Office of Inspector General

January 2007
Report No. 07-002

The Division of Supervision and Consumer Protection's Information Technology-Risk Management Program

AUDIT REPORT

Office of Audits

oig

Office of Audits

Report No. 07-002
January 2007

The Division of Supervision and Consumer Protection's Information Technology-Risk Management Program

Background and Purpose of Audit

Information is one of a financial institution's most important assets. Protection of information assets is necessary to establish and maintain trust between the financial institution and its customers, maintain compliance with the law, and protect the reputation of the institution. Information security is the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations.

Interagency guidelines require financial institutions to implement a comprehensive written information security program. To ensure that FDIC-supervised financial institutions implement adequate information security program controls, the Corporation conducts periodic onsite information technology (IT) examinations and, in August 2005, the Division of Supervision and Consumer Protection (DSC) established the Information Technology-Risk Management Program (IT-RMP). IT-RMP replaced the broad-based technology and control reviews conducted under the former IT examination program.

The objective of this audit was to determine whether the FDIC has established and implemented adequate procedures for addressing IT security risks at FDIC-supervised institutions that offer electronic banking products and services. We focused this review on the IT-RMP and DSC's examiner training framework in relationship to the new program.

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

Results of Audit

DSC has established procedures within the IT-RMP for addressing IT security risks at FDIC-supervised financial institutions. These procedures address most of the information security requirements contained in interagency guidance. Our review of 12 IT examinations found that examiners generally followed the procedures outlined in the IT-RMP, and in doing so, carried out the following activities:

- Identified the risks and technology deployed at the institution for the purpose of determining examination staffing needs.
- Reviewed the financial institution's Officer's Questionnaire regarding the bank's risk management practices.
- Performed onsite examination procedures to assess the financial institution's information security program.
- Assigned an IT composite rating at the conclusion of the examination and reported IT examination findings in the report of examination.

However, improvements to the IT-RMP program would help to ensure adequate and consistent implementation of the IT-RMP and related examination procedures. Specifically, DSC could revise certain IT-RMP tools to assist examiners in more effectively identifying relevant IT security risks to be assessed. We concluded that DSC could:

- Clarify in the IT-RMP guidance the purpose and use of the Technology Profile Script, which is used to determine examiner staffing needs, or reevaluate the benefits of continued use of this tool.
- Enhance the Officer's Questionnaire provided to the financial institution to address certain information security requirements contained in interagency guidelines.
- Modify IT-RMP guidance to (a) replace some "yes/no" questions in the Officer's Questionnaire with more descriptive questions and (b) require that examiners evaluate, based on identified risks, a sample of positive responses to questions in the Officer's Questionnaire to ensure their accuracy.
- Expand instructions for the Summary Analysis, an IT-RMP examination scoping and reporting tool, to clarify the extent to which examiners should document an institution's risk profile and corresponding procedures to address the risks.

DSC also needs to update IT-RMP guidance to more clearly address the methodology examiners should use in deriving the IT composite rating for a financial institution. Clarified guidance could increase assurance that IT ratings accurately and consistently reflect the effectiveness of an institution's IT risk management practices and the adequacy of its information security program.

The report makes 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 is taking responsive action to review DSC's 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.

TABLE OF CONTENTS

ACRONYMS

ACH	Automated Clearing House
AMDS	Audit, Management, Development and Acquisition, and Support and Delivery
CPO	Corporate Performance Objective
DSC	Division of Supervision and Consumer Protection
FACT Act	Fair and Accurate Credit Transactions Act of 2003
FDI	Federal Deposit Insurance
FFIEC	Federal Financial Institutions Examination Council
FIL	Financial Institution Letter
GLBA	Gramm-Leach-Bliley Act
IT	Information Technology
ITEC	Information Technology Examination Course
IT-MERIT	Information Technology Maximum Efficiency, Risk-Focused, Institution Targeted
IT-OJT	Information Technology On-the-Job Training
IT-RMP	Information Technology- Risk Management Program
OIG	Office of Inspector General
RDM	Regional Directors Memorandum
RM	Relationship Manager
ROE	Report of Examination
TSP	Technology Service Provider
URSIT	Uniform Rating System for Information Technology
U.S.C.	United States Code
ViSION	Virtual Supervisory Information on the Net

FDIC

Federal Deposit Insurance
3501 Fairfax Drive, Arlington, VA 22226

Office of Audits
Office of Inspector General

DATE: January 10, 2007

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

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

SUBJECT: *The Division of Supervision and Consumer Protection's Information Technology-Risk Management Program* (Report No. 07-002)

This report presents the results of our audit of the Division of Supervision and Consumer Protection's (DSC) procedures for addressing information technology (IT) security risks at FDIC-supervised financial institutions. To ensure that FDIC-supervised financial institutions implement adequate information security program controls, DSC conducts periodic onsite IT examinations generally in concert with its safety and soundness examinations.

The objective of the audit was to determine whether the FDIC had established and implemented adequate procedures for addressing IT security risks at FDIC-supervised financial institutions that offer electronic banking products and services. We focused this audit on DSC's Information Technology-Risk Management Program (IT-RMP), an examination process implemented in August 2005 and designed to review a financial institution's information security program and related risk-management practices.[1] Appendix I of this report discusses our audit objective, scope, and methodology in detail.

BACKGROUND

Information is one of a financial institution's most important assets. Protection of information assets is necessary to establish and maintain trust between the financial institution and its customers, maintain compliance with the law, and protect the reputation of the institution. Timely and reliable information is necessary to process transactions and support financial institution and customer decisions. A financial institution's earnings and capital can be adversely affected if information becomes known to unauthorized parties, is altered, or is not available when it is needed.

Information security is the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its

[1] The FDIC Office of Inspector General (OIG) is evaluating FDIC examiners' use of a subset of the IT-RMP examination procedures related to technology service providers (TSP). The results of that audit will be published in a separate report.

operations. On a broad scale, financial institutions have a primary role in protecting the nation's financial services infrastructure. The security of the financial institutions' systems and information is essential to their safety and soundness and to the privacy of customer information.

Organizations often inaccurately perceive information security as the state or condition of controls at a point in time. Security is an ongoing process, whereby the condition of a financial institution's controls is just one indicator of its overall security posture. Other indicators include the ability of the institution to continually assess its posture and react appropriately in the face of rapidly changing threats, technologies, and business conditions. A financial institution establishes and maintains effective information security when it continuously integrates processes, people, and technology to mitigate risk in accordance with risk assessment and acceptable risk-tolerance levels.

Interagency Guidelines Establishing Information Security Standards

Pursuant to section 39 of the Federal Deposit Insurance (FDI) Act, and sections 501 and 505(b) of the Gramm-Leach-Bliley Act (GLBA), the federal banking agencies issued *Interagency Guidelines Establishing Information Security Standards* (Guidelines). These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. The Guidelines require each financial institution to implement a comprehensive written information security program designed 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 such information that could result in substantial harm or inconvenience to any customer.

The Guidelines further require that the board of directors or an appropriate committee of the board of each financial institution:

- approve the financial institution's written information security program and
- oversee the development, implementation, and maintenance of the financial institution's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

FFIEC Information Security Booklet

In July 2006, the Federal Financial Institutions Examination Council (FFIEC) issued revised guidance for examiners and financial institutions in identifying information security risks and evaluating the adequacy of controls and applicable risk management practices of financial institutions. The *Information Security Booklet* is 1 of 12 that, in total, comprise the FFIEC *IT Examination Handbook*. The *Information Security Booklet* describes how an institution should protect and secure the systems and facilities that process and maintain information and builds on the Guidelines (discussed above) by providing additional and more detailed explanations of sound security-process elements. The booklet states that financial institutions and TSPs must maintain effective security programs tailored to the complexity of their operations. The July 2006 *Information Security Booklet* updated a 2002 version and addressed changes in technology, risk assessments, mitigation strategies, and regulatory guidance.

DSC's IT-Risk Management Program

DSC generally conducts IT examinations in conjunction with safety and soundness examinations every 12 or 18 months, depending on the asset size and financial condition of the institution. Institutions found to be in noncompliance with the Guidelines can face supervisory actions ranging from informal agreements to civil monetary penalties or other enforcement actions.

In 2005, DSC updated its risk-focused IT examination procedures for FDIC-supervised financial institutions. DSC issued a Regional Directors Memorandum (RDM), *Information Technology – Risk Management Program (IT-RMP)* on August 15, 2005, to implement the IT-RMP and related examination procedures (RDM 2005-031). The IT-RMP replaced the broad-based technology and control reviews conducted under the former IT-Maximum Efficiency, Risk Focused, Institution Targeted (IT-MERIT) program and related work programs with a top-down approach to assess the adequacy of an institution's information security program. 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 the FDIC's Relationship Manager Program[2] by including the results of the IT examination within the safety and soundness Report of Examination (ROE) for all FDIC-supervised financial institutions, regardless of size, technical complexity, or prior examination rating.

The Five Key Areas of Focus Under IT-RMP

- Risk Assessment
- Operations Security and Risk Management
- Audit and Independent Review
- Disaster Recovery and Business Continuity
- Compliance with Part 364, Appendix B, of the FDIC's Rules and Regulations

Source: RDM 2005-031.

[2] DSC implemented the Relationship Manager Program in September 2005. A key aspect of this program is the designation of a Relationship Manager (RM) for every FDIC-supervised financial institution. Each RM serves as the designated local point-of-contact for the respective financial institutions in their portfolio.

Key components of the IT-RMP include the following:

- **Technology Profile Script (Profile Script).** A mandatory tool used to measure the risk and complexity of technology deployed at an institution and to assess examination staffing needs. Examiners use the Profile Script, which contains 20 questions, to collect information about an institution's IT environment and, using a numeric scoring process, categorize institutions into one of three risk/complexity categories (Type I&II, III, or IV). The categories are also used to assign appropriately-qualified IT examiners to IT examinations. Together with the Officer's Questionnaire (see below) and other information, the Profile Script is used to develop an institution risk profile and preliminary examination scope.

Technology Profile Script Institution Types
Institutions for which IT examinations had been started and completed from January 1, 2006 to June 19, 2006: Type I&II – 328 institutions Type III – 385 institutions Type IV – 37 institutions

Source: OIG-prepared from DSC examination information.

- **IT Examination Officer's Questionnaire (Officer's Questionnaire).** A mandatory tool examiners use to collect key information about an institution's IT environment prior to conducting an IT examination. The questionnaire represents the financial institution's self-assessment of its information security program and contains 85 questions, generally in a "yes/no" format, targeting the 5 key areas of focus under IT-RMP. Information collected through the questionnaire is used with other relevant information to support risk analysis and scoping of IT examinations. The questionnaire must be signed by an executive-level management official of the institution attesting to its accuracy and completeness.

- **Flexible Use of Work Programs.** The IT-RMP introduced a new IT Snapshot Work Program (Work Program) and an IT Summary Analysis (Summary Analysis) that examiners must use to document IT examination findings and conclusions. Examiners may also use applicable FDIC- or FFIEC-approved work programs, FDIC Financial Institution Letters (FIL), or other regulatory guidance in conducting an examination. IT-RMP procedures provide examiners with considerable discretion in determining the scope of an IT examination.

- **IT Rating Guidelines.** Examiners assign a single "composite" rating at the conclusion of an IT examination using the Uniform Rating System for Information Technology (URSIT). The rating reflects "the effectiveness of an institution's IT risk management practices and the completeness of its information security program."[3] The URSIT ratings are discussed in the IT Composite Scoring section of this report.

Appendix II provides an overview of the IT-RMP examination procedures and illustrates the tools used in the various stages of an IT examination.

[3] On January 13, 1999, the FFIEC adopted a revised URSIT to be used for IT examinations of all banks and TSPs. The URSIT rating is based on a risk evaluation of four critical components, namely: (1) Audit, (2) Management, (3) Development and Acquisition, and (4) Support and Delivery.

RESULTS OF AUDIT

DSC has established procedures within the IT-RMP for addressing IT security risks at FDIC-supervised financial institutions. These procedures address most of the information security requirements contained in the Guidelines. Our review of 12 IT examinations found that examiners generally followed the procedures outlined in the IT-RMP, and in doing so, carried out the following activities:

- Identified the risks and technology deployed at the institution for the purpose of determining examination staffing needs.
- Reviewed the financial institution's Officer's Questionnaire regarding the bank's risk management practices.
- Performed onsite examination procedures to assess the financial institution's information security program.
- Assigned an IT composite rating at the conclusion of the examination and reported IT examination findings in the ROE.

However, improvements to the IT-RMP would help to ensure adequate and consistent implementation of the IT-RMP and related examination procedures. Specifically, DSC could revise certain IT-RMP tools to assist examiners in more effectively identifying relevant IT security risks to be assessed. We concluded that DSC could:

- Clarify in the IT-RMP guidance the purpose and use of the Profile Script or reevaluate the benefits of the continued use of this tool.
- Enhance the Officer's Questionnaire to address certain information security requirements contained in the Guidelines.
- Modify IT-RMP guidance to (a) replace some "yes/no" questions in the Officer's Questionnaire with more descriptive questions and (b) require that examiners evaluate, based on identified risks, a sample of positive responses to questions in the Officer's Questionnaire to ensure their accuracy.
- Expand instructions for the Summary Analysis to clarify the extent to which examiners should document an institution's risk profile and corresponding procedures to address risks **(IT-RMP Tools)**.

DSC also needs to update IT-RMP guidance to more clearly address the methodology examiners should use in deriving the IT composite rating for a financial institution. Clarified guidance could increase assurance that IT ratings accurately and consistently reflect the effectiveness of an institution's IT risk management practices and the completeness of its information security program **(IT Composite Scoring)**.

DSC is in the process of incorporating the IT-RMP approach into its examiner training courses. In doing so, DSC needs to better align the examiner training program with the top-down, risk-focused objective of the IT-RMP and consider expanding the program to ensure that more examiners are sufficiently trained to perform effective IT examinations (**Examiner IT Training**).

IT-RMP TOOLS

As described earlier, the IT-RMP includes key components for identifying and addressing IT risks at financial institutions: the Profile Script, Officer's Questionnaire, Work Program, and Summary Analysis. Improvements could be made to these tools to help examiners more effectively provide coverage of the most significant IT security risks.

Technology Profile Script

DSC needs to reevaluate the benefits of the Profile Script within the IT-RMP program. DSC designed the Profile Script under the former IT-MERIT examination program to be a standardized basic measurement of the complexity and risk of the technology deployed at a financial institution. The Profile Script was, and still is, the primary tool for categorizing financial institutions into risk/complexity categories (Type I&II, III, or IV). Under the previous IT-MERIT program, DSC used the Profile Script tool to:
(1) determine the examination work program,[4] report format, and rating format;
(2) allocate examination resources and match examiner skills to the complexity of the institution; and (3) determine training needs.

RDM 2005-031 states that, under the IT-RMP, the Profile Script "…will no longer dictate examiner scope, but should be used to assess examination staffing needs and changes to the financial institution's technology environment." The Profile Script consists of 20 questions in 4 categories – Core Processing, Networking, E-Banking, and Other. Seventeen of the questions have a 5-point value, and the remaining three questions are valued at 10, 15, or 20 points. The total points of all four categories are added together to derive a financial institution's profile score, as shown in the Technology Profile Scoring Matrix. The resulting category or type is one factor that DSC considers in determining the appropriate examiner training and skill level needed to perform the IT examination, as illustrated in the FDIC's *IT Examination Resource Strategy Matrix* shown in Appendix III of this report.

Technology Profile Scoring Matrix

Type	Score Range
I&II	0-49
III	50-79
IV	80-130

Source: RDM 2005-031.

Although DSC refocused the use of the Profile Script, DSC elected not to revise the content of the tool. For example, the Profile Script used for the IT-RMP, an IT risk-management-focused program, contains the identical questions and scoring matrix used in the previous IT-MERIT program, which was technology-based. Further, each financial institution continues to be categorized by type, using the existing Technology Profile Scoring Matrix. In addition, although the IT-RMP program description and requirements state that the Profile Script will no longer dictate the examination scope, IT-RMP examination procedures in RDM 005-031 provide that the Profile Script will be

[4] Under the IT-MERIT examination program, examiners were required to use the following work programs: (a) Type I institutions – IT-MERIT Procedures, (b) Type II institutions – IT General Work Program, (c) Type III institutions – IT General Work Program supplemented by FFIEC work programs, and (d) Type IV institutions – FFIEC work programs.

used as a scoping tool in concert with the Officer's Questionnaire and other information obtained prior to onsite work in developing an institution's risk profile.

DSC examination personnel commented on the usefulness of the Profile Script. Some examiners noted that the Profile Script may no longer be necessary because the IT-RMP is used for all financial institutions, regardless of a financial institution's risk category (Type I & II, III, or IV), thus the tool is not needed for establishing the examination work program. In regard to using the Profile Script to assess examination staffing requirements with the current scoring system, some examination personnel believed that a wide range of financial institutions fall into the Type III category and that some Type III banks may not need an experienced IT examiner to conduct the IT examination. One DSC official said that the Profile Script is useful, but added that it should be updated to reflect risks related to institutions that offer credit-card processing or utilize *FedLine Advantage*.[5] Another DSC official stated that the Profile Script focuses on technology, and the training identified in the *IT Examination Resource Strategy Matrix* (Appendix III) is technology-focused; however, IT-RMP is management-focused.

Most of the information in the Profile Script is also reflected in the Officer's Questionnaire and Work Program. For example, three of the four categories in the Profile Script – Core Processing, Networking, and E-Banking – are addressed in the *Part 2 – Operations Security and Risk Management* section of the Officer's Questionnaire. The FDIC could consider using the information in the Officer's Questionnaire for IT examination scoping and staffing decisions rather than continuing to require that examination personnel complete the Profile Script. A DSC official estimated that examination personnel spend 1 hour preparing the Profile Script, which would equate to about 757 hours that could have been expended for the IT examinations started and completed for the first 6 months of 2006.[6]

DSC should either clarify the new purpose and use of the Profile Script in the IT-RMP or reevaluate the need for continued use of the Profile Script. Since DSC currently relies on Profile Script information to determine examination staffing, clarifying the tool's intended purpose and utilization in the IT-RMP could increase the FDIC's assurance that IT examiner skills and experience are commensurate with the risks associated with a particular institution. However, given that similar information is already reflected in the Officer's Questionnaire, DSC may be in a position to eliminate preparation of the Profile Script. Finally, re-evaluating the utility of the Profile Script as a scoping and staffing tool could result in time-saving opportunities for IT-RMP examinations.

[5] *FedLine Advantage* is the Federal Reserve Bank's electronic delivery channel, which uses Web technologies to provide financial institutions access to critical payment systems, including Fedwire Funds Service, Fedwire Securities Service, and FedACH (Automated Clearing House).

[6] These results comprise all DSC IT examinations started and completed during the period January 1, 2006 to June 20, 2006 for which a Profile Script had been entered into the Virtual Supervisory Information On the Net (ViSION) system, based on data collected from ViSION on June 21, 2006.

IT Examination Officer's Questionnaire (Officer's Questionnaire)

DSC could enhance the Officer's Questionnaire by including additional information security risks for IT examiners' assessments. 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. The Officer's Questionnaire contains 85 questions for the financial institution to answer in the IT-RMP's key areas: (1) risk assessment; (2) operations security and risk management; (3) audit and independent review; (4) disaster recovery and business continuity; and (5) compliance with Part 364, Appendix B, of the FDIC's Rules and Regulations.

The Officer's Questionnaire includes most, but not all, of the relevant information security requirements contained in the FFIEC's *Information Security Booklet*. We compared the IT-RMP guidance with the *Information Security Booklet* and identified certain areas for which the Officer's Questionnaire coverage could be more complete, as follows:

Identification of vulnerabilities as part of the risk assessment process: The *Information Security Booklet* states that financial institutions should assess potential threats and vulnerabilities of their information systems. Vulnerabilities can be characterized as weaknesses in a system, or control gaps, that, if exploited, could result in the unauthorized disclosure, misuse, alteration, or destruction of information or information systems. The Officer's Questionnaire does not specifically require that the financial institution official provide information on vulnerabilities identified as part of the institution's risk assessment process. The Officer's Questionnaire requires only a "yes" or "no" response on whether vulnerability testing had been performed on internal systems and the date and by whom the testing had been performed but not the results of the vulnerability testing.

Benchmarks and security performance metrics for the information security program: The *Information Security Booklet* provides that performance metrics can be used to measure security policy implementation, the effectiveness and efficiency of security services delivery, and the impact of security events on business processes. The measurement of security characteristics can allow management to increase control and drive improvements to the security process. The Officer's Questionnaire does not address the financial institution's establishment or monitoring of security performance metrics and benchmarks.

Access controls over customer information systems: The *Information Security Booklet* states that the goal of access control is to allow access by authorized individuals[7] and devices[8] and to disallow access to all others. The booklet also states that financial

[7] Authorized individuals may be institution and TSP employees, vendors, contractors, customers, or visitors. Access should be authorized and provided only to individuals whose identity is established, and their activities should be limited to the minimum required for business purposes.

[8] Authorized devices are those whose placement on the network is approved in accordance with institution policy.

institutions should have an effective process to administer access rights. The Officer's Questionnaire does not address certain aspects of access controls over customer information systems, such as: developing security strategies to limit unauthorized access and the ability to perform unauthorized actions; implementing least privilege concepts to restrict access to those with proper authorization; and establishing multiple control points between threats and organization assets by layering controls.

Encryption of electronic customer information: The *Information Security Booklet* states that financial institutions should use effective authentication methods to include encrypting the transmission and storage of authenticators, such as passwords, personal identification numbers, and digital certificates. The Officer's Questionnaire has no questions related to encryption.

Insurance coverage: The *Information Security Booklet* states that financial institutions should carefully evaluate the extent and availability of insurance coverage in relation to the specific IT risks that institutions are seeking to mitigate. Insurance may include coverage for the following risks – vandalism of financial institution Web sites; computer extortion associated with threats of attack or disclosure of data; theft of confidential information; destruction or manipulation of data (including viruses); and insiders who exceed system authorization. The Officer's Questionnaire has no questions related to insurance. However, DSC officials stated that questions related to insurance may already be addressed through safety and soundness examinations.

Personnel security: The *Information Security Booklet* states that financial institutions should mitigate the risks posed by internal users of bank data by: (1) performing appropriate background checks and screening of new employees; (2) obtaining agreements covering confidentiality, nondisclosure, and authorized use; (3) using job descriptions, employment agreements, and training to increase accountability for security; and (4) providing training to support awareness and policy compliance. DSC officials pointed out that two questions addressed personnel security controls: (1) Do you have an employee acceptable use policy (Y/N)?, and (2) Do you have an employee security awareness training program (Y/N)? However, we noted that the Officer's Questionnaire does not address certain personnel security areas such as background checks and confidentiality agreements for key individuals holding positions critical to the implementation and oversight of the institution's information security program.

Senior DSC officials responsible for the IT-RMP told us that the program has been in place for 1 year and is ready for review and revisions, as necessary. DSC plans to obtain input and suggestions for improvements to the IT-RMP from IT Assistant Regional Directors' quarterly meetings, the division's internal review reports, IT examiners, and OIG reviews.

Yes/No Format of Officer's Questionnaire: DSC should also consider rephrasing the questions in the Officer's Questionnaire to improve the IT-RMP and related examination procedures. Specifically, the "yes/no" format design of some questions in the Questionnaire does not always provide IT examiners meaningful information on which to base risk-focused examination procedures or prompt the financial institution to provide detailed information in the response. Several of the questions were designed to determine not only whether a policy or procedure existed, but also whether that policy or procedure was compliant or consistent with established criteria. For example, one question asks "Does the scope of your risk assessment include an analysis of internal and external threats to confidential customer and consumer information as described in Part 364, Appendix B, of the FDIC's Rules and Regulations (Y/N)?" Such a question is designed to obtain information related to the adequacy or completeness of a control or requirement. IT examiners could obtain more meaningful information during examination planning if certain questions were rephrased to address an institution's compliance or consistency with specific regulations and guidance as shown below.

Current Question: "Do you have an anti-spyware management program to protect end-user systems (Y/N)?"

OIG-Proposed Question: Describe the institution's policies, procedures, and practices for preventing and detecting spyware on computer systems consistent with the FDIC's FIL-66-2005, *Guidance on Mitigating Risks from Spyware*, dated July 22, 2005. Spyware is a commonly-used term to describe software that collects data without the prior knowledge or informed consent of the data's owner.

Current Question: "Do you have policies/procedures for the proper disposal of information assets (Y/N)?"

OIG-Proposed Question: Describe the institution's policies, procedures, and practices for disposing of information assets consistent with the *Interagency Guidelines Establishing Information Security Standards*.

IT Snapshot Work Program (Work Program)

RDM 2005-031 directs examiners to use the Officer's Questionnaire as a risk analysis and scoping tool for quickly identifying potential security program strengths and weaknesses. The memorandum states that examiners should always evaluate all responses to the Officer's Questionnaire in the context of effective IT risk management, keeping in mind the potential severity, impact, and relationship of any "No" or blank response to other responses in the same and other risk management categories, and paying particular attention to responses that could affect the quality of the entire information security program. Examiners may choose not to document "No" or blank responses, provided the reason(s) for the scope adjustment or modification is documented in the Summary Analysis (discussed in the next section of this report).

RDM 2005-031 does not specifically require examiners to evaluate "Yes" responses. Rather, the guidance identifies the "No" responses as potential "red flag indicators" and describes "Yes" responses as being equally important when evaluating the adequacy and effectiveness of a financial institution's information security program. Examiners we interviewed indicated that bankers have an inferred bias toward answering "Yes" to questions on the Officer's Questionnaire because they know that the "No" answers could be construed as an indication of a problem.

For all 12 IT examinations we reviewed, the examiners followed up on selected "Yes" responses from the Officer's Questionnaire. However, for all 12 examinations reviewed, we could not determine why certain "Yes" responses had been selected for additional procedures, because examiners did not discuss the reason why in the examination scope. Further, for 6 of the 12 examinations, we could not determine which procedures had been completed to follow up on certain "Yes" responses, because examiners did not identify these procedures in the Work Program comments or discuss them in the examination scope.

In making changes to the IT-RMP, DSC should consider revising RDM 2005-031 to include a provision that examiners evaluate, based on identified risks, a sample of "Yes" responses contained in the Officer's Questionnaire. Requiring validation of selected "Yes" responses during the onsite discussion and verification phase of the examination would provide the FDIC with additional assurance as to the adequacy of the financial institution's information security program. Also, this action could further assure the FDIC that the institution official completing the questionnaire was informed and knowledgeable about the information security program. Follow-up activity on IT areas considered higher risk or selected "yes" responses related to specifically-identified IT security risks would be consistent with the risk-focused approach of the IT-RMP examination procedures.

IT Summary Analysis (Summary Analysis)

DSC could clarify its expectations of what information examiners should document in the Summary Analysis. The Summary Analysis has two primary purposes: (1) scope development that includes preparing a preliminary institution risk profile from historical information and information gathered with other risk scoping tools, such as the Profile Script and the Officer's Questionnaire, and (2) report preparation that begins with documenting the IT examination findings in the Summary Analysis. IT-RMP examination procedures make the following references to an institution's risk profile:

- The completed Profile Script, Officer's Questionnaire, and other pre-examination information should help examiners gain an understanding of bank operations and supporting infrastructure. The goal of this process is to develop a preliminary institution risk profile based on historical and other information obtained during the preplanning phase.
- An institution's risk profile should consider risk management, technical, and other components.
- After completing the scoping process, examiners should have a reasonable understanding of the institution's risk profile and, therefore, have a tentative list of items to be reviewed during the onsite examination.

Although RDM 2005-031 requires that examiners develop a preliminary institution risk profile as part of completing the Summary Analysis, the memorandum does not specifically require that examiners document the risk profile. Further, RDM 2005-031 does not clearly identify what information should be included in a risk profile.

RDM 2005-031 states that for initial examinations under the IT-RMP, the examination scope will include, at a minimum, the procedures shown here. IT examiners are instructed to document the pre-planned examination scope under the "Initial Examination Scope" heading of the Summary Analysis and scope changes that occur during the examination in the "Final Examination Scope" section of this tool.

Minimum IT-RMP Exam Procedures

- Site security inspection
- Risk assessment review
- Audit/independent review
- Part 364 review
- Onsite discussion or verification of all "N," blank, "N/A," and "None" responses
- ACH and wire transfer review

Source: RDM 2005-031.

We reviewed the Summary Analysis document for each of the 12 sampled IT examinations to determine the IT security risks that examiners had identified for the financial institutions. For our analysis, we used information from DSC's IT-RMP training presentations and three case studies to determine what type of information should be included in a risk profile. We identified the following key scoping elements in the Summary Analysis section that could be used to present an institution's risk profile.

Scoping Elements Related to Risk Profiling

Summary Analysis Section	Key Scoping Elements
Pre-Examination Information	-- Service Providers and Technologies Used. -- Services and Products Offered. -- Bank Ownership and Structure. -- Prior Examination Results, Ratings, and Status of Findings. -- Changes in Technologies, Personnel, Products, Services, Auditors, and Service Providers. -- Enforcement Actions Outstanding. -- Other Risks Identified Through Officer's Questionnaire Responses.
Initial Examination Scope Comments	-- IT-RMP Minimum (Mandatory) Procedures for Baseline Scope. -- Pre-examination Information Items for Initial Discussions with Management and Direction for Onsite Work.
Final Examination Scope Comments (if different from initial scope)	-- Changes in Risk and Testing Based on Results of Executing Initial Examination Scope.

Source: IT-RMP Train-the-Trainer Course Materials.

The Summary Analysis for all 12 IT examinations we reviewed contained certain elements of an institution risk profile shown in the table above; however, these elements were not consistently captured for each examination. With respect to IT-RMP minimum procedures, we found that the examiners did not identify all of the minimum-required procedures in the Summary Analysis scope comments for 5 of the 12 examinations that we reviewed. However, in all five instances, examination working papers indicated that the minimum procedures had been performed.

The risk profile is an important tool that can help an examiner in assessing a financial institution's IT security risk management program and directing examiner resources toward examining areas in the financial institution with higher degrees of risk. Senior DSC officials responsible for the IT-RMP agreed that examiners should document the institution's risk profile and the examination procedures planned and performed to address identified risks. Doing so would provide greater assurance that the IT examination procedures are risk-focused and prioritized and reflect the most effective use of examiner resources. Moreover, a well-documented risk profile could serve as a baseline for determining IT changes to an institution's technology environment during future IT examinations.

RECOMMENDATIONS

We recommend that the Director, DSC:

1. Modify the IT-RMP guidance to clarify the purpose and use of the Technology Profile Script as distinguished from its previous utilization under the IT-MERIT program, or reevaluate the costs and benefits of the continued use of this tool.

2. Modify the IT Examination Officer's Questionnaire and IT Snapshot Work Program to provide for enhanced coverage of the following:
   - Identification of vulnerabilities as part of the risk assessment process.
   - Establishment of benchmarks and performance metrics for the information security program.
   - Access controls for customer information systems.
   - Encryption of electronic customer information.
   - Insurance coverage.
   - Personnel security.

3. Modify IT-RMP guidance to (a) replace some "yes/no" questions in the Officer's Questionnaire with more descriptive questions that will facilitate risk analysis and scoping IT examinations and (b) require that examiners evaluate, based on identified risks, a sample of positive responses to the questions in the Officer's Questionnaire to ensure their accuracy.

4. Modify IT-RMP guidance to clarify (a) what information should be included in an institution's risk profile and (b) the extent to which examiners should document the risk profile and corresponding procedures planned and performed to address identified risks.

IT COMPOSITE SCORING

For the 12 IT examinations we sampled, examiners had employed different methodologies when assigning an IT composite rating.[9] Presently, RDM 2005-031 and examiner training provide high-level guidance on the assignment of IT composite ratings used to classify IT examination results rather than detailed guidelines on developing the ratings. DSC could enhance IT-RMP guidance to provide for a clearer correlation between the IT composite rating definitions and the results of IT examination procedures performed in the Work Program. Additional guidance could increase the FDIC's assurance that IT composite ratings assigned to financial institutions consistently reflect the information security environment of the financial institutions examined. Comparability of IT composite rating data also improves DSC's ability to use that data for trend analysis and performance measurement purposes.

The URSIT stipulates that a direct relationship exists between the composite rating and the individual Audit, Management, Development and Acquisition, and Support and Delivery (AMDS) component performance ratings but adds that the composite rating is not a mathematical average of the individual components, and examiner judgment is used to weigh the relative risk of the examination results for each component. Accordingly, a poor rating in one component may influence the overall composite rating for an institution. For example, if the audit function of a financial institution is viewed as inadequate, the overall integrity of the IT systems is not readily verifiable. The URSIT suggests in this case that a composite rating of less than satisfactory ("3," "4," or "5") would normally be appropriate.

According to the URSIT, a principal purpose of the composite rating is to identify those financial institutions and service providers that pose an inordinate amount of IT risk and warrant special supervisory attention. Thus, individual risk exposures that more explicitly affect the viability of the organization and/or its customers should be given more weight in the composite rating. In determining a composite rating, an examiner also considers assessment factors such as (1) the significance of existing IT weaknesses, (2) the adequacy of risk management practices, and (3) the sufficiency of strategic planning. The URSIT rating definitions provide descriptive examples for each of the "1" to "5" composite ratings. For example, a composite "1" definition states that the financial institution has strong performance in every respect; generally has components rated "1" or "2"; and exhibits (a) minor IT weaknesses, (b) risk management processes that provide a comprehensive program to identify and monitor risk, (c) well-defined strategic plans, (d) prompt management identification of weaknesses, and (e) the strong financial condition and performance of the service provider. Appendix IV contains the FFIEC URSIT composite ratings definitions.

[9] The composite ratings are assigned on a scale of "1" to "5." A rating of "1" indicates the strongest performance and management practices and the least degree of supervisory concern, while a rating of "5" indicates the weakest performance and management practices and, therefore, the highest degree of supervisory concern.

Under the IT-RMP, DSC eliminated the assignment of IT component ratings but elected to retain the use of the URSIT rating definitions for assigning an IT composite rating to a financial institution.[10] Specifically, RDM 2005-031 provides that (1) the examiner will assign a composite rating at the conclusion of the examination using the URSIT rating definitions, and (2) the assigned composite rating will reflect the effectiveness of a financial institution's IT risk management practices and the completeness of its information security program as documented in the Work Program. However, according to RDM 2005-031, while risk management is the focus of the IT-RMP, coverage of existing URSIT component ratings is preserved. DSC is still required to develop the component ratings during certain IT examinations.

IT Composite Ratings Definitions and Development

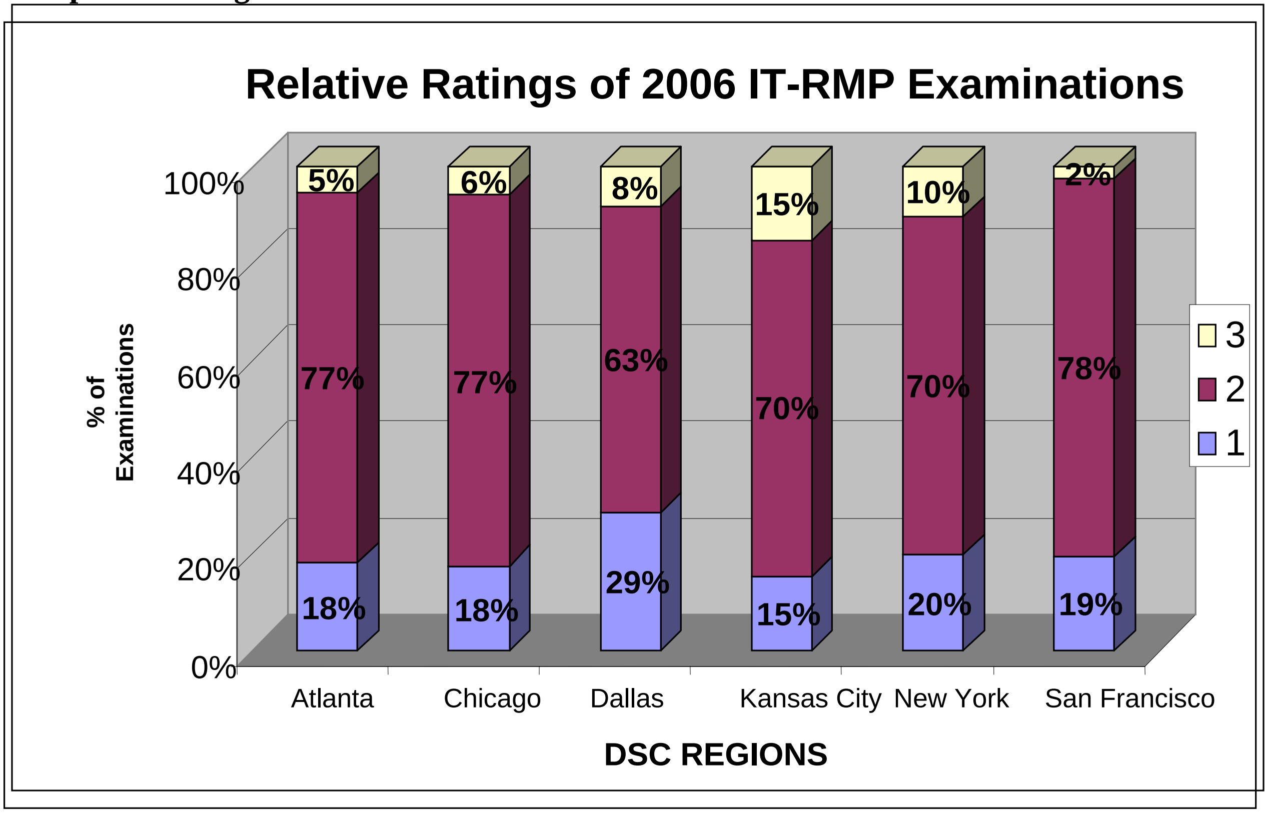
Examiners who conducted the 12 IT examinations in our sample used different approaches to develop the IT composite rating. Examiners for 8 of the 12 examinations we reviewed indicated that they had used the URSIT component methodology for developing the composite ratings. Examiners for the remaining four examinations indicated they had used a less structured method. For example, in one case, the rating decision was based on the significance of the findings identified.

DSC could clarify RDM 2005-031 guidance that states "coverage of existing FFIEC component ratings is preserved." It is not clear whether this statement requires the examiner to develop a ratings analysis using the URSIT component methodology or whether it is a general comment on information that could be considered by the examiner. Although the IT General Work Program is aligned to the four IT component rating categories, examiners are not required to complete this work program under the IT-RMP. In addition, RDM 2005-031 could more clearly explain the correlation between IT examination procedures and the assessment factors in the URSIT composite rating definitions. To illustrate, the Snapshot Work Program has only one general procedure that directly references strategic planning. However, strategic planning is specifically addressed as a key element in the URSIT composite rating definitions. Additional guidance on other IT-RMP procedures that relate to the strategic planning analysis could help ensure that this element (strategic planning) is consistently evaluated.

Consistency in developing IT composite ratings could enhance DSC's ability to use the results of its examinations activities for trend analysis or performance measurement purposes. The following figure identifies the IT composite rating results for FDIC IT examinations performed during the first half of 2006.

[10] IT component ratings will continue to be developed for examinations of TSPs.

Composite Ratings for FDIC IT Examinations Conducted in the First Half of 2006



Source: OIG review of ViSION data.
Note: The data in the figure comprise all DSC IT examinations started and completed during the period January 1, 2006 to June 19, 2006.

As shown, there are differences in the percentages of institutions rated “1,” “2,” or “3” among the regions. This information could be important to DSC in analyzing trends and assessing IT risks. However, for such information to be useful, it is important to ensure that composite rating determinations are consistently developed among examiners. It should be noted that other factors may be causing or contributing to the differences noted in the figure above, including variations in the population of financial institutions supervised by each region.

Moreover, the figure shows that the majority of financial institutions were assigned an IT composite rating of “2.” The URSIT definition indicates that a financial institution with a “2” rating exhibits safe and sound performance but may demonstrate modest weaknesses in operating performance, monitoring, management processes, or system development. ROEs for banks in our sample with an IT composite rating of “2” referred to the bank’s IT program as “adequate” or “satisfactory.” Given the level of assurance conveyed for the bank’s risk management and security processes by a “2” rating, it is important that the process for developing this rating be clearly defined and consistently implemented.

IT Rating Documentation

RDM 2005-031 and IT-RMP training presentations we reviewed do not address whether the IT composite ratings analysis should be documented in the examination workpapers to show how the examiners (1) considered the assessment factors in the URSIT composite rating definitions or (2) weighted various examination findings in the development of the composite rating. None of the examination workpapers for the 12 sampled examinations clearly documented how the composite rating had been determined. Examiners are no longer required to assign URSIT component ratings, which, in part, provide a standard means by which examiners can support how they developed a composite rating. Absent such a requirement, it is important that examiners follow a consistent, documented approach in making composite rating determinations.

RECOMMENDATION

We recommend that the Director, DSC:

5. Develop additional IT-RMP guidance to provide a consistent approach to developing and documenting a financial institution's IT composite rating analysis. Guidance should clearly describe the correlation between the IT-RMP examination procedures and results and the FFIEC URSIT composite ratings definitions.

EXAMINER IT TRAINING

DSC is in the process of incorporating some of the elements of the IT-RMP into examiner training courses, but the current training program could be better aligned to the top-down, risk-focused objective of the IT-RMP. Additionally, the current IT examiner training program could be expanded to provide non-IT examiners who are assigned to conduct IT examinations with the opportunity for periodic on-the-job training at financial institutions. These training program improvements would provide the FDIC with greater assurance that IT examiners are well-prepared to effectively conduct IT examinations.

Alignment of IT-RMP Training

The IT examiner training program is primarily focused on technical subjects,[11] yet the IT-RMP approach places considerable emphasis on bank management, information security program content, and confirmation and assurances through audit or independent review. DSC provides examiner IT training through formal classroom and online training and a formal IT-OJT program for IT specialty examiners. RDM 2005-031 includes an *IT Examination Resource Strategy Matrix*, which recommends examiner skills and training required for the particular category, or type, of financial institution determined by the Profile Script. The matrix is included in Appendix III of this report. DSC used the same

[11] Examples of technical subjects include the IT examiner conference, transmission control protocol/Internet protocol, operating system platforms, firewalls, intrusion detection system, and virtual private network.

matrix under the previous IT-MERIT program but has not revised the matrix to reflect the new management-centric approach of the IT-RMP.

DSC's examiner IT training curriculum could be strengthened by including specific courses that address business risk in an IT environment and prepare the examiner to:

- identify and assess risk management deficiencies in a financial institution's information security program,
- prepare a written risk profile of a financial institution, and
- prepare the IT examination scope that is justified by the institution's risk profile.

With a training curriculum aligned to the objective of IT-RMP, examiners conducting IT examinations would be better prepared to risk-focus the examination to the identified business risks of the financial institution, rather than just the technical risks. In turn, the FDIC would have greater assurance that the examination procedures conducted thoroughly cover the management of a financial institution's information security program. DSC has initiated training in audit, business continuity, and risk assessment and indicated that examiners have been requesting additional management-focused training.

IT On-the-Job Training (IT-OJT) for Non-IT Examiners

DSC needs to consider expanding its IT-OJT program to provide DSC examiners with more periodic exposure to financial institution IT environments. The IT-OJT program and many of the IT training courses are geared to more experienced IT specialty examiners. However, commissioned examiners who are not designated IT specialty examiners may also conduct IT examinations, thus these examiners could benefit from the IT-OJT program.

Commissioned DSC examiners submit applications to participate in the IT-OJT. This program prepares safety and soundness examiners to conduct IT examinations of more technologically-complex institutions. DSC assigns the less technologically complex financial institutions having a lower risk profile to non-IT examiners who may have completed certain basic IT training. DSC has stated that a positive attribute of IT-RMP is that safety and soundness examiners would be competent to conduct IT examinations at financial institutions that fall into the Type I & II category, once these examiners have completed the requisite basic IT training. However, 16 of the 45 regional and field office personnel we interviewed expressed concern that less-experienced examiners conducting IT examinations may not always know when to ask specific questions in order to "drill down" from summary information to more detailed data that is needed to adequately assess an institution's information security program.

Moreover, some questions in the Officer's Questionnaire require the examiner to possess an in-depth understanding of core processing, networks, and telecommunications. For example, Part 2.f, *Operations Security and Risk Management*, of the Officer's Questionnaire and Work Program, asks, "Do you have formal configuration, change management, and patch management procedures for all applicable platforms identified?" Part 3.d, *Audit/Independent Review Program,* asks, "Does audit coverage include a comparison of actual system configurations to documented/baseline configuration standards?" These two questions require the examiner to understand formal configuration standards, policies, and procedures for identified platforms and to understand the audit coverage for system configurations. Without this level of understanding, the examiner would not be able to determine whether the configuration management procedures and audit program are adequate.

In the area of IT-RMP training, DSC: (1) provided an overview briefing to IT examiners in August 2005; (2) presented to certain specialty IT examiners an introduction to the IT-RMP "train-the-trainer" course in December 2005 through February 2006; and (3) awarded a contract to amend examiner course content and develop a course focused on risk assessments, business continuity, and audit. IT-RMP program implementation preceded the training by several months, and in certain cases, the risk-focused course offerings have been scheduled only for future dates.

DSC examiners we interviewed consistently identified the need to get examiners into the IT-OJT program. We estimated that 97 percent (733 of 757) of the financial institutions examined during the first half of 2006 use networks in their operations.[12] This illustrates a need for a larger and specialized cadre of examiners capable of (1) conducting all levels of IT examinations, and (2) coaching and training participants in the IT-OJT program.

Although DSC has made some progress in aligning the examiner training program to the objective of the IT-RMP, with additional enhancements to the IT training program, the FDIC would have greater assurance that examiners are sufficiently prepared to conduct effective IT examinations.

RECOMMENDATIONS

We recommend that the Director, DSC:

6. Revise DSC examiner training for conducting IT examinations to align with the objective of the IT-RMP.

7. Initiate efforts to increase the number of non-IT examiners who participate in IT-OJT examination training to increase DSC's overall capability to conduct IT examinations.

[12] These results comprise all DSC IT examinations started and completed during the period January 1, 2006 to June 20, 2006 for which a Technology Profile Script had been entered into ViSION, based on data collected from ViSION on June 21, 2006.

CORPORATION COMMENTS AND OIG EVALUATION

On January 4, 2007, the Director, DSC, provided a written response, dated December 12, 2006, to a draft of this report. DSC's response is presented in its entirety as Appendix V to this report. DSC generally agreed with our recommendations, noting that it has plans to evaluate the first-year implementation of the August 2005 revision of the IT-RMP. With regard to the IT-RMP tools and guidance, DSC will incorporate OIG recommendations into its evaluation and issue revised guidance as deemed necessary. With regard to DSC's IT training programs, DSC will review its training processes and determine whether enhancements are needed. DSC plans to complete these actions by September 30, 2007.

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

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this audit was to determine whether the FDIC had established and implemented adequate procedures for addressing IT security risks at FDIC-supervised financial institutions that offer electronic banking products and services. We conducted our audit in accordance with generally accepted government auditing standards during the period December 2005 through September 2006.

Scope and Methodology

The scope of the audit focused on assessing the guidance and procedures that supported the implementation of the top-down, risk-focused objective of the IT-RMP for IT examinations of FDIC-supervised institutions. We performed the following:

- Evaluated the IT-RMP procedures for assessing IT security risks and examining IT security programs, detailed in RDM 2005-031, *Information Technology-Risk Management Program (IT-RMP)*, for consistency with applicable laws, regulations, and other guidelines related to IT security. Other guidelines included the FFIEC's *Information Security Booklet* (December 2002 and July 2006 revisions), 1 of 12 booklets, that, in total, comprise the *FFIEC Information Technology (IT) Examination Handbook*.
- Interviewed DSC personnel responsible for development and oversight of the IT-RMP and the subsequent training on the IT-RMP.
- Interviewed DSC personnel involved with DSC activities related to monitoring new and emerging technologies.
- Interviewed other regional DSC personnel involved with the IT-RMP implementation, including DSC IT Assistant Regional Directors and IT Examination Specialists.
- Reviewed the management information system reports used by the FDIC in its self-assessment of the IT examination program.

We selected a judgmental sample of 12 examinations from a total of 292 examinations conducted during the period January 2006 through March 2006, consisting of 4 examinations conducted in the New York Region, 4 in the San Francisco Region, and 4 in the Kansas City Region. To select our sample, we performed the following.

- Stratified the population of examinations conducted during our period of review by the following areas: (1) the existence of a transactional Web site within the financial institution, (2) DSC region, (3) TPS risk type, (4) URSIT composite rating, (5) total Profile Script score (a measure of complexity and thus risk), and (6) institution asset size as of December 31, 2005.
- Considered transactional Web capability and a high-total Profile Script score to be indicative of key information security risk factors.

- Considered the URSIT composite rating and institution asset size to be reflective of the relative potential impact of those risk factors.
- Considered only banks with transactional Web sites and Profile Script risks types I-II or III for selection.

Because of the size, complexity, and visibility of financial institutions with a Profile Script risk type IV, we concluded there was a lower risk that they may not receive an appropriate level of supervisory review, and thus, did not include financial institutions with a Profile Script risk type IV in our sample.

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 that we should consider in selecting our sample. We incorporated these suggestions as appropriate, and performed the following audit steps:

- reviewed ROEs and supporting working paper documentation for the 12 sampled examinations to evaluate consistency with the IT-RMP, and
- interviewed regional and field office DSC personnel responsible for implementing the IT-RMP for the sampled IT examinations, including IT examiners.

Internal Controls

We gained an understanding of relevant internal controls by reviewing: (1) FDIC policies and procedures, such as Regional Directors Memoranda, related to the IT-RMP; (2) the IT examiner training curriculum; (3) FDIC procedures for assessing the adequacy of IT examination work; and (4) available FDIC documentation regarding the implementation of IT examination and supervision procedures. In addition, we interviewed DSC individuals involved in IT examinations, supervision, and IT training activities.

Reliance on Computer-Based Data

We obtained certain data from DSC's ViSION system to identify IT examinations conducted subsequent to the August 15, 2005 implementation of the IT-RMP and to provide historical data on the Profile Script scores and IT composite ratings for those examinations. 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*, the *FDIC 2005 Annual Performance Plan*, 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 2005 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.

The *FDIC 2006 Annual Performance Plan* includes similar means and strategies information and adds that, in regard to training, 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 reviewed the FDIC's *Corporate Performance Objectives* (CPO) for 2005 and 2006. We determined that none of the 2005 or 2006 CPOs directly relate to the IT-RMP. However, two CPO goals indirectly relate to IT examinations:

- Enhance the FDIC's ability to manage its insurance risk to include ensuring that the supervision program effectively identifies and mitigates risk (as stated in the 2006 CPO).
- Continue to improve the FDIC's risk management and compliance examination programs by implementing the Relationship Manager Program (2005 CPO) and enhancing the data security examination program for TSPs (2006 CPO).

We also reviewed DSC's 2006 Division Objectives and identified an action to update the Directors' College ROE workshop and develop an Advanced Director's College. The planned action states that the ROE update will include IT and compliance ratings and corresponding comments.

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 objective. However, throughout the audit, we were sensitive to the potential for fraud, waste, abuse, and mismanagement.

Laws and Regulations

In conducting the audit, we considered the following laws, rules, and regulations.

- **Gramm-Leach-Bliley Act.** GLBA (15 United States Code (U.S.C.) §6801) 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 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 that could result in substantial harm or inconvenience to any customer.
- **Fair and Accurate Credit Transactions Act of 2003 (FACT Act).** This Act amends the Fair Credit Reporting Act (15 U.S.C. §1681) by adding provisions covering identity theft, consumers' access to credit information, enhanced consumer report accuracy, and financial literacy.
- **FDI Act Section 10 - Provisions Related to Examination Authority.** The FDI Act requires the FDIC to perform periodic "full scope" examinations of banks. There is no specific requirement in the Act for the performance of IT examinations; however, they are considered to be intended as part of the "full scope" provision.
- **FDIC Rules and Regulations Part 364, Appendix B - Interagency Guidelines Establishing Information Security Standards (Including Supplement A).** These guidelines establish standards for financial institution information security programs, including administrative, technical, and physical safeguards; measures to properly dispose of consumer information; and elements of a financial institution's response program to address unauthorized access to, or use of, customer information, including customer notification procedures.[13]

Prior Audit Coverage

The OIG has conducted several prior audits on the FDIC's IT examination procedures and related efforts to protect sensitive customer information.

[13] 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.

- **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 to help the FDIC: (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. 06-009,** ***FDIC's Guidance to Institutions and Examiners for Implementing the Gramm-Leach-Bliley Act Title V and the Fair and Accurate Credit Transactions Act*****, issued February 24, 2006.** The objective was to determine whether the FDIC provided adequate guidance to FDIC-supervised institutions and examiners for implementing the data privacy and security provisions of the GLBA Title V and FACT Act. We recommended that the FDIC finalize the interim examination guidance that addresses FACT Act provisions and develop, in coordination with the joint-agency rulemaking committee, a more aggressive project management plan to expedite the issuance of final rules and regulations for all FACT Act provisions. DSC's responses and proposed actions were sufficient to resolve each recommendation.

- **Audit Report No. 04-022,** ***FDIC's Information Technology Examination Program,*** **issued June 15, 2004.** The objective of this audit was to determine whether the FDIC's IT examinations provided reasonable assurance that IT risks were being addressed by the risk management programs in FDIC-supervised financial institutions. The audit also determined whether the FDIC had implemented GLBA-related recommendations in OIG Audit Report No. 03-044, *The Federal Deposit Insurance Corporation's Progress in Implementing the Gramm-Leach-Bliley Act, Title V – Privacy Provisions,* dated September 26, 2003. We recommended that DSC institute a standardized quality review of all phases of the IT examination process and supporting documentation prior to issuance of IT examination results. DSC's responses and proposed actions were sufficient to resolve the recommendation.

IT-RMP EXAMINATION STEPS

Step	Procedure	Tool Used
#1	**<u>Preplanning</u>** Review prior/post examination documents; incorporate management discussions, changes in technology, personnel and services, security incidents, and audit findings.	Technology Profile Script
#2	**<u>Preplanning</u>** Send IT Examination Officer’s Questionnaire to financial institution.	IT Examination Officer’s Questionnaire
#3	**<u>Risk Scoping</u>** Gain an understanding of the financial institution’s risk management practices.	Technology Profile Script and IT Examination Officer’s Questionnaire
#4	**<u>Scope Development</u>** Develop a preliminary financial institution risk profile based on historical and other information obtained during preplanning and risk-scoping activities.	IT Summary Analysis
#5	**<u>Onsite Examination Procedures</u>** Execute scope based on a preliminary assessment and understanding of the financial institution’s risk profile.	IT Snapshot Work Program and IT Summary Analysis
#6	**<u>IT Composite Rating</u>** Assign the rating at the conclusion of the examination based on FFIEC ratings definitions.	IT Summary Analysis
#7	**<u>Report Preparation</u>** Document IT examination findings and prepare ROE comments. Update ViSION.	IT Summary Analysis

APPENDIX III

IT EXAMINATION RESOURCE STRATEGY MATRIX

Institution Characteristics			Examiner Skills Required	Examiner Training
Type	**Score**			
I	0-49	-- Limited networking -- Limited E-Banking activities -- Minimal external threats -- Risks are centered in core processing -- No in-house programming -- Does not process core applications for others	-- Basic networking concepts* -- Ability to evaluate pre-exam questionnaire responses -- High-level core application procedures* *Available in safety and soundness IT refresher training.	Required -- Commissioned Examiner -- Annual IT refresher -- Computer-based training (various) Recommended -- Information Technology Examination Course (ITEC) Note: Phase-in requirement for all Commissioned Examiners to attend ITEC
II		-- Limited networking -- Limited E-Banking activities -- Minimal external threats -- Risks are centered in core processing	-- Basic network concepts -- Ability to evaluate pre-exam questionnaire responses -- Ability to apply and complete IT General Work Program -- Vendor-specific knowledge for core processing systems	Required -- See Type I required training -- ITEC Recommended -- i-NET+, Network+, Security+* -- Transmission Control Protocol/Internet Protocol (TCP/IP) -- Regional seminars -- Begin OJT mentoring -- FFIEC conference * Intermediate IT courses.

APPENDIX III

Institution Characteristics			Examiner Skills Required	Examiner Training
Type	**Score**		**Type**	**Score**
III	50-79	-- Networks are an integral element of technology operations -- E-Banking activities -- Threats = Type II threats and introduction of external threats -- Risk = Type II and exposure to public networks and external breaches	-- Intermediate network concepts -- Ability to evaluate pre-exam questionnaire responses -- Ability to apply and complete IT General Work Program -- Vendor and device-specific knowledge of all systems	<u>Required</u> -- See Type II required training -- i-NET+, Network+, Security+ -- TCP-IP -- Operating system platforms -- IT-OJT – intermediate <u>Recommended</u> -- Flexible training -- Firewalls, Intrusion Detection System (IDS), virtual private networks (VPNs), wireless, advanced platforms -- Certifications -- FFIEC conference -- FDIC seminar
IV	80-130	-- Communication systems are critical to operations -- Widely distributed Internet working -- Threats = Type III threats and multiple external sources of threats -- Risk = Type III and higher administrative and security risks	-- Advanced platform-specific knowledge -- Advanced knowledge of networking & telecommunications concepts -- High level of understanding of security concepts	<u>Required</u> -- See Type III required training -- IS/OJT – Advanced -- Firewalls, IDS, VPNs, wireless, advanced platforms <u>Recommended</u> -- Flexible training -- FDIC seminar -- Certifications -- Product specialization

FFIEC's URSIT COMPOSITE RATINGS DEFINITIONS

Composite 1

Financial institutions and service providers rated composite "1" exhibit strong performance in every respect and generally have components rated "1" or "2." Weaknesses in IT are minor in nature and are easily corrected during the normal course of business. Risk management processes provide a comprehensive program to identify and monitor risk relative to the size, complexity, and risk profile of the entity. Strategic plans are well defined and fully integrated throughout the organization. This allows management to quickly adapt to changing market, business, and technological needs of the entity. Management identifies weaknesses promptly and takes appropriate corrective action to resolve audit and regulatory concerns. The financial condition of the service provider is strong, and overall performance shows no cause for supervisory concern.

Composite 2

Financial institutions and service providers rated composite "2" exhibit safe and sound performance but may demonstrate modest weaknesses in operating performance, monitoring, management processes, or system development. Generally, senior management corrects weaknesses in the normal course of business. Risk management processes adequately identify and monitor risk relative to the size, complexity, and risk profile of the entity. Strategic plans are defined but may require clarification, better coordination, or improved communication throughout the organization. As a result, management anticipates but responds less quickly to changes in market, business, and technological needs of the entity. Management normally identifies weaknesses and takes appropriate corrective action. However, greater reliance is placed on audit and regulatory intervention to identify and resolve concerns. The financial condition of the service provider is acceptable, and while internal control weaknesses may exist, there are no significant supervisory concerns. As a result, supervisory action is informal and limited.

Composite 3

Financial institutions and service providers rated composite "3" exhibit some degree of supervisory concern due to a combination of weaknesses that may range from moderate to severe. If weaknesses persist, further deterioration in the condition and performance of the institution or service provider is likely. Risk management processes may not effectively identify risks and may not be appropriate for the size, complexity, or risk profile of the entity. Strategic plans are vaguely defined and may not provide adequate direction for IT initiatives. As a result, management often has difficulty responding to changes in business, market, and technological needs of the entity. Self-assessment practices are weak and are generally reactive to audit and regulatory exceptions. Repeat concerns may exist, indicating that management may lack the ability or willingness to resolve concerns. The financial condition of the service provider may be weak, and/or negative trends may be evident. While financial or operational failure is unlikely, increased supervision is necessary. Formal or informal supervisory action may be necessary to secure corrective action.

Composite 4

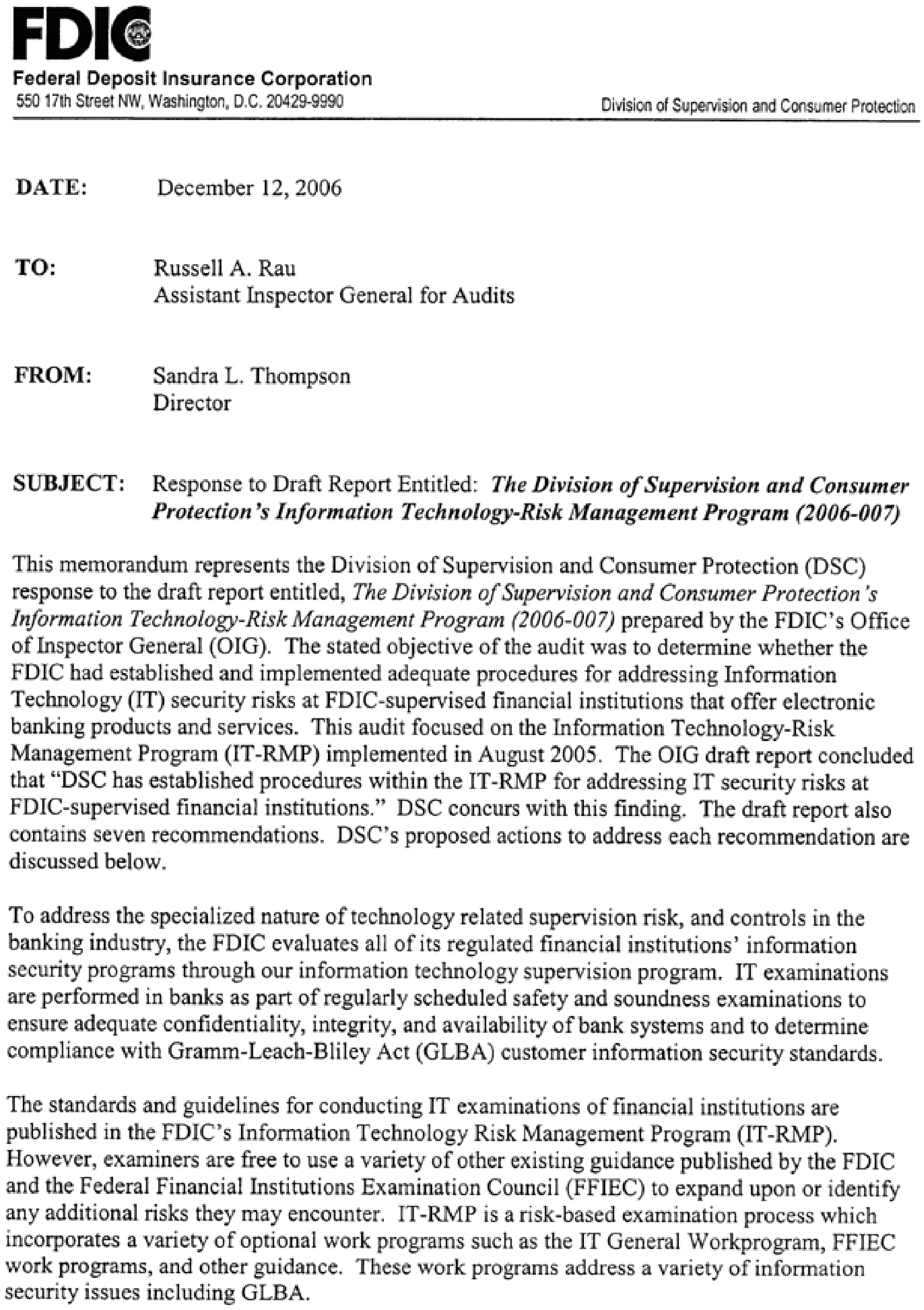
Financial institutions and service providers rated composite “4” operate in an unsafe and unsound environment that may impair the future viability of the entity. Operating weaknesses are indicative of serious managerial deficiencies. Risk management processes inadequately identify and monitor risk, and practices are not appropriate given the size, complexity, and risk profile of the entity. Strategic plans are poorly defined and not coordinated or communicated throughout the organization. As a result, management and the board are not committed to, or may be incapable of, ensuring that technological needs are met. Management does not perform self-assessments and demonstrates an inability or unwillingness to correct audit and regulatory concerns. The financial condition of the service provider is severely impaired and/or deteriorating. Failure of the financial institution or service provider may be likely unless IT problems are remedied. Close supervisory attention is necessary and, in most cases, formal enforcement action is warranted.

Composite 5

Financial institutions and service providers rated composite “5” exhibit critically deficient operating performance and are in need of immediate remedial action. Operational problems and serious weaknesses may exist throughout the organization. Risk management processes are severely deficient and provide management little or no perception of risk relative to the size, complexity, and risk profile of the entity. Strategic plans do not exist or are ineffective, and management and the board provide little or no direction for IT initiatives. As a result, management is unaware of, or inattentive to, technological needs of the entity. Management is unwilling or incapable of correcting audit and regulatory concerns. The financial condition of the service provider is poor, and failure is highly probable due to poor operating performance or financial instability. Ongoing supervisory attention is necessary.

APPENDIX V

CORPORATION COMMENTS



FDIC

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Division of Supervision and Consumer Protection

DATE: December 12, 2006

TO: Russell A. Rau
Assistant Inspector General for Audits

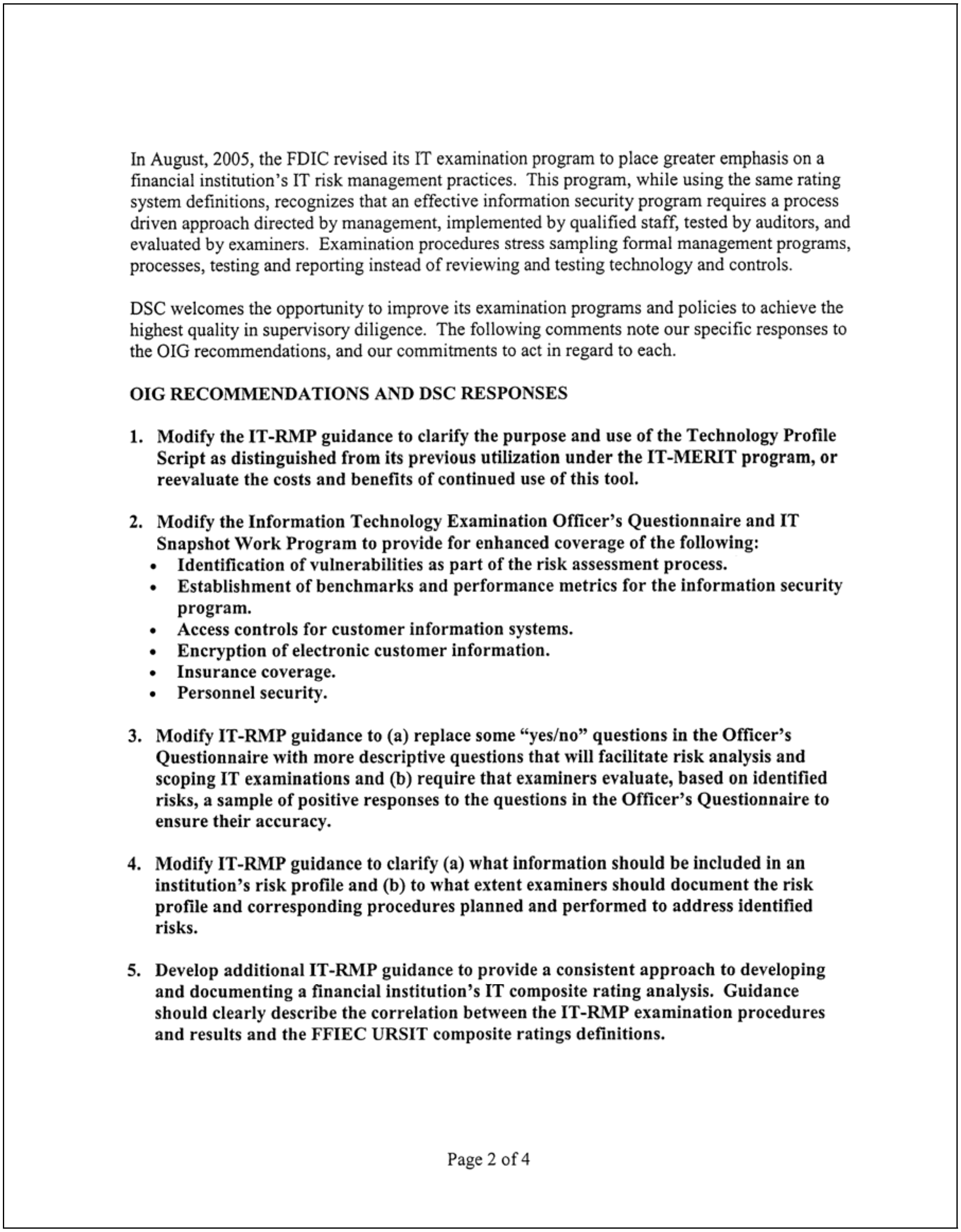
FROM: Sandra L. Thompson
Director

SUBJECT: Response to Draft Report Entitled: ***The Division of Supervision and Consumer Protection's Information Technology-Risk Management Program (2006-007)***

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-Risk Management Program (2006-007)* prepared by the FDIC's Office of Inspector General (OIG). The stated objective of the audit was to determine whether the FDIC had established and implemented adequate procedures for addressing Information Technology (IT) security risks at FDIC-supervised financial institutions that offer electronic banking products and services. This audit focused on the Information Technology-Risk Management Program (IT-RMP) implemented in August 2005. The OIG draft report concluded that "DSC has established procedures within the IT-RMP for addressing IT security risks at FDIC-supervised financial institutions." DSC concurs with this finding. The draft report also contains seven recommendations. DSC's proposed actions to address each recommendation are discussed below.

To address the specialized nature of technology related supervision risk, and controls in the banking industry, the FDIC evaluates all of its regulated financial institutions' information security programs through our information technology supervision program. IT examinations are performed in banks as part of regularly scheduled safety and soundness examinations to ensure adequate confidentiality, integrity, and availability of bank systems and to determine compliance with Gramm-Leach-Bliley Act (GLBA) customer information security standards.

The standards and guidelines for conducting IT examinations of financial institutions are published in the FDIC's Information Technology Risk Management Program (IT-RMP). However, examiners are free to use a variety of other existing guidance published by the FDIC and the Federal Financial Institutions Examination Council (FFIEC) to expand upon or identify any additional risks they may encounter. IT-RMP is a risk-based examination process which incorporates a variety of optional work programs such as the IT General Workprogram, FFIEC work programs, and other guidance. These work programs address a variety of information security issues including GLBA.



In August, 2005, the FDIC revised its IT examination program to place greater emphasis on a financial institution's IT risk management practices. This program, while using the same rating system definitions, recognizes that an effective information security program requires a process driven approach directed by management, implemented by qualified staff, tested by auditors, and evaluated by examiners. Examination procedures stress sampling formal management programs, processes, testing and reporting instead of reviewing and testing technology and controls.

DSC welcomes the opportunity to improve its examination programs and policies to achieve the highest quality in supervisory diligence. The following comments note our specific responses to the OIG recommendations, and our commitments to act in regard to each.

OIG RECOMMENDATIONS AND DSC RESPONSES

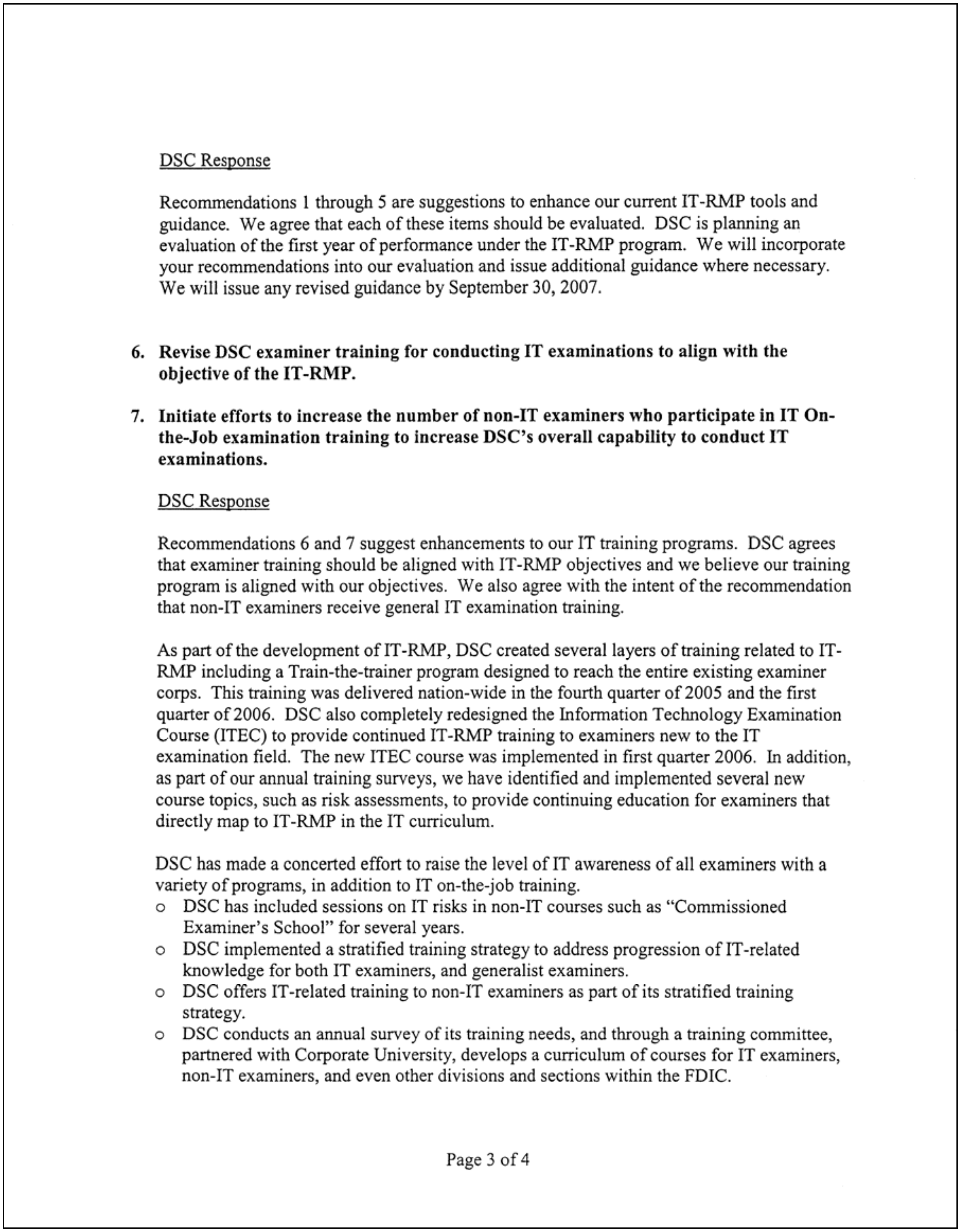
1. **Modify the IT-RMP guidance to clarify the purpose and use of the Technology Profile Script as distinguished from its previous utilization under the IT-MERIT program, or reevaluate the costs and benefits of continued use of this tool.**

2. **Modify the Information Technology Examination Officer's Questionnaire and IT Snapshot Work Program to provide for enhanced coverage of the following:**
   - **Identification of vulnerabilities as part of the risk assessment process.**
   - **Establishment of benchmarks and performance metrics for the information security program.**
   - **Access controls for customer information systems.**
   - **Encryption of electronic customer information.**
   - **Insurance coverage.**
   - **Personnel security.**

3. **Modify IT-RMP guidance to (a) replace some "yes/no" questions in the Officer's Questionnaire with more descriptive questions that will facilitate risk analysis and scoping IT examinations and (b) require that examiners evaluate, based on identified risks, a sample of positive responses to the questions in the Officer's Questionnaire to ensure their accuracy.**

4. **Modify IT-RMP guidance to clarify (a) what information should be included in an institution's risk profile and (b) to what extent examiners should document the risk profile and corresponding procedures planned and performed to address identified risks.**

5. **Develop additional IT-RMP guidance to provide a consistent approach to developing and documenting a financial institution's IT composite rating analysis. Guidance should clearly describe the correlation between the IT-RMP examination procedures and results and the FFIEC URSIT composite ratings definitions.**



DSC Response

Recommendations 1 through 5 are suggestions to enhance 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.

6. **Revise DSC examiner training for conducting IT examinations to align with the objective of the IT-RMP.**

7. **Initiate efforts to increase the number of non-IT examiners who participate in IT On-the-Job examination training to increase DSC's overall capability to conduct IT examinations.**

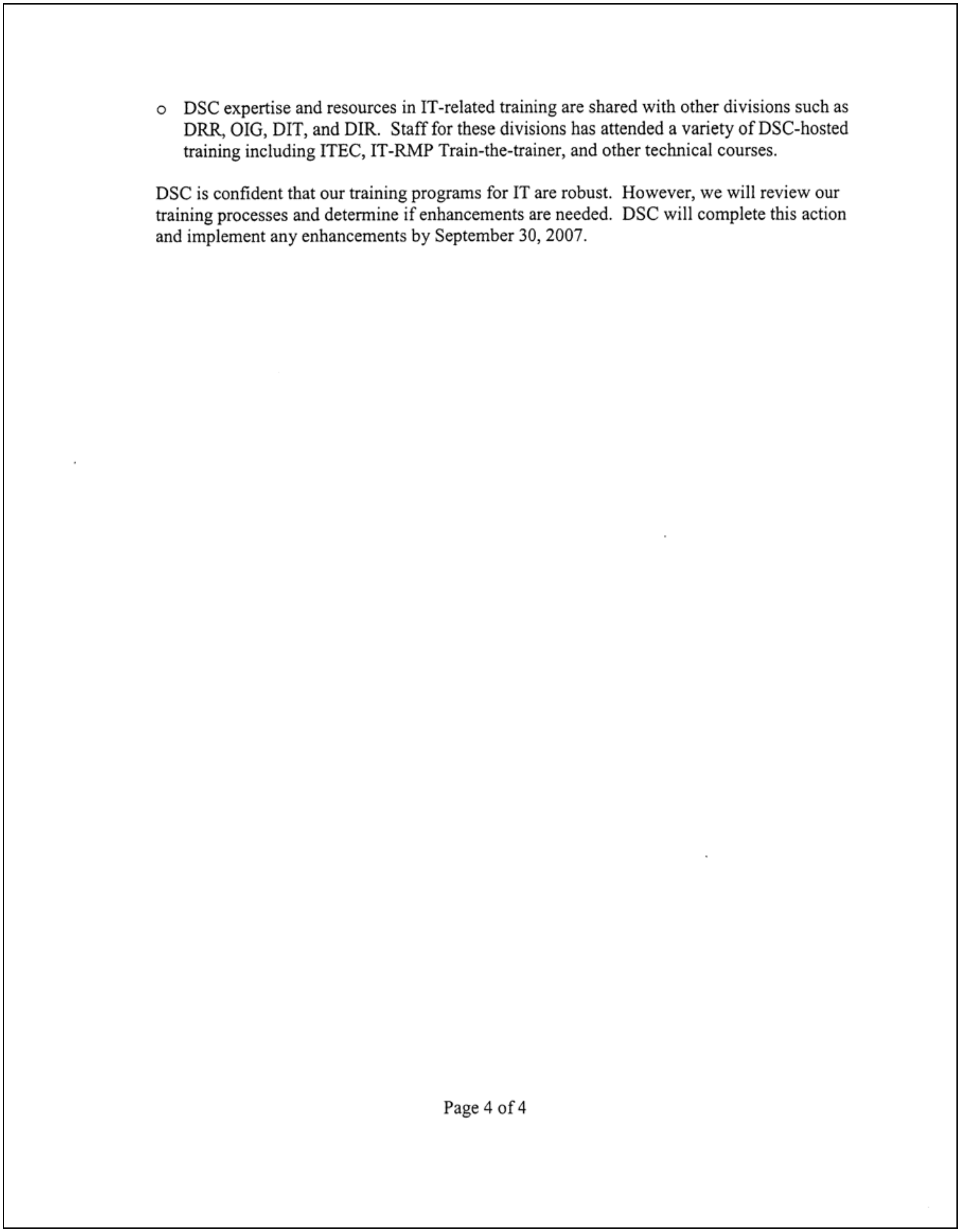
DSC Response

Recommendations 6 and 7 suggest enhancements to our IT training programs. DSC agrees that examiner training should be aligned with IT-RMP objectives and we believe our training program is aligned with our objectives. We also agree with the intent of the recommendation that non-IT examiners receive general IT examination training.

As part of the development of IT-RMP, DSC created several layers of training related to IT-RMP including a Train-the-trainer program designed to reach the entire existing examiner corps. This training was delivered nation-wide in the fourth quarter of 2005 and the first quarter of 2006. DSC also completely redesigned the Information Technology Examination Course (ITEC) to provide continued IT-RMP training to examiners new to the IT examination field. The new ITEC course was implemented in first quarter 2006. In addition, as part of our annual training surveys, we have identified and implemented several new course topics, such as risk assessments, to provide continuing education for examiners that directly map to IT-RMP in the IT curriculum.

DSC has made a concerted effort to raise the level of IT awareness of all examiners with a variety of programs, in addition to IT on-the-job training.

- DSC has included sessions on IT risks in non-IT courses such as "Commissioned Examiner's School" for several years.
- DSC implemented a stratified training strategy to address progression of IT-related knowledge for both IT examiners, and generalist examiners.
- DSC offers IT-related training to non-IT examiners as part of its stratified training strategy.
- DSC conducts an annual survey of its training needs, and through a training committee, partnered with Corporate University, develops a curriculum of courses for IT examiners, non-IT examiners, and even other divisions and sections within the FDIC.



- DSC expertise and resources in IT-related training are shared with other divisions such as DRR, OIG, DIT, and DIR. Staff for these divisions has attended a variety of DSC-hosted training including ITEC, IT-RMP Train-the-trainer, and other technical courses.

DSC is confident that our training programs for IT are robust. However, we will review our training processes and determine if enhancements are needed. DSC will complete this action and implement any enhancements by September 30, 2007.

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 - 5	DSC will incorporate these recommendations into its planned evaluation of the first year of performance under the IT-RMP program and issue additional guidance where necessary.	September 30, 2007	0	Yes	Open
6 and 7	DSC will review its training processes and determine if enhancements are needed.	September 30, 2007	0	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.