Office of Inspector General

February 2007
Report No. 07-005

Information Technology Examination Coverage of Financial Institutions' Oversight of Technology Service Providers

AUDIT REPORT

Office of Audits

OIG

Office of Audits

Report No. 07-005
February 2007

Information Technology Examination Coverage of Financial Institutions' Oversight of Technology Service Providers

Background and Purpose of Audit

In the first 10 months of 2006, over half of the 213 information security breaches reported by financial institutions to the FDIC involved technology service providers (TSP). In accordance with federal laws and regulations, financial institutions must safeguard sensitive customer information against unauthorized disclosure when outsourcing various information technology (IT) operations to TSPs.

Interagency guidelines contained in Part 364 of the FDIC Rules and Regulations establish key controls over TSPs, noting that each bank shall (1) exercise due diligence in selecting TSPs, (2) have contractual arrangements with their TSPs that require appropriate measures to safeguard customer information, and (3) provide ongoing monitoring of TSPs to ensure they have satisfied their contractual obligations. To ensure that FDIC-supervised financial institutions implement adequate information security program controls, the FDIC conducts periodic onsite IT examinations through its Information Technology-Risk Management Program (IT-RMP).

The objective of this audit was to assess the Division of Supervision and Consumer Protection's (1) IT examination procedures for addressing the security of sensitive customer information when FDIC-supervised institutions use TSPs and (2) examiners' implementation of those procedures.

To view the full report, go to www.fdicig.gov/2007reports.asp

Results of Audit

The FDIC has provided guidance to examiners to assess financial institutions' oversight of TSPs. In particular, the IT-RMP guidance requires examiners to consider the interagency guidelines in scoping examinations but does not detail examination procedures to assess compliance with the key controls over TSPs. Two of the four IT-RMP tools could be enhanced to provide information and examination procedures for assessing the risks associated with protecting the security and confidentiality of sensitive customer information when FDIC-supervised institutions use TSPs. Specifically, the IT-RMP Officer's Questionnaire, completed by institution management, could request information about the financial institution's key controls over TSPs. Additionally, guidance in the Snapshot Work Program could specifically address key controls related to due diligence in the selection of TSPs, contract provisions, and ongoing monitoring of TSPs.

All 12 examinations in our sample included assessments of the financial institutions' oversight of TSPs as required by the IT-RMP, and most provided at least some coverage of the key controls in the interagency guidelines. However, documentation for 10 of the 12 examinations did not contain sufficient written support that examiners had fully assessed institutions' compliance with the interagency guidelines regarding oversight of TSP protection of sensitive customer information. The IT-RMP Snapshot Work Program provides examiners considerable flexibility in tailoring IT examination procedures to the institution being examined and does not specifically require examiners to test or document the extent of an institution's oversight of TSPs.

The FDIC can achieve greater assurance that financial institutions are ensuring that TSPs safeguard customer information by enhancing IT-RMP guidance and IT examination documentation. Such assurance will help in protecting customers from identity theft and institutions from fraud and reputational and other risks associated with unauthorized access to or use of customer information.

Recommendations and Management Response

The report makes two recommendations that the FDIC: (1) revise IT-RMP guidance to ensure that examiners adequately assess financial institution compliance with the interagency guidelines pertaining to the oversight of TSPs and (2) reemphasize the need for examiners to clearly document decisions and supporting logic for the approach used in assessing compliance with the interagency guidelines related to TSPs as well as support for examiner conclusions. FDIC management agreed with both recommendations, noting that it is planning to evaluate the first year of performance under the IT-RMP. This evaluation will incorporate our recommendations, and the FDIC will issue additional guidance where necessary. Additionally, the FDIC will reemphasize examination documentation requirements to examiners.

TABLE OF CONTENTS

ACRONYMS

C.F.R.	**Code of Federal Regulations**
DSC	**Division of Supervision and Consumer Protection**
FACT	**Fair and Accurate Credit Transactions**
FDI	**Federal Deposit Insurance**
FDIC	**Federal Deposit Insurance Corporation**
FFIEC	**Federal Financial Institutions Examination Council**
FIL	**Financial Institution Letter**
GLBA	**Gramm-Leach-Bliley Act**
IT	**Information Technology**
IT-RMP	**Information Technology-Risk Management Program**
MERIT	**Maximum Efficiency, Risk-Focused, Institution Targeted**
OCC	**Office of the Comptroller of the Currency**
OIG	**Office of Inspector General**
OTS	**Office of Thrift Supervision**
RDM	**Regional Directors Memorandum**
ROE	**Report of Examination**
TSP	**Technology Service Provider**
U.S.C.	**United States Code**

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226

Office of Audits
Office of Inspector General

DATE: February 5, 2007

MEMORANDUM TO: Sandra L. Thompson, Director
Division of Supervision and Consumer Protection

/Signed/
FROM: Russell A. Rau
Assistant Inspector General for Audits

SUBJECT: *Information Technology Examination Coverage of Financial Institutions' Oversight of Technology Service Providers* (Report No. 07-005)

This report presents the results of the Office of Inspector General's (OIG) second audit in a series of audits pertaining to the FDIC's oversight of technology service providers (TSP).[1] The overall purpose of these audits is to assess the FDIC's examination coverage of TSPs and related efforts to protect sensitive customer information.[2] Our prior audit assessed the FDIC's process for identifying and monitoring TSPs used by FDIC-supervised institutions and for prioritizing examination coverage of TSPs.[3] For the current audit, our objective was to assess the Division of Supervision and Consumer Protection's (DSC) (1) information technology (IT) examination procedures for addressing the security of sensitive customer information[4] when FDIC-supervised institutions use TSPs and (2) examiners' implementation of those procedures. Appendix I of this report details our objective, scope, and methodology.

BACKGROUND

In accordance with federal laws and regulations (see Appendix II for additional information), financial institutions must safeguard sensitive customer information against unauthorized disclosure or use. The FDIC is responsible for examining FDIC-supervised financial institutions for adherence to these laws and regulations as part of its legislative

[1] According to *Interagency Guidelines Establishing Information Security Standards* (Appendix B to Part 364 of the FDIC Rules and Regulations), service provider ". . . means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the bank."

[2] Sensitive customer information is defined by Appendix B to Part 364 of the FDIC Rules and Regulations as a customer's Social Security number, personal identification number, password, or account number in conjunction with a personal identifier such as the customer's name, address, or telephone number. Such information would also include any combination of components of a customer's information such as a user name and password that would allow someone to log onto or access another person's account.

[3] OIG Report No. 06-015, *FDIC's Oversight of Technology Service Providers*, issued in July 2006.

[4] Security of customer information differs from financial privacy in that security measures are designed to safeguard against unauthorized access to or use of customer information, while financial privacy rules address a financial institution's ability to disclose data.

mandate to maintain stability and public confidence in the nation's financial system. Many financial institutions outsource various IT operations to TSPs. However, a financial institution's use of a TSP to provide needed products and services does not diminish the responsibility of the institution's board of directors and management to ensure that these activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations. According to FDIC IT examination guidance, TSP relationships should be subject to the same or greater risk management, security, privacy, and other internal controls and policies that would be expected if the financial institution were conducting the activities directly.

Statutory and Regulatory Guidance

The primary federal law governing the protection of sensitive customer information is the Gramm-Leach-Bliley Act (GLBA), Public Law 106-102. GLBA, enacted in 1999, requires financial institutions to protect the security and confidentiality of customer information. Under GLBA, each federal banking agency is required to establish appropriate standards for the financial institutions subject to their jurisdiction that would serve to:

- ensure the security and confidentiality of customer records;
- protect against anticipated threats or hazards to the security or integrity of such records; and
- protect against unauthorized access to or use of such records which would result in substantial harm or inconvenience to any customer.

To that end, in 2001 the federal banking agencies promulgated the *Interagency Guidelines Establishing Information Security Standards* (Interagency Guidelines), codified in the FDIC Rules and Regulations at 12 Code of Federal Regulations (C.F.R.) Part 364, Appendix B. Pursuant to the Interagency Guidelines, each bank must implement a customer information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. The security program must include a written plan that identifies key risks and controls related to the protection of customer information. Section III of the Interagency Guidelines notes that while overseeing service provider arrangements, each financial institution shall:

- exercise appropriate due diligence in selecting its TSPs;
- require its service providers, by contract, to implement appropriate measures designed to meet the objectives of the Interagency Guidelines; and

Key Controls in the Customer Information Security Program Applicable to TSPs

- ✓ **Due Diligence**
- ✓ **Contract Provisions**
- ✓ **Ongoing Monitoring**

Source: 12 C.F.R. Part 364.

- where indicated by the bank's risk assessment, monitor its TSPs to confirm that they have satisfied their obligations to implement appropriate security measures for customer information. As part of this monitoring, financial institutions should review audits, summaries of test results, or other equivalent evaluations of their TSPs.

Institution Guidance

The FDIC, in conjunction with the Federal Financial Institutions Examination Council (FFIEC)[5] has issued various Financial Institution Letters (FIL) addressing the outsourcing of technology services by financial institutions (see Appendix II).

Of particular note, the FDIC issued FIL-22-2001[6] in March 2001 to introduce the requirements of the Interagency Guidelines to the financial institutions it supervises. The FIL noted that the Interagency Guidelines describe the oversight role of an institution's board of directors in the process for creating, implementing, and maintaining an information security program for safeguarding customer information and its continuing duty to evaluate and oversee the program's overall status. Further, the FIL stated that the Interagency Guidelines describe the elements of a comprehensive risk-management plan to control risks to the security and confidentiality of customer information and identify the factors an institution should consider in evaluating the adequacy of its policies and procedures related to protecting customer information. The FIL states that institutions should exercise appropriate management of outsourcing arrangements, including confirming that service providers have implemented effective information security programs to protect customer information.

Also, the FDIC issued FIL-68-2001[7] in August 2001 to introduce examination procedures designed to help ensure institution compliance with customer safeguards in the Interagency Guidelines and to ensure that the standards established in the Interagency Guidelines are applied consistently. FIL-68-2001 provided extensive coverage of GLBA requirements and included key questions related to measures taken by an institution to oversee service providers. The procedures cover all three of the key controls related to TSPs as identified by the Interagency Guidelines.

Examiner Guidance

DSC generally conducts IT examinations in conjunction with risk management examinations every 12 or 18 months, depending on the asset size and condition of the institution. In 2005, DSC updated its risk-focused IT examination procedures for FDIC-supervised financial institutions. Specifically, DSC issued Regional Directors Memorandum (RDM 2005-031), *Information Technology-Risk Management Program (IT-RMP)*, on August 15, 2005.[8] The previous process focused on broad-based

[5] In addition to the FDIC, the FFIEC includes the Federal Reserve Board, National Credit Union Administration, Office of the Comptroller of the Currency (OCC), and Office of Thrift Supervision (OTS).
[6] Entitled, *Security Standards for Customer Information*.
[7] Entitled, *501(b) Examination Guidance.*
[8] The IT-RMP replaced the former IT-Maximum Efficiency, Risk-Focused, Institution Targeted (IT-MERIT) program and related work programs.

technology and control reviews, while the IT-RMP places considerable emphasis on management, information security program content, and confirmations and assurances obtained through audit or independent review. The IT-RMP integrates with other examination activities by embedding the results of the IT examination within the risk management Report of Examination (ROE), which documents the results of safety and soundness examinations of FDIC-supervised financial institutions, regardless of institution size, technical complexity, or prior examination rating.[9]

Under the IT-RMP, a review of the Interagency Guidelines is mandatory for each examination, including a review of the controls pertaining to TSPs. The IT-RMP contains four tools to assist examiners in an examination. The two primary tools that examiners use to assess a financial institution's oversight of TSPs are the IT Examination Officer's Questionnaire (Officer's Questionnaire) and the IT Examination Snapshot Work Program (Snapshot Work Program).

Key Tools of the IT-RMP

- ✓ **Technology Profile Script**
- ✓ **IT Summary Analysis**
- ✓ **Officer's Questionnaire**
- ✓ **Snapshot Work Program**

Source: FDIC IT-RMP Guidance.

- **Officer's Questionnaire** - This examiner risk-scoping tool is required to be completed by institution management and is used to collect key information about the institution's IT environment prior to an IT examination. The questionnaire represents the financial institution's self-assessment of its information security program and contains a series of questions, primarily in a "yes/no" format. The Officer's Questionnaire is organized as follows:

  Part 1, *Risk Assessment*
  Part 2, *Operations Security and Risk Management*
  Part 3, *Audit/Independent Review Program*
  Part 4, *Disaster Recovery and Business Continuity*
  Part 5, *Gramm-Leach-Bliley Act/FDIC Rules and Regulations-12 CFR Part 364, Appendix B*

  The assessment of an institution's controls over TSPs is generally included in Part 2, *Operations Security and Risk Management*, under the section on vendor management. Part 5 of the Officer's Questionnaire focuses on the institution's compliance with the Interagency Guidelines and does not specifically include information pertaining to TSPs.

- **Snapshot Work Program** - This examiner tool is used to guide examiner effort and document conclusions reached in the course of an IT examination. The Snapshot Work Program is tailored after the Officer's Questionnaire and provides "quick reference guidance" to examiners. Part 2 of the Snapshot Work Program contains guidance pertaining to the need for comprehensive contracts when

[9] FIL-81-2005 entitled, *Information Technology Risk Management Program (IT-RMP): New Information Technology Examination Procedures*, was issued August 18, 2005, notifying institutions of the new IT-RMP.

institutions use TSPs. It is important to note that examiners have considerable discretion in supplementing the Snapshot Work Program with any other approved FDIC or FFIEC work programs.

Reported Breaches of Security Related to Customer Information

The importance of protecting sensitive customer information at TSPs is underscored by the number of data security breaches reported by financial institutions to the FDIC in 2006. According to information obtained from the FDIC's security incident report, approximately 213 security breaches were reported at banks during the period January 2006 though October 2006, of which approximately 125 (59 percent) involved TSPs. These breaches included TSPs providing services to institutions for Internet banking, debit and credit cards, automated teller machines, and network operating systems.

RESULTS OF AUDIT

The FDIC has provided guidance to examiners for assessing financial institutions' oversight of TSPs. While we concluded that the 2001 examination guidance contained detailed procedures for assessing compliance with the Interagency Guidelines related to TSPs, this guidance is not mandatory. IT-RMP guidance, which is mandatory, requires examiners to consider the Interagency Guidelines in scoping examinations but does not detail examination procedures for assessing compliance with the key controls over TSPs. Two of the four IT-RMP tools could be enhanced to provide information and examination procedures for assessing the risks associated with protecting the security and confidentiality of sensitive customer information when FDIC-supervised institutions use TSPs. Specifically, the IT-RMP Officer's Questionnaire, completed by institution management, could request information about the financial institution's key controls over TSPs. Additionally, guidance in the Snapshot Work Program could specifically address key controls in the Interagency Guidelines related to due diligence in the selection of TSPs, contract provisions, and ongoing monitoring of TSPs (see **IT-RMP Guidance on Financial Institutions' Controls Over TSPs**).

All 12 examinations in our sample included assessments of the financial institutions' oversight of TSPs as required by IT-RMP, and most provided at least some coverage of the key controls in the interagency guidelines. However, documentation for 10 of the 12 examinations did not contain sufficient written support that examiners had fully assessed institutions' compliance with the Interagency Guidelines regarding oversight of TSP protection of customer information. The IT-RMP Snapshot Work Program provides examiners considerable flexibility in tailoring IT examination procedures to the institution examined and does not specifically require examiners to test or document the extent of an institution's oversight of TSPs. As noted above, the IT-RMP guidance also does not include detailed examination procedures to assess compliance with the Interagency Guidelines related to TSPs (see **Examiner Implementation of IT-RMP Guidance on Financial Institutions' Controls Over TSPs**).

The FDIC can achieve greater assurance that financial institutions are ensuring the security and confidentiality of customer information when using TSPs by enhancing IT-RMP guidance and IT examination documentation. Such assurance will help in protecting customers from identity theft and institutions from fraud and reputational and other risks associated with unauthorized access or use of customer information.

IT-RMP GUIDANCE ON FINANCIAL INSTITUTIONS' CONTROLS OVER TSPs

IT-RMP guidance could be enhanced to increase assurance that examiners are thoroughly assessing how financial institutions ensure that their TSPs are safeguarding sensitive customer information. Specifically, two primary examiner tools for assessing compliance with the Interagency Guidelines related to TSPs, the Officer's Questionnaire and Snapshot Work Program, could further ensure that examiners assess the three key controls of the Interagency Guidelines - due diligence, contract provisions, and ongoing monitoring.

Officer's Questionnaire

The Officer's Questionnaire is an integral component of the IT-RMP and, when completed, serves as the financial institution's self-assessment of its information security program. For examiners, the questionnaire serves as a risk analysis and scoping tool to identify strengths and weaknesses in the institution's information security program. The 5-part Officer's Questionnaire contains 85 questions for completion by the financial institution (see the *Background* section of this report). The two parts of the questionnaire that pertain to TSPs are discussed below.

Part 2 of the Officer's Questionnaire, *Operations Security and Risk Management*, asks whether the institution has a vendor management program. The question is intended to be answered with a "Yes" or "No" response and does not request information on the vendor management program. As a result, the institution's response may not be particularly useful for purposes of using the Officer's Questionnaire as a means to gain an understanding of the institution's risk management practices related to the protection of sensitive customer information by TSPs. Although the Snapshot Work Program provides more detailed examination guidance in assessing compliance with the Interagency Guidelines related to TSPs, the Officer's Questionnaire is a risk-scoping tool that is completed earlier in the IT-RMP process and could be used more effectively to solicit such information as the nature and extent of the institution's use of TSPs to process sensitive customer information, risk assessments related to the use of TSPs, and significant changes in TSP relationships since the prior examination.

Part 5 of the Officer's Questionnaire, *Gramm-Leach-Bliley Act/FDIC Rules and Regulations – 12 CFR Part 364, Appendix B,* addresses compliance with the Interagency Guidelines. The IT-RMP guidance for the Officer's Questionnaire addresses whether bank management has developed a written information security program meeting the standards of the Interagency Guidelines. The Questionnaire requests information on

those responsible for overseeing and implementing the security program, compliance audits, and the completion of employee awareness training related to the Interagency Guidelines. However, none of the five questions in Part 5 of the Officer's Questionnaire specifically address oversight of TSPs. Further, three of the five questions are intended to be answered with only a "Yes" or "No" response. In our opinion, the questionnaire could be improved by requesting information that describes the institution's information security program as it relates to TSPs and the TSP-related security controls identified in the Interagency Guidelines, such as: the due diligence process used in the selection of TSPs that have access to sensitive customer information, contract provisions that provide for security programs at TSPs, and ongoing monitoring of the activities of service providers with access to sensitive customer information. To facilitate completion of the Questionnaire, the questions in Part 2 could be consolidated under Part 5, which specifically relates to implementation of the Interagency Guidelines.

Snapshot Work Program

Examiners use the Snapshot Work Program both as a guide in performing the examination and to document examiners' findings and conclusions. The guidance in the Snapshot Work Program provides examiners considerable flexibility in tailoring examination procedures to the institution being examined. The Snapshot Work Program guidance encourages the use of appropriate portions of other FDIC and FFIEC examination guidance, as needed, to reach conclusions about an institution's effectiveness in managing IT risk. Although not specifically referenced, other guidance would include FIL-68-2001, previously discussed, which provides detailed examination procedures for assessing compliance with the Interagency Guidelines related to TSPs. However, the Snapshot Work Program itself does not ensure that examiners assess the key risks identified in the completed Officer's Questionnaire and associated with the oversight of TSPs. Specifically, the Snapshot Work Program could be supplemented with additional procedures for examiners to review due diligence, contract provisions and ongoing monitoring in relation to the customer information security activities involving TSPs, as discussed below.

Similar to the Officer's Questionnaire, Part 2 of the Snapshot Work Program, *Operations Security and Risk Management*, asks whether the institution has a vendor management program. Part 2 of the Snapshot Work Program states:

> Management should establish and maintain a formal vendor management program that defines the framework for controlling the risks associated with key vendors and service providers. For example, comprehensive contracts should be established that include service level agreement, audit expectations, and confidentiality/nondisclosure statements. In addition, the program should require service providers and vendors to maintain security programs that comply with requirements outlined within Part 364, Appendix B of the FDIC's Rules and Regulations. In summary, the vendor management program should require security standards that meet or exceed the bank's own standards. For additional information, refer to the FFIEC Handbooks and FILs regarding this topic.

While the above guidance is notable in that it addresses the need for a robust vendor management program, comprehensive contracts with TSPs, and TSP-maintained customer information security programs, the guidance could be enhanced by more clearly defining risk-based examination procedures for areas such as:

- institution vendor management policies and procedures related to customer information security, including risk assessment;
- consideration by the institution of TSP measures to protect customer information as part of due diligence in selecting TSPs;
- contracts with service providers incorporating the Interagency Guidelines;
- service provider reporting, including response to security compromises; and
- institution management review of TSP audits, test results, and other security-related evaluations and follow-up on corrective actions.

Part 5 of the Snapshot Work Program, *Gramm-Leach-Bliley Act/FDIC Rules and Regulations – 12 CFR Part 364, Appendix B,* addressing an institution's overall compliance with the Interagency Guidelines includes the following:

> An assessment of Part 364, Appendix B is mandatory at every examination. Based on management responses and your assessment of the bank's risk management practices, is management meeting Part 364, Appendix B requirements?

Part 5 also lists questions similar to those in Part 5 of the Officer's Questionnaire. This guidance is clear about the mandatory nature of coverage of the Interagency Guidelines as part of every examination and the importance DSC places on customer information security. However, Part 5 of the Snapshot Work Program does not specifically mention TSPs and could be improved by including specific procedures for examiners to consider in determining whether an institution is complying with the TSP provisions of the Interagency Guidelines. Similar to our conclusion related to the Officer's Questionnaire, the guidance in the Snapshot Work Program could also be consolidated under Part 5 of the program, which is specifically related to implementation of the Interagency Guidelines. Consolidation of the procedures could help to ensure appropriate coverage of the key controls in the Interagency Guidelines.

EXAMINER IMPLEMENTATION OF IT-RMP GUIDANCE ON FINANCIAL INSTITUTIONS' CONTROLS OVER TSPs

All 12 examinations we reviewed included a review of the institutions' compliance with the Interagency Guidelines, and most provided at least some coverage of key controls. However, documentation for 10 of 12 IT examinations did not contain sufficient written support that examiners had fully assessed financial institutions' compliance with the Interagency Guidelines regarding the oversight of TSPs in the three key control areas of due diligence, contract provisions, and ongoing monitoring. These key controls provide for the protection of customer information entrusted by the institution to the TSP. Assessments of these controls as part of an examination increase assurance that customer information is used by the TSP as intended by the institution. We based our conclusions on a review of how examiners assessed 17 TSP-specific steps that we identified in the Interagency Guidelines and institution and examiner guidance related to the key control areas in the Interagency Guidelines (see Appendixes III and IV for our analysis of the specific steps under the three key control areas). Also, we used existing DSC guidelines for examination documentation to assess examiners' written support. In some cases, where we were unable to determine the extent of the examiner's assessment of financial institution compliance with the Interagency Guidelines, DSC obtained additional documentation from the financial institutions to facilitate our review.

Documentation of Examiner Procedures

In accordance with RDM 2001-039, *Guidelines for Examination Workpapers and Discretionary Use of Examination Documentation Modules*, at a minimum, examiners should summarize the documentation relied upon during their review and briefly detail the procedures used and analysis conducted to support conclusions relative to significant areas of review. This guidance is applicable to examination coverage of institution oversight of TSPs. In addition, examination documentation should (1) demonstrate a clear trail of decisions and supporting logic within a given area, (2) provide written support for examination and verification procedures performed and conclusions reached, and (3) support assertions of fact or opinion in the financial schedules and narrative comments in the ROE. Furthermore, DSC's *Risk Management Manual of Examination Policies, Section 1.1-Basic Examination Concepts and Guidelines*, states that examination findings should be documented through a combination of brief summaries, bank source documents, ROE comments, and examination work papers that address both management practices and financial institution condition.

We recognize that there is a need for flexibility in choosing examination procedures and documenting support for examination procedures. For example, if the contract between the financial institution and its service providers had been reviewed in a separate examination of the TSP or a prior examination, and the term of a TSP contract extends into the period of the next examination cycle, there may not be a need for the IT examiner to review the contract again in the next IT examination. However, DSC should emphasize that examiners must clearly document decisions and the supporting logic for the approach used for assessing compliance with the Interagency Guidelines and support for conclusions reached on key controls, as discussed below. This will aid in ensuring

that risks are appropriately addressed in the current examination and in planning the scope for future examinations.

Due Diligence

The Interagency Guidelines require that each financial institution exercises appropriate due diligence in selecting its TSPs to help ensure that sensitive customer information is safeguarded. For 8 of the 12 examinations, there was documentation of at least a limited assessment of due diligence. For 3 of the 12 IT examinations, we found sufficient documentation that examiners had assessed the financial institutions' due diligence in selecting TSPs, particularly with regard to the protection of customer information. Five examinations included limited documentation that the financial institutions' compliance had been assessed; therefore, we could not conclude whether the examiners' review confirmed that the institution had:

Due Diligence Controls Assessed

✓ Determine the adequacy of the TSP's controls to safeguard the bank's sensitive customer information.
✓ Conduct background checks on key personnel.
✓ Determine extent of TSP's use of subcontractors, and conduct due diligence on subcontractors.

Source: OIG Analysis of FDIC and FFIEC Guidance.

- determined the adequacy of a TSP's controls to safeguard the bank's sensitive customer information;
- conducted background checks on key personnel; and
- determined the extent to which TSPs will use subcontractors, and if used, that the bank had conducted due diligence on the subcontractors.

The remaining four examinations did not include documentation that the institutions' compliance with due diligence requirements had been assessed by the IT examiners.

Contract Provisions

The Interagency Guidelines mandate that each financial institution require its service providers, by contract, to implement appropriate measures designed to:

- ensure the security and confidentiality of customer information,
- protect against any anticipated threats or hazards to the security of the information,
- protect against unauthorized access to or use of information that could result in substantial harm or inconvenience to any customer, and
- ensure the proper disposal of customer information.

To ensure that institutions have adequate controls over sensitive customer information at TSPs, IT examiners should confirm that institutions have established controls with the TSPs through appropriate contract provisions. However, for 10 of the 12 IT examinations we reviewed, there was limited or no documentation that examiners had confirmed the institutions' protection of sensitive customer information at TSPs through all of the appropriate contract provisions identified in TSP-related guidance. We based this conclusion on our review of examination documentation and available TSP contracts, along with interviews of the IT examiners who had conducted the work.

Contract Controls Assessed

✓ Protection of the bank's data from unauthorized access at the TSP.
✓ Incident response plan for unauthorized access and notification to the bank of a breach.
✓ Adequate disposal of the bank's sensitive customer information by the TSP.
✓ Adherence to regulatory guidance and requirements for the protection of sensitive customer information, including providing accurate information and timely access to a bank's regulatory agency.
✓ Specific or custom information security standards required by the bank (i.e., encryption and use of firewalls).
✓ Notification to the bank of subcontractor arrangements with the TSPs.
✓ Ownership of the bank's customer information, including the timely return of information at termination to the bank.
✓ Confidentiality of an institution's sensitive customer information.
✓ Types of evaluations, reviews, audits, or other reports of the TSP's controls to protect sensitive customer information or the right of the bank to audit the TSP.
✓ Determination on whether the institution's Legal Counsel had reviewed the contract.

Source: OIG Analysis of FDIC and FFIEC Guidance.

In reviewing the examiners' documentation of the 12 IT examinations, we made the following observations:

- **Evidence of review** - Documentation for three of the IT examinations did not contain any evidence of examiners' reviews of TSP contracts. Furthermore, the IT examiners could not recall whether any specific contracts had been reviewed.

- **Review of subcontractor arrangements** - TSPs subcontract with other service providers on occasion to perform portions of the services required by financial institutions. For nine of the IT examinations, there was limited or no documentation that examiners had ensured the financial institutions' contracts included provisions requiring TSPs to notify the institutions of subcontractor arrangements with TSPs. Without this contract provision, a financial institution may not be informed of other service providers handling the institution's customer information and, therefore, cannot adequately ensure the information is protected in accordance with the Interagency Guidelines.

- **Legal counsel review** - For 10 examinations, we did not find support that the IT examiners had ensured that the financial institution's legal counsel reviewed the contracts. According to the FFIEC's *Outsourcing Technology Services* Handbook, the contract is the single most important control in the outsourcing process, and institutions should engage legal counsel early in the process to help prepare and review the proposed contract.

Although all the financial institutions in our sample employed TSPs, only 4 of the 12 sets of IT examination work papers we reviewed contained copies of TSP contracts. In total,

we reviewed nine contracts contained in the IT examination work papers and concluded that:

- seven of the contracts did not contain provisions requiring an incident response plan in the event of unauthorized access to sensitive customer information at the TSP and notification to the bank;[10]
- six of the contracts did not include provisions for the TSPs' adequate disposal of the bank's sensitive customer information; and
- six of the contracts did not include provisions for evaluations, reviews, audits, or reports on the TSP's controls to protect sensitive customer information or the right of the bank to audit the TSP.

We also obtained four contracts from three additional institutions through DSC. We noted that all four of these contracts lacked key provisions such as:

- an incident response plan addressing unauthorized access to the bank's sensitive customer information at the TSP and notification to the bank,
- adequate disposal of the bank's sensitive customer information by the TSP, and
- specific information security standards required by the institution.

These examples indicate that some financial institution contracts with TSPs could more completely address the service provider's responsibilities for the security and confidentiality of customer information. Further, specific examination procedures could aid examiners in the review of contract provisions for compliance with the Interagency Guidelines.

Ongoing Monitoring

Ongoing monitoring of TSPs entails understanding the scope and nature of the services sufficiently to identify and appropriately react when the services provided are not at the level indicated in the agreement, no longer appropriately coordinate with the security controls at the institution, or no longer provide the risk mitigation desired. The Interagency Guidelines require banks to monitor their service providers, where indicated by the bank's risk assessment, to confirm that service providers have satisfied their obligations as required by the contract. As part of the bank's monitoring, it should review audits, summaries of test results, or other equivalent evaluations of its service

Ongoing Monitoring Controls Assessed

✓ Audit and regulatory reports of the TSP's general control environment, including information security practices, standards, and procedures for protecting the bank's sensitive customer information.
✓ Ensure that the TSP takes corrective action to address findings included in the audit and regulatory reports of the TSP.
✓ Conformance with specific or custom information security standards required by the bank and included in the contract.
✓ Subcontractors' compliance with Part 364, Appendix B security requirements.

Source: OIG Analysis of FDIC and FFIEC Guidance.

[10] According to FIL-27-2005, *Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, when an incident of unauthorized access to sensitive customer information involves information systems maintained by a bank's TSP, it is the institution's responsibility to notify its customers and regulator. However, a bank may contract with its TSP to notify the institution's customers or regulator on its behalf.

providers. For 9 of the 12 IT examinations we reviewed, we found support that examiners had ensured that financial institutions were obtaining independent, external reviews of the TSPs. In these cases, the reviews were performed in accordance with the American Institute of Certified Public Accountants Statement on Auditing Standards No. 70[11] entitled, *Reports on the Processing of Transactions by Service Organizations*. The reports of these reviews describe and, in some cases, document tests of the general control environment and information security practices, standards, and procedures of the TSPs. However, we determined that there was limited or no support that examiners had assessed whether financial institutions ensured that TSPs took appropriate corrective measures to address findings identified in audits, summaries of test results, or other equivalent evaluations of TSPs. In the remaining three instances, there was limited or no support in the examination documentation that examiners had ensured that institutions were obtaining independent, external reviews of TSPs.

We also noted that there was limited or no support in documentation for 8 of the12 IT examinations for the examiners' assessment of whether subcontractors were being used by TSPs for processing customer information, and if so, whether the subcontractors were being monitored for compliance with the Interagency Guidelines. The potential use of subcontractors to process customer information presents considerable risk to the security and confidentiality of the information that should be covered through the implementation of controls consistent with the Interagency Guidelines.

Ongoing monitoring of TSPs and their subcontractors by financial institutions helps to ensure that the TSPs safeguard the institution's sensitive customer information. Accordingly, examiners should perform procedures to confirm whether financial institutions ensure that TSPs and their subcontractors conform to contractual customer information security requirements.

CONCLUSION

Safeguarding sensitive customer information is critical to ensuring that consumers are protected from identity theft and institutions are protected from fraud and reputational and other risks. IT-RMP guidance could be enhanced to more specifically address key provisions of the Interagency Guidelines pertaining to due diligence in the selection of TSPs, contract provisions covering TSP relationships, and ongoing monitoring of TSPs. The IT-RMP guidance provides examiners considerable flexibility in tailoring examination procedures. Much of the guidance for an IT examination is contained in various FDIC and FFIEC work programs. Accordingly, the FDIC can achieve greater assurance that financial institutions are adequately ensuring the security and confidentiality of customer information when using TSPs by enhancing IT-RMP guidance and IT examination documentation.

[11] Statement on Auditing Standards No. 70 defines the professional standards used by an auditor to assess the internal controls of a service organization. Service organizations, such as data centers, insurance claims processors, and credit processing companies, provide outsourcing services that affect the operation of the contracting enterprise.

RECOMMENDATIONS

We recommend the Director, DSC:

1. Revise IT-RMP guidance to ensure that examiners adequately assess financial institution compliance with the Interagency Guidelines provision pertaining to the oversight of TSPs by:

    - Adding questions to the IT Examination Officer's Questionnaire that request information on the (a) identification and risk assessment of all TSPs with access to sensitive customer information and (b) compliance with the control areas of due diligence, contract provisions, and ongoing monitoring. Consideration should be given to consolidation of the questions pertaining to the Interagency Guidelines under one part of the Officer's Questionnaire.

    - Amend the IT Snapshot Work Program to consolidate all guidance related to compliance with the Interagency Guidelines under one section and to include specific examination procedures to address the three TSP-related control areas of due diligence, contract provisions, and ongoing monitoring contained in the Interagency Guidelines. Consideration should be given to the TSP-specific steps identified in Appendixes III and IV of this report.

2. Reemphasize the need for examiners to clearly document decisions and supporting logic for the approach used in assessing compliance with the Interagency Guidelines related to TSPs as well as support for examiner conclusions.

CORPORATION COMMENTS AND OIG EVALUATION

On January 29, 2007, the Director, DSC, provided a written response to a draft of this report. DSC's response is presented in its entirety as Appendix V to this report. DSC agreed with both recommendations, noting that it is planning to evaluate the first year of performance under the IT-RMP. This evaluation will incorporate our recommendations, and DSC will issue additional guidance where necessary. Additionally, DSC will reemphasize examination documentation requirements to examiners.

DSC's actions are responsive to our recommendations. A summary of management's response to the recommendations is in Appendix VI. The recommendations are resolved but will remain open until we have determined that agreed-to corrective actions have been completed and are effective.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this audit was to assess DSC's (1) IT examination procedures for addressing the security of sensitive customer information when FDIC-supervised institutions use TSPs and (2) examiners' implementation of those procedures. We conducted our audit in accordance with generally accepted government auditing standards during the period April through November 2006.

Scope and Methodology

The audit focused on DSC's examination assessment of FDIC-supervised institutions' compliance with the Interagency Guidelines pertaining to the oversight of TSPs. To accomplish the audit objective, we evaluated relevant supervisory procedures for assessing TSP oversight consistent with RDM 2005-031, *Information Technology-Risk Management Program (IT-RMP)*. We also evaluated the IT-RMP guidance for consistency with applicable federal laws, regulations, policies, and guidelines related to the oversight of TSPs. Additionally, we considered other supplementary guidance such as FFIEC handbooks, industry best practices, and guidance issued by other regulators.

We coordinated our audit work with a separate FDIC OIG audit of IT-RMP, and both audits relied on the same sample of examinations. We selected a non-statistical[12] sample of 12 examinations from a total of 292 examinations conducted during the period January through March 2006, consisting of 4 examinations conducted in the FDIC's New York Region, 4 in the San Francisco Region, and 4 in the Kansas City Region.

We selected our sample from the New York, Kansas City, and San Francisco regions based on the following considerations.

- The New York Region had the largest dollar-value financial institutions in our sample population.
- The Kansas City Region had the largest number of financial institutions in our sample population.
- The San Francisco Region had the most widely dispersed financial institutions in our sample population.

We discussed our proposed sample with DSC management to explain our methodology and to ensure that our sample would produce meaningful results. DSC provided suggestions regarding which regional offices, IT composite ratings, and institution asset sizes we should consider in selecting our sample.

[12] The results of a non-statistical sample cannot be projected to the intended population by standard statistical methods.

Further, we interviewed DSC staff who had responsibilities for establishing and implementing the IT-RMP. We also did the following:

- Assessed policies and procedures developed and used by DSC for examining IT security risks when institutions use TSPs.
- Reviewed DSC's criteria in IT-RMP guidance for categorizing IT security risks in financial institutions with TSPs.
- Conducted interviews with IT examination specialists and IT examiners.
- Reviewed applicable laws and regulations and FDIC policies, procedures, and directives.
- Reviewed FFIEC guidance, including *Outsourcing Technology Services* (June 2004), *Supervision of Technology Service Providers* (March 2003), *Information Security* (December 2002 and July 2006 revision), *Business Continuity Planning* (March 2003), and *Audit* (August 2003), which are 5 of 12 booklets that, in total, comprise the *FFIEC Information Technology Handbook*.

Internal Controls

We identified, gained an understanding of, and evaluated selected internal controls over the establishment and implementation of supervisory procedures that addressed the FDIC-supervised institutions' management of IT security risks. We reviewed the FDIC's (1) policies and procedures related to the oversight of TSPs and the protection of sensitive customer information and (2) applicable policies and procedures in the FDIC Rules and Regulations, Regional Directors Memoranda, FILs, and FFIEC IT examination and supervision guidance. We also interviewed DSC individuals involved in IT examinations. This report discusses internal control concerns, identified during our audit, that relate to IT-RMP guidance.

Reliance on Computer-Based Data

We obtained certain data from DSC's information system to identify IT examinations conducted subsequent to the August 15, 2005 implementation of the IT-RMP and data security breaches reported for the period January through October 2006. We did not assess the reliability of the computer-based data because these data were not significant to our findings, conclusions, or recommendations.

Government Performance and Results Act

The Government Performance and Results Act of 1993 directs federal agencies to develop a strategic plan and annual performance plans to help improve federal program effectiveness and service delivery. We reviewed the FDIC's *Strategic Plan for 2005-2010* and the *FDIC 2006 Annual Performance Plan*. We determined that the FDIC did not have a strategic goal or objective specifically related to IT examinations. However, the means and strategies the FDIC uses to achieve a strategic goal that FDIC-supervised institutions are safe and sound includes IT examinations in general, as stated in the *FDIC 2006 Annual Performance Plan*:

The FDIC also continues to focus on the risks posed by technology. Both onsite risk management and information technology examinations cover technology-related activities to determine how each FDIC-supervised depository institution manages risk in that area. The FDIC uses a monitoring system to proactively identify and assess indicators of technology risks that may impact FDIC-supervised institutions. The FDIC will also augment its general training curriculum for examiners to include more training on technology issues and the Information Technology Examination Course, which teaches examiners how to better integrate technology risk management, will be revised as a result of the IT-RMP.

We did not assess IT-RMP training as part of this audit. Rather, we provided coverage of IT-RMP training in a separate audit assignment that was ongoing at the completion of our fieldwork (for details, see the section entitled, *Prior Audit Coverage*).

Fraud and Illegal Acts

We did not develop specific audit procedures to detect fraud and illegal acts because they were not considered material to the audit objectives. However, throughout the audit, we were alert to the possibility for fraud and illegal acts, and none came to our attention.

Laws and Regulations

In conducting the audit, we considered the following laws and regulations, as well as additional laws and regulations identified in Appendix II.

- GLBA provides for the protection of nonpublic personal information. Each financial institution has an obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. Each financial institution must establish administrative, technical, and physical safeguards to ensure the confidentiality of customer records and information; to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

- Fair and Accurate Credit Transactions (FACT) Act. This Act amends the Fair Credit Reporting Act by adding provisions covering identity theft, consumers' access to credit information, enhanced consumer report accuracy, and financial literacy. The statutes prescribe financial institutions' responsibilities for protecting consumer information and sharing it with other entities.

- Federal Deposit Insurance (FDI) Act Section 10 - *Provisions Related to Examination Authority*. The FDI Act requires the FDIC to perform periodic "full scope" examinations of FDIC-supervised institutions. IT examinations are included as part of a "full scope" examination.

- FDIC Rules and Regulations, Part 364, Appendix B - *Interagency Guidelines Establishing Information Security Standards*. These standards require financial institutions to conduct appropriate due diligence in selecting service providers; require service providers, by contract, to implement appropriate measures to protect customer information; and monitor service providers.

Prior Audit Coverage

Audit Report No. 06-015, *FDIC's Oversight of Technology Service Providers*, issued July 20, 2006. The objective was to assess the FDIC's examination coverage of TSPs and related efforts to protect sensitive customer information. The report made six recommendations for the FDIC to: (1) better identify and monitor TSPs with access to sensitive customer information and (2) improve the process the FDIC uses (in conjunction with the other FFIEC agencies) for assessing the risks posed by, and prioritizing for examination, those TSPs with access to sensitive customer information. DSC's response and proposed actions were sufficient to resolve each recommendation.

Audit Report No. 07-002, *The Division of Supervision and Consumer Protection's Information Technology-Risk Management Program*, issued January 10, 2007. The objective was to determine whether the FDIC had established and implemented adequate procedures for addressing IT security risks at FDIC-supervised institutions that offer electronic banking products and services. The report made seven recommendations to enhance the tools and guidance under the IT-RMP methodology and the IT training programs. FDIC management generally agreed with our recommendations and will review the tools, guidance, and training programs as part of an evaluation of the first year of performance under the IT-RMP program and will issue revised guidance or make enhancements as deemed necessary.

APPENDIX II

SELECTED LAWS, REGULATIONS, AND GUIDANCE RELATED TO TSP PROTECTION OF CUSTOMER INFORMATION

Laws	**Provisions**
15 United States Code (U.S.C.) 6801 Gramm-Leach-Bliley Act (GLBA)	GLBA provides for the protection of nonpublic personal information by establishing: (a) privacy obligation policy - it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information; and (b) financial institutions' safeguards. In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards: (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. As mandated by this law, interagency examination guidelines and procedures were developed to address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.
Regulations	
12 C.F.R. Part 332, *Privacy of Consumer Financial Information*	(a) Purpose. Part 332 governs the treatment of nonpublic personal information about consumers by the financial institutions listed in paragraph (b) of this section. This part: (1) Requires a financial institution to provide notice to customers about its privacy policies and practices. (2) Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties. (3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to the exceptions in §§ 332.13, 332.14, and 332.15. (b) Scope. (1) Part 332 applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes. This part does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes. This part applies to the United States offices or entities for which the FDIC has primary supervisory authority.
12 C.F.R. Part 364, *Standards for Safety and Soundness*, Appendix B, *Interagency Guidelines Establishing Information Security Standards*	(a) General standards. The *Interagency Guidelines Establishing Security Standards* prescribed pursuant to section 39 of the FDI Act (12 U.S.C. 1831p--1), as set forth in Appendix A to this part, apply to all insured state nonmember banks and to state-licensed insured branches of foreign banks that are subject to the provisions of section 39 of the FDI Act. (b) *Interagency Guidelines Establishing Information Security Standards*. These guidelines, prescribed pursuant to section 39 of the FDI Act (12 U.S.C. 1831p--1) and sections 501 and 505(b) of GLBA (15 U.S.C. 6801, 6805(b)), and with respect to the proper disposal of consumer information requirements pursuant to section 628 of the Fair

	Credit Reporting Act (15 U.S.C. 1681w), as set forth in Appendix B to this part, apply to all insured state nonmember banks, insured state-licensed branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).
Interagency Guidance	
FIL-81-2000, *FFIEC Guidance on Managing Risks Associated With Outsourcing Technology Services* November 2000	Through the FFIEC, the regulators issued this guidance on key management issues when outsourcing technology. These issues include risk assessment, service provider selection, contract terms, and oversight of outsourcing arrangements. The guidance is intended to assist financial institutions that are increasingly relying on outside firms for technology-related products and services to support an array of banking functions. Institutions of all sizes are using these products and services, as technology grows more complex and dynamic, creating a greater impetus to outsource.
FIL-22-2001, *Security Standards For Customer Information* March 2001	The purpose of this FIL was to identify, establish, approve, and issue joint guidelines establishing standards for safeguarding customer information as required by GLBA. The guidelines provide expectations for creating, implementing, and maintaining an information security program and the oversight and continuing duty of the institution's board of directors to identify and assess the risks that may threaten customer information. In addition, the FIL requires that the institution develop a written plan containing policies and procedures to manage and control risk; implement and test the plan; and adjust the plan on a continuing basis to account for changes in technology, sensitivity of customer information; and internal or external threats to information security.
FIL-50-2001, *Bank Technology Bulletin on Outsourcing* June 2001	Contained in this FIL are documents that were provided to FDIC-supervised institutions, providing practical information to community banks on how to select service providers, draft contract terms, and oversee multiple service providers when outsourcing for technology services and products.
FIL-68-2001, *501(b) Examination Guidance* August 2001	This FIL provides joint examination procedures to evaluate sensitive customer information in accordance with GLBA 501(b), which identifies the standards to ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.
FIL-89-2004, *FFIEC Information Technology Examination Handbook* July 2004	The FFIEC has issued booklets with guidance on evaluating management and outsourcing technology services. The FIL states that "outsourcing of an activity does not relieve management and the board of directors of their responsibility to ensure the institution's data are processed in a secure environment and to maintain data integrity."
FIL-81-2005, *Information Technology Risk Management Program (IT-RMP) Examination Procedures*, August 2005	The FIL announced the FDIC's implementation of the new IT-RMP for conducting IT examinations of FDIC-supervised financial institutions. IT-RMP examination procedures apply to all FDIC-supervised banks, regardless of size, technical complexity, or prior examination rating. The FIL also advised that the former IT-MERIT procedures and related work programs have been rescinded.

FFIEC IT Examination Handbook, *Outsourcing Technology Services*, June 2004	Provides guidance and examination procedures to assist examiners and bankers in evaluating a financial institution's risk management processes to establish, manage, and monitor IT outsourcing relationships.
FFIEC IT Examination Handbook, *Supervision of Technology Service Providers*, March 2003	This booklet governs the supervision of TSPs and briefly summarizes the FFIEC member agencies' (agencies) expectations of financial institutions in the oversight and management of their TSP relationships. This booklet outlines the agencies' risk-based supervision approach, the supervisory process, and the examination ratings used for TSPs. In addition, this booklet discusses two special IT-related programs administered by the agencies: the Multi-Regional Data Processing Servicer Program, geared towards examining large TSPs and the Shared Application Software Review Program aimed at reviewing mission-critical software packages.
FFIEC IT Examination Handbook, *Information Security* July 2006	This booklet provides guidance to examiners and organizations on assessing the level of security risks to the organization and evaluating the adequacy of the organization's risk management.
FFIEC IT Handbook, *Audit*, August 2003	This booklet replaces and rescinds Chapter 8 of the *1996 FFIEC Information Systems Examination Handbook*. It is used by agency examiners as a foundation from which they can assess the quality and effectiveness of an institution's IT audit program. It describes the roles and responsibilities of the board of directors, management, and internal or external auditors; identifies effective practices for IT audit programs; and details examination objectives and procedures. Agency examiners will use the examination procedures in Appendix A to assess the adequacy of IT audit programs at both financial institutions and TSPs. The examination guidance and procedures in this booklet focus on IT audit and supplement other, more general, internal and external audit guidance provided by the agencies.
Fair and Accurate Credit Transactions (FACT) Act Implementation	The OCC, FDIC, Federal Reserve, and OTS adopted a final rule to implement section 216 of the FACT Act by amending the *Interagency Guidelines Establishing Information Security Standards*. The final rule generally requires each financial institution to develop, implement, and maintain, as part of its existing information security program, appropriate measures to properly dispose of consumer information derived from consumer reports.
DSC - Regional Directives	
DSC Internal Control Field Territory – Module 3b: Information Technology Examinations (August 15, 2005)	This represents the work program for RDM 2005-031, *Information Technology Risk Management Program*. This work program should be used for examinations starting after August 15, 2005.
RDM 2005-031 – *Information Technology Risk Management Program (IT-RMP)*	The IT-RMP represents a new approach for conducting IT examinations at all FDIC-supervised financial institutions, regardless of size or complexity. Using the new IT-RMP procedures, examiner focus shifts from historic-based technology and control reviews to assessing management and IT risk management practices as communicated through a financial institution's formal information security program.
RDM 2004-014 – *Information Technology General Work Program Revision*	The IT General Work Program, issued through this RDM, was revised to include additional guidance to examiners for a) Appendix B, Part 364, of the FDIC Rules and Regulations; b) imaging technology; and c) wireless technology.

APPENDIX II

RDM 2004-002 – *Report Treatment of Compliance with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information*	To ensure consistency in reporting financial institutions' compliance with the Interagency Guidelines, all safety and soundness and separate-cover IT ROEs should include a comment regarding the subject institution's compliance with the guidelines - 12 C.F.R. Part 364, Appendix B. In the event of serious noncompliance, examiners should document that the financial institution fails to meet the standards prescribed under this section of the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*. Examiners should not include comments to the effect that the bank "is in violation of the Guidelines" or is being "cited for a violation of the Guidelines."
RDM 2001-039 – *Guidelines for Examination Work Papers and Discretionary Use of Examination Documentation Modules*	Examination findings should be documented using a combination of brief summaries, bank source documents, report comments, and other examination work papers that address both management practices and condition.
DSC Examination Manual, Section 1.1, *Basic Examination Concepts and Guidelines*	Examination documentation should demonstrate a clear trail of decisions and supporting logic within a given area. Documentation should provide written support for examination and verification procedures performed and conclusions reached and support the assertions of fact or opinion in the financial schedules and narrative comments in the ROE.

APPENDIX III

ANALYSIS OF EXAMINER DOCUMENTATION OF INSTITUTION COMPLIANCE WITH INTERAGENCY GUIDELINES IN RELATION TO THREE KEY CONTROL AREAS

Three Key Control Areas Reviewed	Bank 1	Bank 2	Bank 3	Bank 4	Bank 5	Bank 6	Bank 7	Bank 8	Bank 9	Bank 10	Bank 11	Bank 12
Due Diligence												
1. Determine the adequacy of the TSP's controls to safeguard the bank's sensitive customer information.	N	N	Y	N	Y	N	N	N	N	N	Y	N
2. Conduct background checks on key personnel.	N	N	Y	N	Y	N	N	N	N	N	Y	N
3. Determine the extent of the TSP's use of subcontractors, and conduct due diligence on subcontractors.	N	N	Y	N	Y	N	N	N	N	N	Y	N
Contract Provisions												
4. Protection of the bank's data from unauthorized access at the TSP.	Y	N	Y	N	Y	N	N	N	N	N	Y	N
5. Incident response plan for unauthorized access and notification to the bank of breach.	N	N	Y	N	Y	N	N	N	N	N	Y	N
6. Adequate disposal of the bank's sensitive customer information by the TSP.	N	N	Y	N	Y	N	N	N	N	N	Y	N
7. Adherence to regulatory guidance and requirements for the protection of sensitive customer information, including providing accurate information and timely access to a bank's regulatory agency.	Y	N	Y	N	Y	N	N	N	N	N	Y	N
8. Specific or custom information security standards required by the bank (i.e., 128-bit encryption, use of firewalls).	N	N	Y	N	Y	N	N	N	N	N	Y	N
9. Notification to the bank of subcontractor arrangements with the TSPs.	N	N	Y	N	Y	N	N	N	N	N	Y	N
10. Ownership of the bank's customer information, including the timely return of information at contract termination to the bank.	N	N	Y	N	Y	N	N	N	N	N	Y	N
11. Confidentiality of an institution's sensitive customer information.	N	N	Y	N	Y	Y	N	N	N	N	Y	N
12. Types of evaluations, reviews, audits, or other reports of the TSP's controls to protect sensitive customer information or the right of the bank to audit the TSP.	N	N	Y	N	Y	N	N	N	N	N	N	N
13. Determine whether the institution's Legal Counsel had reviewed the contract.	N	N	Y	N	Y	N	N	N	N	N	N	N

Legend: Y = Sufficient documentation.
N = Limited or no documentation.

Three Key Control Areas Reviewed	Bank 1	Bank 2	Bank 3	Bank 4	Bank 5	Bank 6	Bank 7	Bank 8	Bank 9	Bank 10	Bank 11	Bank 12
Ongoing Monitoring												
14. Audit and regulatory reports on the TSP's general control environment, including information security practices, standards, and procedures for protecting the bank's sensitive customer information.	Y	N	Y	N	Y	Y	Y	Y	Y	Y	N	Y
15. Ensure that the TSP takes corrective action to address findings included in the audit and regulatory reports on the TSP.	N	N	Y	N	Y	N	N	Y	N	Y	N	N
16. Conformance with specific or custom information security standards required by the bank and included in the contract.	Y	N	Y	N	Y	N	N	Y	N	Y	N	N
17. Subcontractors' compliance with Part 364, Appendix B, security requirements.	N	N	Y	N	Y	N	N	Y	N	Y	N	N

Source: OIG analysis of 12 IT examinations sampled. We used FDIC RDM 2001-039 as the basis for making our determinations with regard to the sufficiency of documentation.

APPENDIX IV

SUMMARY ANALYSIS OF EXAMINER DOCUMENTATION OF INSTITUTION COMPLIANCE WITH INTERAGENCY GUIDELINES IN RELATION TO THREE KEY CONTROL AREAS

Three Key Control Areas Reviewed	Sufficient Documentation	Limited or No Documentation
	Number of Examinations	
Due Diligence		
1. Determine the adequacy of the TSP's controls to safeguard the bank's sensitive customer information.	3	9
2. Conduct background checks on key personnel.	3	9
3. Determine the extent of the TSP's use of subcontractors, and conduct due diligence on subcontractors.	3	9
Contract Provisions		
4. Protection of the bank's data from unauthorized access at the TSP.	4	8
5. Incident response plan for unauthorized access and notification to the bank of breach.	3	9
6. Adequate disposal of the bank's sensitive customer information by the TSP.	3	9
7. Adherence to regulatory guidance and requirements for the protection of sensitive customer information, including providing accurate information and timely access to a bank's regulatory agency.	4	8
8. Specific or custom information security standards required by the bank (i.e., 128-bit encryption, use of firewalls).	3	9
9. Notification to the bank of subcontractor arrangements with the TSPs.	3	9
10. Ownership of the bank's customer information, including the timely return of information at contract termination to the bank.	3	9
11. Confidentiality of an institution's sensitive customer information.	4	8
12. Types of evaluations, reviews, audits, or other reports of the TSP's controls to protect sensitive customer information or the right of the bank to audit the TSP.	2	10
13. Determine whether the institution's Legal Counsel had reviewed the contract.	2	10
Ongoing Monitoring		
14. Audit and regulatory reports on the TSP's general control environment, including information security practices, standards, and procedures for protecting the bank's sensitive customer information.	9	3
15. Ensure that the TSP takes corrective action to address findings included in the audit and regulatory reports on the TSP.	4	8
16. Conformance with specific or custom information security standards required by the bank and included in the contract.	5	7
17. Subcontractors' compliance with Part 364, Appendix B, security requirements.	4	8

Source: OIG analysis of 12 IT examinations sampled. We used FDIC RDM 2001-039 as the basis for making our determinations with regard to the sufficiency of documentation.

CORPORATION COMMENTS

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

DATE: January 29, 2007

TO: Russell A. Rau
Assistant Inspector General for Audits

FROM: Sandra L. Thompson
Director

SUBJECT: Response to Draft Report Entitled: ***Information Technology Examination Coverage of Financial Institutions' Oversight of Technology Service Providers*** **(2006-018)**

This memorandum represents the Division of Supervision and Consumer Protection (DSC) response to the draft report entitled, *The Division of Supervision and Consumer Protection's Information Technology Examination Coverage of Financial Institutions' Oversight of Technology Service Providers* (2006-018) prepared by the FDIC's Office of Inspector General (OIG). This audit focused on DSC's examination assessment of FDIC-supervised institutions' compliance with the Interagency Guidelines pertaining to the oversight of Technology Service Providers (TSPs). The OIG draft report concluded that "FDIC has provided guidance to examiners to assess financial institutions' oversight of TSPs." DSC's actions to address each recommendation are discussed below.

OIG RECOMMENDATIONS AND DSC RESPONSES

1. **Revise IT-RMP guidance to ensure that examiners adequately assess financial institution compliance with the Interagency Guidelines provision pertaining to the oversight of TSPs by:**

   - **Adding questions to the IT Examination Officer's Questionnaire that request information on the (a) identification and risk assessment of all TSPs with access to sensitive customer information and (b) compliance with the control areas of due diligence, contract provisions, and ongoing monitoring. Consideration should be given to consolidation of the questions pertaining to the Interagency Guidelines under one part of the Officer's Questionnaire.**

   - **Amend the IT Snapshot Work Program to consolidate all guidance related to compliance with the Interagency Guidelines under one section and to include specific examination procedures to address the three TSP-related control areas of due diligence, contract provisions, and ongoing monitoring contained in the Interagency Guidelines. Consideration should be given to the TSP-specific steps identified in Appendixes III and IV of this report.**

DSC Response

Recommendation one suggests enhancements to our current IT-RMP tools and guidance. We agree that each of these items should be evaluated. DSC is planning an evaluation of the first year of performance under the IT-RMP program. We will incorporate your recommendations into our evaluation and issue additional guidance where necessary. We will issue any revised guidance by September 30, 2007.

2. **Reemphasize the need for examiners to clearly document decisions and supporting logic for the approach used in assessing compliance with the Interagency Guidelines related to TSPs as well as support for examiner conclusions.**

DSC Response

DSC currently requires examiners to clearly document work performed related to TSP oversight. By March 30, 2007, DSC will re-emphasize examination documentation requirements.

MANAGEMENT RESPONSE TO RECOMMENDATIONS

This table presents the management response on the recommendations in our report and the status of the recommendations 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	DSC is planning an evaluation of the first year of performance under the IT-RMP program. DSC will incorporate the recommendations into its evaluation and issue additional guidance where necessary.	September 30, 2007	N/A	Yes	Open
2	DSC will re-emphasize examination documentation requirements.	March 30, 2007	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 the agreed-upon corrective actions have been completed and are effective, the recommendation can be closed.