scores may be adjusted downward, for these three banks no adjustments were recorded in the Technology Profile Scripts to reduce the scores below 80.

**Work Programs Used**

For five Type IV institutions that had extensive core processing, networking, and e-banking systems, IT examiners used rescinded 1996 security-related work programs instead of the required 2002 security-related work programs implemented in January 2003. Examiners thought the 2002 Information Security Booklet was not yet finalized and that they had the discretion to use 1996 work programs. According to the Technology Profile Scripts, each of the five institutions scored 85 or more, resulting in a Type IV profile, and each IT examination began after March 30, 2003. For one of the five institutions, IT examiners used the security-related sections of the 1996 FFIEC Community Financial Institution IS Examination Workprogram[10] to review the bank's information security. For the remaining four banks, examiners used the

[10] The 1996 FFIEC Community Financial Institution IS Examination Workprogram is applicable to small institutions using vendor supplied and supported software. Use of this program is predicated on the fact that there are no on-site systems and programming activity being performed by either bank staff or private consultants.

security-related sections of the 1996 *FFIEC Information Systems Examination Handbook* work programs to review the banks' information security.

On January 31, 2003, the Associate Director of DSC's Technology Supervision Branch sent an e-mail to the Assistant Regional Directors (ARD) responsible for IT examinations that the FFIEC had issued new guidance and examination procedures regarding information security. Specifically, the e-mail discussed the FFIEC's new *Information Security Booklet*, the first in a series of booklets comprising the new *FFIEC Information Technology Examination Handbook*. The Associate Director pointed out that the December 2002 booklet updates and rescinds the security-related guidance in the 1996 *FFIEC Information Systems Examination Handbook*, including chapters 12 through 14. The e-mail stated that the remainder of the 1996 handbook was still in effect and that examiners should use the work programs in the booklet in place of those in the 1996 handbook for all examinations, beginning immediately.

The FDIC advised examiners and the financial institutions it regulates of the issuance of the new FFIEC guidance on information security through FIL-11-2003, *New Information Security Guidance for Examiners and Financial Institutions*, dated February 12, 2003. The FIL states that on January 29, 2003, the FFIEC issued revised guidance for examiners and financial institutions to use in identifying information security risks and evaluating the adequacy of controls and applicable risk-management practices of financial institutions. The FIL stated that the *Information Security Booklet* is the first in a series of updates to the 1996 *FFIEC Information Systems Examination Handbook* and that the updates will address significant changes in technology since 1996 and incorporate a risk-based examination approach.

In four Type IV institutions, the IT examiners used work programs from the 1996 handbook instead of using the new 2002 examination procedures to assess the adequacy of information security. Total assets at these banks ranged from $1.5 billion to $14.1 billion. In addition, for a fifth examination, an IT examiner used the security-related section of the 1996 FFIEC Community Financial Institution IS Examination Workprogram to review the information security program at the bank. That workprogram included some questions in the new FDIC IT General Work Program, which is prescribed for Type II and III institutions. The institution had assets of about $4.8 billion and used extensive core processing, networking, and other critical systems.

FDIC regional management advised us that it had addressed continued use of the 1996 FFIEC work programs by a few IT examiners. In summary, FDIC management stated that although errors in the process occurred, no substantive areas of the banks' IT systems were omitted from review through the use of the 1996 work programs. According to FDIC, the security assessments did not lack in scope or depth, and the pertinent security risks were appropriately identified.

We disagree with the position that Type IV examinations conducted using 1996 FFIEC work programs for IT security-related work resulted in a complete review of the banks' information security programs. According to the FFIEC, the new *Information Security Booklet* contains more than four times the information in the security section of the 1996 *Information Security*

*Examination Handbook*; therefore, there is a potential to miss areas of significant supervisory concern. For example, new or significantly increased information applies to the following areas:

- Logical and Administrative Access Control
- Physical Security
- Encryption
- Malicious Code
- Systems Development, Acquisition, and Maintenance
- Software Development and Acquisition
- Host and User Equipment Acquisition and Maintenance
- Personnel Security
- Electronic and Paper-based Media Handling
- Logging and Data Collection
- Service Provider Oversight
- Intrusion Detection and Response
- Business Continuity Considerations
- Insurance

Many of the procedures used to review these areas are intended to be performed during in-depth reviews of IT security rather than during the basic risk analysis. Consequently, review of the areas listed above was not performed in five of the seven Type IV banks in our sample that had Type IV examinations. The areas were considered by examiners to be outside the scope of the basic risk analyses performed for the five banks. Only one Type IV examination in the Dallas Region and one in the New York Region used the in-depth verification procedures to review IT security. The expanded examination steps are also referred to as Tier 2 procedures. For the remaining five examinations, examiners performed procedures designed to provide an overview of risk and risk management processes, referred to as Tier 1 procedures. We found that there are no criteria or standards to prompt examiners to perform Tier 2 in-depth review procedures.

**Evidence to Support the Report of Examination**

Three IT reports of examination were not sufficiently supported because documentation of examiners' reviews was either incomplete or missing. In addition, examiners who prepared many of the work papers did not date, initial, or sign them or show the name of the institution and its location.

According to RD Memorandum 2001-039, *Guidelines for Examination Work Papers and Discretionary Use of Examination Documentation Modules,* dated September 25, 2001, the preparation of examination work papers is an important part of documenting the examination process and supporting examination conclusions. All work papers should be labeled with the institution's name and location and should be dated and signed or initialed by the examiner who prepared the document. Examination findings should be documented through a combination of brief summaries, bank source documents, report comments, and other examination work papers that address both management practices and condition. Examination documentation should demonstrate a clear trail of decisions and supporting logic. Documentation should identify examination and verification procedures performed and conclusions reached and should support

the assertions of fact or opinion in the financial schedules and narrative comments in the reports of examination. Examiners should prepare a "Summary Statement," which includes at a minimum:

- a summation of the documentation relied upon during the review;
- the procedures used and analyses conducted to support conclusions relative to the assigned CAMELS components, Bank Secrecy Act[11] examination findings, and other significant areas of review; and
- material discussions with management.

***IT General Work Program***

For one institution with assets valued at $2.6 billion, the IT General Work Program was generally blank, and exceptions noted in the report of examination were not always supported or detailed in either the work program or other examiner work papers. Although the work papers contained numerous internal audit reports, internal bank meeting minutes, and bank policies and procedures, there was no evidence of review (margin notes, highlighting, etc.) of any of these items. Most of the questions in the IT General Work Program were not completed. For example, all eight work program questions were answered in the institution's *Audits* section. However, for the *Management* section, only half of the 18 questions were answered; for the *Development and Acquisition* section, none of the 4 questions were answered; and for the *Support and Delivery* section, only 8 of 37 questions were answered. Overall, 25 (37 percent) of 67 work program questions were answered. The examiner appeared to have relied heavily on the institution's contracted internal auditor's reports, risk scoping procedures, and review of the questionnaire completed by bank personnel.

Based on our review of the IT General Work Program and documentation contained in the field office IT work papers, we found two areas where the IT examiner(s) did not sufficiently document their review of the IT area or support their IT exceptions:

- The embedded IT examination report contained the exception: "The scope of the internal audit is adequate but the frequency of audits is not adequate." Our review of the examination work papers and work program revealed no write-ups or examiner analysis of the frequency of the bank's internal audit program. Instead, a notation on the work program discussed the bank's outsourcing of the internal audit function. There was no indication in the work papers or work program of how the examiner determined that the frequency was not adequate.

[11] The Bank Secrecy Act of 1970, Public Law 91-508, codified to 31 U.S.C. Section 5311 et seq., requires financial institutions to maintain appropriate records and to file certain reports that are used in criminal, tax, or regulatory investigations or proceedings. Congress enacted the BSA to prevent banks and other financial service providers from being used as intermediaries for, or to hide the transfer or deposit of, money derived from criminal activity.

- The report also contained the exception: "There is no independent third party review of disaster recovery testing." Our review of the examination work papers and work program indicated that the examiner noted "5 backup servers" and that the "[Bank] uses a contractor for offsite storage of daily backups of four of the five servers." The work program and work papers contained no write-ups, notations, or analysis to support criticism of an independent third party review of disaster recovery testing.

In response to our inquiries about the reason the examiner performed only 37 percent of the IT General Work Program and relied more upon the work of others, the responsible Field Supervisor intends to institute an IT work paper review program at the field office level to prevent future discrepancies of this type.

***IT Examination Work Papers***

Work papers were missing for two institutions. For one institution with $1.1 billion in assets, most of the IT General Work Program was missing from the work papers. Only one page containing three questions from different sections of the work program was included in the examination workpapers.

Regional management told us that the Examiner-in-Charge (EIC) had experienced computer problems during the completion of the examination that resulted in the loss of all data, including the examination report. This ultimately resulted in the EIC having to reconstruct the report. Electronic work paper data files were also lost. Although the IT General Work Program was missing except for the one page, the other work papers were extensive, including summaries, write-ups, and documents gathered and reviewed. A memorandum, dated May 9, 2003, was prepared for the regional office Report and Correspondence files by a regional office IT specialist, explaining the delayed processing of the report and lost electronic work papers due to the computer problems.

In response to our inquiries about the missing IT General Work Program and computerized work paper failure, the responsible Field Supervisor intended to institute an IT work paper review program as discussed earlier.

For one institution with $12 billion in assets, the physical and data security work program used to support the assessment and evaluation of the institution's information security was missing. Specifically, the examiners used the 1996 FFIEC work programs in their examination, and within those work papers, reference was made to the use of the 1996 FFIEC *Security -- Physical and Data Workprogram* and associated work papers. However, these work papers were not among the regional and field office work papers provided. Other work programs included documentation of risk scoping and work performed, including review of documents and completed FFIEC work programs for each area reviewed. In response to our inquiries about the missing work papers, a Regional IT Specialist made inquiries to determine the whereabouts of the work papers but did not locate them.

The errors found in our sample could have been prevented by management oversight during the planning and field work phases of the IT examination and supervisory review of supporting work

papers. Because IT examiners have broad discretion and must exercise considerable judgment in planning, conducting, and drawing conclusions about an institution's IT risk management program, periodic reviews by regional office IT specialists during all phases of IT examinations would help to improve the quality of IT examinations.

**Recommendation**

We recommend that the Director, DSC, institute a quality review process for all phases of IT examinations including planning, field work, supporting documentation, and reporting, to ensure that IT examiners:

- consistently exercise sound judgment;
- apply the appropriate IT examination procedures;
- expand examination procedures when warranted;
- perform and document adequate work to support IT examination findings, conclusions, and ratings; and
- initial or sign and date the work papers and label them with the institution's name and location.

## CORPORATION COMMENTS AND OIG EVALUATION

On June 4, 2004, the DSC Director provided a written response to the draft report. The response is presented in its entirety in Appendix V to this report. DSC generally concurred with the report's findings and agreed that the IT review process could be enhanced. DSC provided an action plan in its response to the OIG recommendation that will enhance its quality review process for the regional and field offices.

**Field Office: Review of Pre-Examination Planning Memorandum**

To ensure that examiners are performing the correct type of IT examination and using the correct IT work program, DSC will assess and revise as necessary the instructions for the IT pre-examination planning (PEP) memoranda, or in the case of embedded examinations, the safety and soundness PEP, to include the following items: type of examination planned, Technology Profile Script score, and the intended work program to be used. The PEP will reconcile any difference between the type of examination and the Technology Profile Script score. Thus, the PEP will provide a vehicle for supervisory personnel to review and approve major IT examination decisions. The PEP will serve as a quality control measure at the beginning of the IT examination process. DSC will assess, revise, and issue, as necessary the instructions for the appropriate PEP memoranda by December 31, 2004.

**Regional Office: Review of IT Examination Work**

Currently, DSC's regional offices have field office audit procedures that are administered by regional office staff to verify that work programs are properly completed and findings are adequately supported and documented. These programs commonly include reviews of IT

examination work papers and generally address the five items that we recommended be addressed in the quality review procedures.

To help strengthen this program, the DSC is standardizing a field office review program to ensure examination program conformance with FDIC policies and to apply the appropriate emphasis on areas reviewed. The standardized field office review program will incorporate the items we suggested be addressed. The review program will also include periodic sampling of IT examination work papers and a review of examination processing that will provide a quality control measure at the completion of the IT examination process. DSC will implement enhancements by March 31, 2005.

DSC's response to the draft report meets the intent of the recommendation. Accordingly, the recommendation is resolved but will remain undispositioned and open until we have determined that the agreed-to corrective actions have been implemented and are effective.

## OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine whether DSC's examinations provide reasonable assurance that IT risks are being addressed by the risk management programs in FDIC-supervised financial institutions. The audit field work was performed at DSC regional offices in Dallas, Texas, and New York, New York. We performed our audit from October 2003 through April 2004 and in accordance with generally accepted government auditing standards. We focused our work primarily on IT examinations in banks with complex or sophisticated technology systems and more than $1 billion in assets. To accomplish the audit objective, we did the following.

- Reviewed four IT examination files – one of each technology profile category type – from FDIC's Chicago region to determine the general content and organization of the files.
- Reviewed a copy of DSC's Information Technology Risk Monitoring Interim Database (ITRMID), a system for collecting technology risk profiles for each FDIC-supervised financial institution and technology service provider.
- Interviewed officials at DSC's Washington, D.C., headquarters office and the Chicago, Dallas, and New York regional offices.
- Obtained and reviewed a sample of 21 IT examinations performed in the Dallas and New York regions, including reports of examination and supporting documentation.
- Obtained and reviewed various bank examination data from FDIC's Virtual Supervisory Information On the Net (ViSION) system.
- Reviewed DSC RD Memoranda, FILs, and operating manuals and policies pertaining to the safety and soundness and IT examination processes.
- Obtained and reviewed FFIEC guidelines and work programs relating to IT examinations.

### Reliance on Computer-Generated Data

We relied on some computer-generated data pertaining to reports of examination from the Interagency Examination Repository, bank information from ViSION, and IT examination data from the ITRMID. We performed limited tests to determine the reliability of the data and found no reason to expand testing.

### Management Controls

Our review of the management controls for the examinations we sampled identified several control weaknesses that are discussed in the finding section of this report.

## Prior Audit Coverage

The U.S. General Accounting Office (GAO), issued *Electronic Banking: Enhancing Federal Oversight of Internet Banking Activities*, GAO/GGD-99-91, on July 6, 1999. The GAO found that some regulators had been more proactive than others in examining Internet banking. GAO also found that the FDIC had completed the most examinations of on-line banking operations at that time and that the Office of Thrift Supervision and the FDIC had been actively issuing policies and procedures for Internet banking examinations. However, GAO concluded that too few examinations had been conducted at that time to identify the extent of industry-wide Internet banking-related problems.

## Laws and Regulations

Appendix C of the FFIEC's December 2002 *Information Security Booklet* identifies laws and regulations issued by federal banking regulatory agencies that are currently applicable to IT security. These include the following:

- **Laws**
  - 12 U.S.C. 1867(c): Bank Service Company Act
  - 12 U.S.C. 1882: Bank Protection Act
  - 15 U.S.C. 6801 and 6805(b): Gramm–Leach–Bliley Act
  - 18 U.S.C. 1030: Fraud and Related Activity in Connection with Computers
- **FDIC Regulations**

  Title 12 of the Code of Federal Regulations (12 C.F.R.), *Banks and Banking*

  - 12 C.F.R. Part 326, Subpart A: Minimum Security Procedures
  - 12 C.F.R. Part 326, Subpart B: Procedures for Monitoring Bank Secrecy Act Compliance
  - 12 C.F.R. Part 332, Privacy of Consumer Financial Information
  - 12 C.F.R. Part 353, Suspicious Activity Reports
  - 12 C.F.R. Part 364, Appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness
  - 12 C.F.R. Part 364, Appendix B: Interagency Guidelines Establishing Standards for Safeguarding Customer Information

We did not test for compliance with these laws and regulations as they were beyond the scope of this audit.

## Government Performance and Results Act

We reviewed DSC's performance measures under the Government Performance and Results Act (GPRA), Public Law 103-62. We determined that the FDIC did not have a corporate performance objective specifically related to the IT examinations. However, according to the FDIC's *2003 Annual Performance Plan*, and as shown in Table 4, the FDIC established the following strategic goal, objective, and annual performance goal that include a review of information technology as part of the FDIC's overall assessment of risk management and safety and soundness. The means and strategies the FDIC uses to achieve this strategic goal include information technology examinations in general.

**Table 4: Performance Measures Related to Supervision and Examination**

| Strategic Goal | Strategic Objective | Annual Performance Goal | Means and Strategies |
|---|---|---|---|
| FDIC-supervised institutions are safe and sound. | FDIC-supervised institutions appropriately manage risk. | Conduct on-site safety and soundness examinations to assess an FDIC-supervised insured depository institution's overall financial condition, management practices and policies, and compliance with applicable regulations. | Both on-site safety and soundness and IT examinations cover technology-related activities to determine how each FDIC-supervised insured depository institution manages risk in that area. |

Source: The FDIC's *2003 Annual Performance Plan.*

## Fraud and Illegal Acts

The limited nature of the audit objective did not require that we assess the possibility for fraud and illegal acts. However, throughout the audit we were alert to the possibility of fraud and illegal acts, and no instances came to our attention.

## SUMMARY TABLE OF RESULTS

| Bank | Assets (billions) | TPS* Score/ Type | Exam Type/ Tier** | Date of Exam | Exam Hours | No Audit Exception | Incorrect Program | Outdated Program | Lacking Support |
|---|---|---|---|---|---|---|---|---|---|
| **A** | $ 9.9 | 75/III | IV/1 | 01.13.03 | 227 | ✓ - **a** | | | |
| **B** | 5.5 | 65/III | III | 02.10.03 | 90 | ✓ | | | |
| **C** | 0.1 | 50/III | III | 06.09.03 | 127 | ✓ | | | |
| **D** | 10.8 | 75/III | III | 06.09.03 | 70 | ✓ | | | |
| **E** | 0.8 | 65/III | III | 06.16.03 | 263 | ✓ | | | |
| **F** | 6.2 | 65/III | III/2 | 06.16.03 | 111 | ✓ | | | |
| **G** | 3.0 | 55/III | III | 08.04.03 | 173 | ✓ | | | |
| **H** | 7.1 | 70/III | III | 08.04.03 | 69 | ✓ | | | |
| **I** | 0.1 | 50/III | III/2 | 08.04.03 | 68 | ✓ | | | |
| **J** | 8.9 | 50/III | III | 11.10.03 | 196 | ✓ | | | |
| **K** | 19.8 | 105/IV | IV/2 | 04.16.03 | 260 | ✓ - **b** | | | |
| **L** | 3.1 | 85/IV | IV/2 | 07.28.03 | 378 | ✓ - **b** | | | |
| **M** | 2.6 | 65/III | III | 07.14.03 | 256 | | | | ✓ - **f** |
| **N** | 1.1 | 80/IV | III | 02.18.03 | 412 | | ✓ - **c** | | ✓ - **g** |
| **O** | 3.1 | 100/IV | III | 09.29.03 | 238 | | ✓ - **c** | | |
| **P** | 1.4 | 85/IV | III | 10.27.03 | 135 | | ✓ - **c** | | |
| **Q** | 12.0 | 95/IV | IV/1 | 03.31.03 | 200 | | | ✓ - **d** | ✓ - **h** |
| **R** | 14.1 | 100/IV | IV/1 | 04.07.03 | 168 | | | ✓ - **d** | |
| **S** | 4.0 | 85/IV | IV/1 | 08.11.03 | 128 | | | ✓ - **d** | |
| **T** | 1.5 | 90/IV | IV/1 | 10.20.03 | 140 | | | ✓ - **d** | |
| **U** | 4.8 | 85/IV | IV/1 | 11.03.03 | 85 | | | ✓ - **e** | |
| **Total** | **$ 119.9** | | | | | **12** | **3** | **5** | **3** |

Source: OIG analysis of 21 sampled IT examinations of FDIC-supervised banks.

***** – Technology Profile Script, discussed in Appendix IV.

****** – Tier 1 examination procedures are an overview of risk and risk management processes, while Tier 2 procedures are more in-depth verification procedures.

**Notes**

**a** – Examination was started before the new December 2002 FFIEC Information Security work program was implemented. Examiners used 1996 FFIEC Information Systems work programs.

**b** – Examiners used the new December 2002 FFIEC Information Security work program.

**c** – Examiners performed less thorough Type III examinations rather than the required Type IV examinations.

**d** – Examiners used outdated 1996 FFIEC Information Systems work programs rather than the required 2002 FFIEC Information Security work program.

**e** – Examiner used the FFIEC Community Financial Institution Examination Networking and Data Security Workprogram (Section 5) instead of the new 2002 FFIEC Information Security work program.

**f** – Most (63 percent) questions and work steps in the IT General Work Program either were not answered or were not completed.

**g** – Only one page of IT General Work Program was in the examination work paper files.

**h** – Missing Physical and Data Security work program. Reference is made to it within other work programs.

## UNIFORM RATING SYSTEM FOR INFORMATION TECHNOLOGY

The Uniform Rating System for Information Technology (URSIT) is based on a risk evaluation of four critical components: Audit, Management, Development and Acquisition, and Support and Delivery. These components are used to assess the overall performance of IT within an organization. Examiners evaluate the functions identified within each component to assess the institution's ability to identify, measure, monitor, and control information technology risks. Each examined organization is assigned a summary or composite rating based on the overall results of the evaluation. The IT composite rating and each component rating are based on a scale of 1 through 5 in ascending order of supervisory concern with 1 representing the highest rating and least degree of concern and 5 representing the lowest rating and highest degree of concern. These components address the following:

- **Audit** – This rating should reflect the adequacy of the organization's overall IT audit program, including the internal and external auditor's abilities to detect and report significant risks to management and the board of directors on a timely basis. The rating should also reflect the internal and external auditor's capability to promote a safe, sound, and effective operation.

- **Management** – This rating should reflect the board's and management's ability as it applies to all aspects of IT operations, that is, to all aspects of IT acquisition, development, and operations.

- **Development and Acquisition** – This rating reflects an organization's ability to identify, acquire, install, and maintain appropriate IT solutions and the adequacy of the institution's systems development methodology and related risk management practices for acquisition and deployment of information technology. The rating also reflects the board's and management's ability to enhance and replace IT prudently in a controlled environment.

- **Support and Delivery** – This rating reflects an organization's ability to provide technology services in a secure environment. The rating reflects not only the condition of IT operations but also factors such as reliability, security, and integrity, which may affect the quality of the information delivery system.

Institutions receive URSIT ratings in accordance with the following guidelines:

- Financial institutions exposed to a very low level of technology risk (those for which IT-MERIT examination procedures were used) are assigned only a composite URSIT rating in a safety and soundness report of examination.

- Financial institutions exposed to low to moderate technology risk that receive a 1 or 2 URSIT composite rating at current IT examinations will be assigned only a composite URSIT rating in a safety and soundness report of examination.

- Financial institutions exposed to low to moderate technology risk with any component URSIT rating of 3, 4, or 5 or a composite rating of 3, 4, or 5 at the current IT examination

will be assigned a full URSIT rating – a rating for each of the four critical components and a composite rating – in a separate IT report of examination.

- Financial institutions exposed to a high level of technology risk will be assigned a full URSIT rating in a separate IT report of examination.

## TECHNOLOGY PROFILE SCRIPT

The Technology Profile Script is a series of questions completed by FDIC Field Supervisors or their designees no more than 3 months before each IT examination. The questions are generally answered by contacting the financial institution but can be completed based on information obtained from prior IT examination reports or from FDIC databases. Examiners use the answers from the profile script to complete a scoring matrix included as part of the profile script. Each technology component used by the institution contributes to the overall matrix score. The Field Supervisor or Supervisory Examiner may also make qualitative adjustments to the numeric scores to address risks that may not be evident in the Technology Profile Script.

The profile script is designed to be a standardized basic measurement of the complexity and risk of the technology deployed at a financial institution. The profile script can be used as a guide to assist examiners and managers in planning IT examinations by identifying key risk areas to review, the level and scope of review needed, and required examination procedures. The profile script can also be used to allocate examination resources and match examiner skills to the complexity of the institution or determine training needs.

The matrix score and other qualitative criteria are used to classify an institution's technology profile. Based on the matrix score, institutions are grouped into one of four technology profile categories. These range from Type I institutions that have limited technology systems to Type IV institutions that have complex or sophisticated technology systems. An institution's technology profile category, or type, is the key factor to determine the examination procedures to be used, such as whether the institution qualifies for IT-MERIT Procedures, the IT General Work Program, or FFIEC work programs. Table 5 quantifies the numerical ranges for determining the technology profile category and required examination procedures to be used at each financial institution being evaluated.

**Table 5: Technology Profile Scoring Matrix**

| Technology Profile Matrix Score Range | Technology Profile Category | Required Work Program |
|---|---|---|
| 0-49 | Type I | IT-MERIT Procedures |
| 0-49 | Type II | IT General Work Program |
| 50-79 | Type III | IT General Work Program supplemented by FFIEC work programs |
| 80-130 | Type IV | FFIEC work programs |

Source: FDIC Regional Directors Memorandum 2002-043.

Type I and Type II financial institutions have similar technology profile characteristics and fall within the same matrix score range. Type I differs from Type II in that Type I institutions have satisfactory ratings and do not conduct in-house programming or processing of core applications for other institutions. Type II institutions are those with less than satisfactory ratings (i.e., any component or composite URSIT rating of 3, 4, or 5 at the prior or current IT examination, including state regulatory authority examinations accepted by the FDIC) and those that conduct

in-house programming or perform core processing services for other insured financial institutions. Characteristics of each technology profile category are shown below.

- Type I financial institutions have limited networking and e-Banking activities and do not conduct in-house programming or perform core processing services for other insured institutions. Institutions in this category have minimal external threats with primary risks centered on the core banking system or vendor management. Examiners will use IT-MERIT procedures exclusively for all Type I institutions.

- Type II financial institutions have limited networking and e-Banking activities and usually do not conduct in-house programming or servicing of other institutions. Institutions in this category have minimal external threats with primary risks centered on the core banking system or vendor management. Examiners will use the IT General Work Program for all Type II institutions.

- Type III financial institutions have fully integrated networking into their operations. Institutions in this category have increased external threats from e-Banking activities and Internet connections or have increased operational risks from limited programming activities or servicing responsibilities. Examiners will use the IT General Work Program, supplemented with FFIEC work programs as needed, for Type III institutions.

- Type IV financial institutions rely on networks and other communication systems as a critical element of their operations. Networking among business clients and partners is common, and Internet connectivity may be relied upon as a critical communications medium. As a result of Internet and other wide-area network connections, risk of compromise or access to critical systems from external sources is present. The complexity of the technology increases system administration and security risks. Examiners will use the FFIEC work programs for all Type IV institutions

# CORPORATION COMMENTS

**Federal Deposit Insurance Corporation**
550 17th Street NW, Washington, D.C. 20429-9990
Division of Supervision and Consumer Protection

**June 4, 2004**

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

**FROM:** Michael J. Zamorski, Director
Division of Supervision and Consumer Protection
[Electronically produced version; original signed by Michael J. Zamorski]

**SUBJECT:** Response to OIG Draft Report Entitled *FDIC's Information Technology Examination Program* (Assignment Number 2003-058)

The Division of Supervision and Consumer Protection (DSC) appreciates the opportunity to respond to the Office of Inspector General's (OIG) draft report dated May 10, 2004, entitled FDIC's Information Technology Examination Program. We are pleased with the audit finding that FDIC's Information Technology (IT) examination program provides reasonable assurance that IT risks are being addressed by risk management programs in FDIC-supervised financial institutions.

We note the report identified opportunities for improving the quality control review of the IT examination process. Overall, DSC agrees that the IT review process may be enhanced. DSC currently reviews the effectiveness of the IT examination program as part of a bi-annual formal review process. Further, each of our six regional offices have quality assurance review processes in place. Currently, DSC is enhancing the quality assurance program covering our Regional and Territory examination programs. Lessons learned from our internal assessments and from this report will be incorporated into enhanced procedures. Provided below is the DSC action plan in response to the OIG recommendation.

OIG recommendation:

*(1) We recommend that the Director, DSC institute a quality review process for all phases of IT examinations including planning, field work, supporting documentation, and reporting, to ensure that IT examiners:*

* *consistently exercise sound judgment;*
* *apply the appropriate IT examination procedures;*
* *expand examination procedures when warranted;*
* *perform and document adequate work to support IT examination findings, conclusions, and ratings; and*
* *initial or sign and date the work papers and label them with the institution's name and location.*

DSC Response:

To ensure that examiners are performing the correct type of IT examination and using the correct IT work program, DSC will assess and revise as necessary the instructions for the IT pre-examination planning (PEP) memoranda, or in the case of embedded examinations, the safety and soundness PEP, to include the following items: type of examination planned, technology script profile score, and the intended work program to be used. The PEP will reconcile any difference between the type of examination and the technology script profile score. Thus, the PEP will provide a vehicle for supervisory personnel to review and approve major IT examination decisions. The PEP will serve as a quality control measure at the beginning of the IT examination process. DSC will assess, revise, and issue, as necessary the instructions for the appropriate PEP memoranda by December 31, 2004.

Currently, all of DSC's regions have field territory audit procedures that are administered by regional office staff to verify that work programs are properly completed and findings are adequately supported and documented. These programs commonly include reviews of IT examination work papers and generally capture the items that were recommended by the OIG.

To help strengthen this program, the DSC is standardizing a field territory review program to ensure examination program conformance with FDIC policies and to apply the appropriate emphasis on areas reviewed. The standardized field territory review program will incorporate the OIG's suggestions. The review program will also include periodic sampling of IT examination work papers and a review of examination processing that will provide a quality control measure at the completion of the IT examination process. DSC will implement enhancements by March 31, 2005.

## MANAGEMENT RESPONSE TO RECOMMENDATIONS

This table presents the management response that has been made on the recommendation in our report and the status of the recommendation as of the date of report issuance. The information in this table is based on management's written response to our report.

| Rec. Number | Corrective Action: Taken or Planned/Status | Expected Completion Date | Monetary Benefits | Resolved:[a] Yes or No | Dispositioned:[b] Yes or No | Open or Closed[c] |
|---|---|---|---|---|---|---|
| 1 | DSC will assess and revise as necessary the instructions for the IT pre-examination planning memoranda to include type of examination planned, Technology Profile Script score, and the intended work program to be used.<br><br>DSC is standardizing a field office review program to ensure examination program conformance with FDIC policies and to apply the appropriate emphasis on areas reviewed. The review program will include periodic sampling of examination work papers and a review of examination processing. | December 31, 2004<br><br>March 31, 2005 | N/A | Yes | No | 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] Dispositioned – The agreed-upon corrective action must be implemented, determined to be effective, and the actual amounts of monetary benefits achieved through implementation identified. The OIG is responsible for determining whether the documentation provided by management is adequate to disposition the recommendation.

[c] Once the OIG dispositions the recommendation, it can then be closed.