Office of Inspector General

March 14, 2001
Audit Report No. 01-007

Audit of the FDIC's Information Technology Risk Management Program

OFFICE OF INSPECTOR GENERAL
OFFICE OF AUDITS

TABLE OF CONTENTS

FDIC
Federal Deposit Insurance Corporation
Washington, D.C. 20434

Office of Audits
Office of Inspector General

DATE: March 14, 2001

TO: Donald C. Demitros, Chief Information Officer and
Director, Division of Information Resources Management

David H Loewenstein

FROM: David H. Loewenstein
Assistant Inspector General

SUBJECT: *Audit of the FDIC's Information Technology Risk Management Program*
(Audit Report Number 01-007)

The FDIC's Office of Inspector General (OIG) has completed an audit of the FDIC's Information Technology Risk Management Program. The FDIC initiated this program in 1997 to comply with federal regulations that require federal agencies to develop policies and procedures that will identify and mitigate risks related to information technology (IT). At the time of the audit, the program was evolving in that the Division of Information Resources Management (DIRM) was either planning or implementing procedural modifications to correct weaknesses noted by its staff and the U.S. General Accounting Office (GAO). While working on a related audit, we identified the need to more fully evaluate DIRM's IT risk management program, particularly DIRM's actions to complete security plans and independent security reviews. In the interest of timely attention to problem areas, we focused our resources to quickly research and identify actions needed to resolve the issues through a collaborative effort with DIRM management and staff. This "real-time" collaboration proved successful in that issues were immediately discussed and most recommended actions were immediately initiated.

BACKGROUND

The FDIC's IT risk management program was designed to identify the applications that process sensitive corporate data and determine their ability to safeguard the confidentiality and reliability of the data. The program is critical to safeguarding the FDIC's infrastructure and is based on and required by *Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Resources.*" OMB requires agencies to identify their major applications and general support systems and implement four controls to manage IT risk. The four control requirements are: (1) assignment of responsibility for security, (2) security plans, (3) periodic independent security reviews (ISRs), and (4) management authorizations. OMB's definitions related to these control requirements follow.

- Major applications are defined as applications that require special security attention by management due to the magnitude of harm that could result from improper operation, inappropriate access, or unauthorized modification. General support systems are the operating systems and utilities that support the operation of applications.

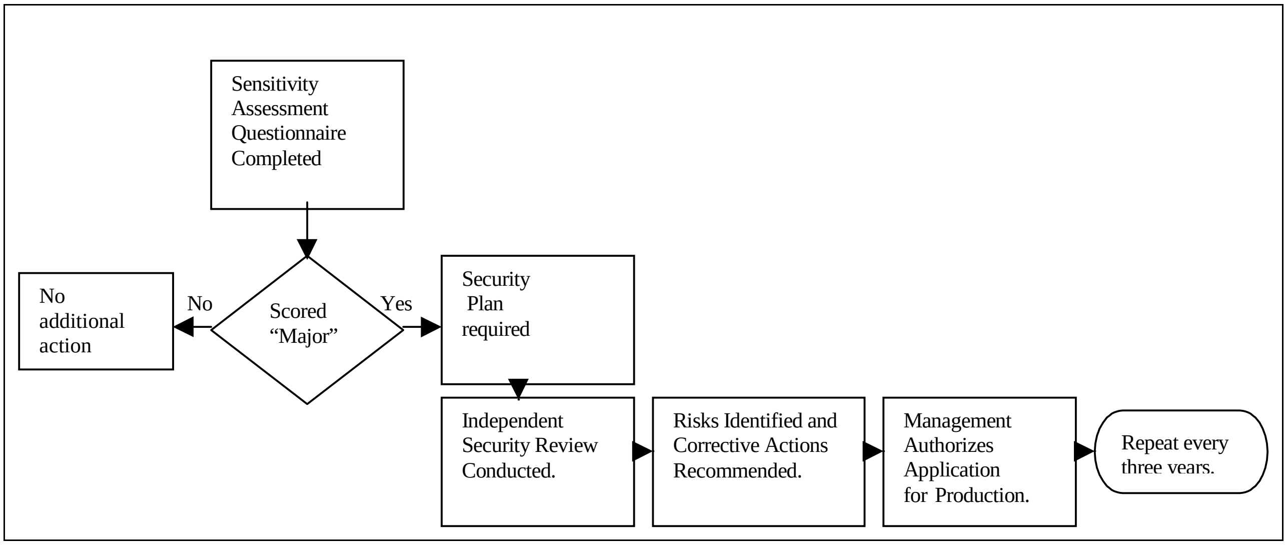
- ISRs, conducted by the FDIC or its contractors, assess the risk of the application or system by reviewing and reporting on security control weaknesses that need to be corrected. The ISR process is based on guidance provided by the National Institute of Standards and Technology (NIST) and Federal Information Processing Standards (FIPS) and should be performed every 3 years.

- Security plans are written documents that provide an overview of the security requirements for the system or application**.** The security plan should be developed during the application's development and serve as the basis for subsequent management authorizations.

- The Sensitivity Assessment Questionnaires (SAQ) are questionnaires that are completed by application system users to assess the confidentiality, integrity, and availability of data processed by the system. The answers are assigned a numerical score. Any applications scoring above a specified numerical threshold are considered major and, thus, require an ISR, security plan, and subsequent management authorization.

The FDIC's IT risk management program, as documented in Circular 1310.3, mirrors these OMB requirements. As shown in figure 1, DIRM's Information Security Section (ISS) distributes the SAQs to all division managers responsible for the application's security and then scores their completed questionnaires. Applications that are identified as major are passed to the risk management program manager who schedules the applications or general support systems for ISRs. The resulting ISR report is presented to the user and the appropriate DIRM unit and identifies control weaknesses and the needed corrective actions to mitigate the IT risk. Division managers document their acceptance of the report's conclusions, particularly the IT risks and the resulting recommendations, by signing a management authorization. The management authorization acknowledges the ISR that lists the weaknesses identified and the needed corrective actions, and can also cite recommendations that will not be acted upon. By signing the management authorization, the managers accept the risks associated with not resolving these issues.

Figure 1: Risk Management Process for Applications


Sensitivity Assessment Questionnaire Completed
Scored "Major"
No
Yes
No additional action
Security Plan required
Independent Security Review Conducted.
Risks Identified and Corrective Actions Recommended.
Management Authorizes Application for Production.
Repeat every three years.

In 1999, using its SAQ process, DIRM identified 70 applications as major applications. In anticipation of performing these ISRs, the FDIC retained an independent contractor at a cost of approximately $4.6 million over 3 years. Contractor costs associated with completing each application ISR total approximately $50,000, while contractor costs for general support system ISRs total approximately $100,000. This financial commitment indicates the FDIC's intent to develop an effective risk management program, particularly when comparing DIRM's program to other federal agencies that we observed. Our "best practices" review of six federal agencies' programs[1] that comply with OMB A-130 indicated that the FDIC had the most comprehensive and ambitious IT risk program**.** However, during its audit of the FDIC's 1999 financial statements, GAO released a management letter, dated July 27, 2000, raising concerns about the adequacy of the FDIC's IT security environment. The letter reported weaknesses in the FDIC's risk management program, particularly noting that the FDIC had not fully or adequately completed ISRs and security plans. These issues cited by GAO still existed at the initiation of our audit.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of the audit was to determine the effectiveness of the FDIC's risk management program in addressing the security-related requirements contained in OMB A-130, Appendix III. The audit was performed in "real-time" in that we worked with DIRM while they were determining or implementing their internal program modifications. As we developed our conclusions and recommendations for program improvement, we communicated them to DIRM. DIRM, in turn, approved and implemented many of these modifications during fieldwork. The audit scope

[1] National Credit Union Association, Office of Thrift Supervision, U.S. Postal Service, Department of Agriculture, Department of Transportation, and the Office of the Comptroller of the Currency

augmented the issues raised by the GAO management letter by identifying the underlying management issues causing the risk-related conditions documented by GAO.

To address our objective, we reviewed the original and updated versions of the FDIC's risk management procedures as well as the federal government requirements for implementing a risk management program. OMB Circular A-130 summarizes the four required components described earlier, while FIPS and NIST documents detail more specifically how the four components should be designed and completed. We determined the FDIC's compliance with these components by reviewing a judgmental sample of two ISRs conducted during 1999 and two others conducted during 2000. Each sample included a major application and a general support system. We also reviewed all completed SAQs, security plans, and management authorizations for major applications for the year 2000 to determine: (1) their compliance with federal and FDIC regulations and (2) the effectiveness and reliability of the SAQs in identifying the major applications.

We reviewed schedules and matrices that DIRM developed during our fieldwork to schedule and track the SAQs, ISRs, security plans, and management authorizations. We also reviewed existing schedules and matrices that supported the corrective action process. We interviewed ISS staff and the risk management program manager and reviewed the FDIC's policies and procedures with respect to IT risk management. We interviewed representatives of five FDIC divisions and offices to capture their ideas for possible improvements for ISRs and the overall risk management program, and we performed a "best practices" review of six outside agencies to obtain an understanding of their risk management procedures.

The audit was performed between July 1, 2000 and October 12, 2000 and covered IT risk management activities for the period of January 1, 2000 through September 9, 2000. The audit was conducted in accordance with generally accepted government auditing standards.

RESULTS OF AUDIT

The FDIC's IT strategic plan includes many control initiatives designed to manage and minimize IT risk. Recent additions to the plan include, but are not limited to, the development of: (1) corporate-wide security training, (2) enhanced virus protection capabilities, (3) public key infrastructure (PKI),[2] (4) intrusion detection capabilities, and (5) an IT incident response program. Additionally, our "best practices" research with six federal agencies indicated that the FDIC risk management program compared favorably with other agencies we researched.

However, the FDIC's risk management program is not yet fully effective in addressing all the requirements of OMB A-130 and, thereby, controlling risk to the Corporation's IT infrastructure. The program has been evolving and DIRM continues to strive to improve it. Many improvements have either recently been made, are in process, or have been planned. We believe that most of the program weaknesses can be resolved with management adjustments. Interestingly, one of these adjustments entails DIRM reducing the number of applications designated as major and, therefore requiring an ISR. This reduction will permit resources

[2] PKI is a cryptography method using computer hardware and software to establish trusted information sharing among a select group of people.

committed to performing ISRs to be reassigned to other security issues and may also result in cost savings of $2.2 million every 3 years by reducing the number of required ISRs to be performed every 3 years (funds to be put to better use - $2.2 million). DIRM recently reduced the number of major applications requiring ISRs from 70 to 26 based on discussions with our office and DIRM's clients.

Adjustments that will further enhance the program include administration modifications that would require a formal, documented reporting system to track the scheduling and completion of the program's milestones and documents. Concerning scheduling, DIRM did not prioritize general support systems and applications when scheduling ISRs. The ISRs for general support systems, particularly the mainframe and the network, should be completed first because they impact the security of all applications operating within their platform. The general support system ISRs should be followed by ISRs of the major applications that pose the greatest risk to the FDIC.

The process of using the SAQ as the sole tool to select major applications resulted in an excessive number of ISRs. This was confirmed from interviews with clients, our review of federal agencies' best practices, and our internal analysis. Client representatives indicated the SAQ was confusing and too subjective and they did not always agree with DIRM's resulting selection of their applications being considered major. Federal agency IT managers we interviewed employ a more centralized approach whereby one manager analyzes all applications and chooses the optimum number of major applications. This approach minimizes the possibility that the program will become overburdened and thus jeopardize the program's primary goals of providing effective, in-depth security reviews. Our internal analysis determined that the SAQ contained some questions that were not reliable in measuring sensitivity, thereby allowing application sensitivity scores that determine major applications to be inflated. To enhance the reliability of the SAQ process, DIRM has agreed to discuss the SAQ scores and other factors with the users to arrive at a mutual decision on which applications or functions require a security review.

The ISR supporting procedures also need to be modified to enhance the effectiveness of the ISR and the resulting corrective actions. Client representatives stated that ISRs were limited because they focused solely on application controls rather than on controls related to an overall business process or function. By broadening the ISR scope in this manner, the FDIC would have increased assurance that the overall control environment supporting the application was evaluated and improved. Additionally, client representatives indicated that the conditions and resulting corrective actions were often outside their control and this drawback impacted their willingness to support the ISR findings, conclusions, and corrective actions. DIRM agreed that improved communications with systems' users would enhance the effectiveness of ISRs.

We noted opportunities to improve contractor oversight of the ISR process. ISR findings and major conclusions were not consistently or adequately supported by working paper documentation. Further, DIRM did not consistently review and ensure the preparation of supporting working papers by its contractor. Finally, DIRM did not adequately review contractor invoices to ensure the accuracy of time charges and costs related to ISR activities.

Although DIRM had identified over 700 corrective actions through the ISR process, none have been resolved. At the beginning of our fieldwork, DIRM had not implemented a system to: (1) identify the corporate officials responsible for corrective actions resulting from ISRs, (2) effectively track resolution of the actions, and (3) document timeframes for completing the actions. The effectiveness of review activities is dependent on the program's ability to resolve any noted weaknesses. If the issues are not resolved, the efforts to identify them are negated.

The issues noted above play an important and direct role in the effectiveness of the FDIC's IT risk management program. An indirect but equally important component to strengthening the program and minimizing risk is the need for ISS to be involved during the development of new applications. FDIC Circular 1320.3 and DIRM's application development procedures require that application security be adequately analyzed and designed prior to implementation. DIRM had not ensured adequate ISS involvement at this critical stage.

The OIG and DIRM agree that a successful risk management program is dependent on a strong ISS role in reviewing and approving application security during the system development process. ISS's early involvement can help ensure that adequate security controls are incorporated that will not only safeguard the specific application data but assist in managing IT risk corporate-wide. To ensure ISS involvement, DIRM should adopt a system development strategy similar to one used by other federal agencies that prohibits the implementation of any major application until information security officials have reviewed and approved the security design.

PROGRAM SUPPORT NEEDS TO BE ENHANCED

During our early fieldwork, DIRM had not developed a formal inventory of applications and general support systems determined to be major which would thus require action to ensure a successful IT risk management program. Without such an inventory, DIRM was unable to centrally track the status of and prioritize SAQs, ISRs, security plans, management authorizations, and corrective actions. OMB A-130 requires that ISRs be scheduled such that general support systems are reviewed first since they have a major impact on the security of all applications within the environment. Further, DIRM had not implemented a centralized system for filing and cataloging documentation created during the various components of its program. Finally, DIRM did not routinely obtain and review OIG and GAO work related to the application or general support system under review in an effort to reduce the scope of its ISRs.

OMB A-130 and prudent management dictate that resources be prioritized to ensure that ISRs of general support systems are performed first. ISRs for general support systems impact all applications on the platform and provide the framework for all related applications, particularly applications that have the largest impact to overall security. By first identifying and resolving security weaknesses related to general support systems, such as mainframe computer and communication network operations, security for all applications is strengthened. Without a formal inventory, DIRM cannot take full advantage of this scheduling strategy.

DIRM also did not have a system to catalog and file documentation related to its IT risk management program. As a result, DIRM experienced difficulties in locating documentation, determining the FDIC's major applications, and developing an effective risk management schedule for performing ISRs. Because of the extensive budget for the ISR program and the importance of these documents to the IT risk management program and the FDIC's overall IT security, a cataloging and filing system is needed.

Finally, ISS personnel did not routinely take advantage of available resources that could reduce the scope of ISRs. The OIG and GAO conduct audits that include similar objectives and steps to those followed during the performance of ISRs. Additionally, the FDIC's divisions and offices perform internal reviews that include objectives that could benefit and support ISRs. DIRM's ISS can improve the effectiveness and efficiency of the ISR process by contacting these divisions and offices to determine whether they have performed work that could benefit and reduce the scope of planned ISRs.

During the course of our audit and in response to our suggestions, DIRM developed a tracking matrix and central filing system. In response to additional suggestions, DIRM improved the matrix by including additional information to track actual versus planned dates and expanded certain fields where multiple deliverables are expected. Additionally, DIRM stated it was aware of the need for ISR schedules to be prioritized. To initiate this enhanced process, DIRM scheduled ISRs for the mainframe and Division of Finance applications to be completed by the end of the 2000.

Recommendation

We recommend that the Director, DIRM, and CIO:

(1) Update the ISR procedure manual to require that: (a) DIRM schedule and prioritize ISRs for general support systems and applications based on their impact to security within the entire IT environment and (b) ISS coordinate with OIG, GAO, and the appropriate FDIC division or office to obtain relevant information on the work performed by those offices when initiating future ISRs.

SAQs AND RELATED PROCEDURES CAN BE ENHANCED

The FDIC can improve its process for determining major systems to be supported by its IT risk management program. OMB A-130 requires that federal entities assess the sensitivity of internal application systems and related data. The purpose of this process is to identify the entity's major systems that require ISRs and related risk management documentation. At the initiation of our fieldwork, the FDIC employed a 3-page Sensitivity Assessment Questionnaire (SAQ) as the sole means of determining its major applications. Using the SAQ, each division answered questions relating to an application's sensitivity based on confidentiality, data integrity, and availability. DIRM's ISS assigned a score to each application based on the responses to the SAQ. Applications that were scored above a specific threshold were deemed major and scheduled for an ISR.

Our analysis of the SAQ process, discussions with officials from FDIC divisions and offices, and review of best practices employed by other federal agencies support the need to supplement the SAQ with additional processes to determine major applications. Interviews with representatives from five of DIRM's major client divisions illustrate a lack of confidence in the SAQ as the sole determinant in identifying the FDIC's major applications. The client representatives indicated that the SAQ questions were confusing and subjective and that they completed the SAQ without clearly understanding the questions. The client representatives also indicated that they did not always agree with DIRM's designation of major applications but were not afforded the opportunity to discuss the designations with DIRM.

We reviewed the SAQ template and all 26 SAQs performed during 2000 that resulted in designating a system as major. Our review determined that some questions contained in the template were not reliable in measuring sensitivity, particularly in the area of data integrity. The SAQ is divided into three parts: data integrity, confidentiality, and availability. Each category comprises one-third of the points in determining major applications. We noted that two questions in the data integrity category could reasonably be answered such that all applications would receive the highest score for this category. With this scoring flaw, the number of major applications may be overstated because applications that do not require the strongest of controls to protect data integrity and may possess only moderate risk regarding confidentiality or availability of data may be classified as major.

Our review of best practices of six other federal entities concluded that other agencies did not employ a process similar to the SAQ in determining their "major" applications. Instead of relying on clients when identifying major applications, these agencies relied on a centralized IT security manager to designate applications as "major." The process provided for a more consistent designation because it permitted a single official to analyze all applications within the organization's IT environment and determine which should be considered "major." This process also resulted in fewer systems being designated as major, minimizing the possibility that the risk management program will become overburdened and jeopardize the program's primary goal of providing effective, in-depth security reviews for the most critical applications. GAO addresses this concept in its publication entitled *Information Security Risk Assessment, Practices of Leading Organizations* which states that: "performing risk assessments for more than 10 to 20 applications would become overwhelming, cumbersome, and strain limited resources."

An additional benefit of selecting the optimum number of "major" applications requiring ISRs is the potential cost savings associated with performing the ISRs. During 1999, DIRM, using its SAQ process, identified 70 applications as major and requiring an ISR. However, following discussions with our office regarding the ISR process and the activities of other federal agencies, DIRM implemented modified procedures including more in-depth discussions with division managers regarding the results of the SAQ process. These modified procedures resulted in reducing the number of major applications requiring ISRs from 70 to 26. Based on DIRM's estimates of the cost of ISRs, this reduction could reduce contractor costs by as much as $2.2 million over the 3-year risk management program cycle. In addition, internal DIRM resources associated with overseeing and administering the ISR portion of the risk management program should be reduced.

The OIG and ISS agree that the SAQ, with modification, is a tool that should continue to be used to identify the sensitivity level of an application and to assist in developing the security plan. Enhancing the SAQ process to reduce subjectivity and increase reliability will improve the FDIC's assessments of its major applications, better focus limited resources, and possibly reduce costs associated with unnecessary efforts related to applications misclassified as major applications. During our fieldwork, ISS developed or implemented changes to improve the SAQ process. ISS met with DOF and DOS to jointly determine the major applications that require ISRs. ISS, as described above, reduced the number of required ISRs from 70 to 26. Additionally, to enhance the reliability of the SAQ process, ISS agreed to add an explanation box for each SAQ question and modify the questions relating to data integrity.

Recommendations

We recommend the Director, DIRM, and CIO should:

(2) Modify the SAQ procedure manual to require meetings between ISS and the user to determine major applications chosen for ISR review. (Funds to be put to better use - $2.2 million). (The OIG and DIRM agree that such meetings will complement the SAQ process by ensuring the client clearly understands and agrees to the final SAQ score and the applications that are chosen for future ISRs).

(3) Develop new SAQ templates that include an explanation box for each question, and modify the data integrity questions in the SAQ to enhance reliability of the responses. (The explanation box will minimize the possibility of client confusion that could result in unreliable SAQ scores).

ENHANCED PROCEDURES CAN PRODUCE MORE EFFECTIVE ISRs

By modifying ISR supporting procedures, ISS can enhance its effectiveness and the effectiveness and implementation of resulting corrective actions. Interviews with representatives of five of the FDIC's divisions and offices and our reviews of ISRs identified concerns regarding the effectiveness of ISRs in identifying risks and developing effective corrective actions. The effectiveness of ISRs was limited because of the ISRs' focus on individual application controls rather than on controls related to an overall business process or function. In addition, the division and office representatives receiving the ISR findings and corrective actions viewed them as redundant and outside their control.

ISR recipients in DIRM's client offices and divisions indicated their belief that many potential security issues and weaknesses were overlooked because ISRs focused solely on controls related to a specific application. Our review of four completed ISRs confirmed that ISRs could be enhanced by consolidating the review of all applications and activities related to a corporate process or function. By broadening the scope of ISRs to include related processes and activities, the FDIC would have increased assurance that the overall control environment related to a specific corporate operation was evaluated and improved. Another potential benefit is improved efficiency and reduced costs in the performance of ISRs. ISRs are usually performed by a DIRM contractor and typically cost the Corporation approximately $50,000 for each application and $100,000 for each support system. As mentioned earlier, DIRM has already begun to reduce the number of ISRs by enhancing the SAQ process and reducing the number of major systems. By eliminating redundant steps in the performance of ISRs and reducing the number of ISRs by broadening their scope to include related processes and activities, the FDIC may be able to further reduce the costs of administering the program.

When developing ISRs, DIRM followed FIPS standards. These standards require specific ISR review steps to be included in each ISR even though some of these review steps do not directly apply to the application being audited and have been reviewed and documented in previous ISRs. DIRM can continue to address the FIPS requirements, enhance the quality of individual ISRs, and increase the confidence of its clients in the ISR process by noting in the report any finding that was identified previously. The report should include the ISR where the finding was initiated and the manager and division responsible for the corrective action. Secondly, DIRM can meet these ISR process goals by first conducting ISRs of the FDIC's general support systems. By doing so, relevant DIRM components can act upon recommendations that affect all applications that rely on the general support systems. Subsequently, during ISRs of individual applications or processes, DIRM can cite the general support system concerns that are relevant to individual applications or processes, note the timeframes for completing the recommended actions, and limit their detailed discussions and recommendations to application or process-specific issues.

Application or process-specific ISR activities could also be improved by increased coordination between the ISR team and the clients. The ISR process could be both more efficient and effective if DIRM included the client in planning the ISR and performing fieldwork tasks. This client involvement could reduce costs related to the ISR process and better focus the reviews on risks identified by the client's routine use of the application and business process. The ISR team could retain its required independence by overseeing and approving all work performed by the client. To ensure the effectiveness and efficiency of the process, an agreement regarding the nature and extent of the user's responsibility should be documented in a Memorandum of Understanding (MOU) that would be completed after initial ISR discussions.

Recommendations

We recommend that the Director, DIRM, and CIO:

(4) Modify ISR procedures to require a meeting between the ISR team and managers before the ISR is initiated. The meeting would include: (1) the ISR team educating the user on applicable FIPS requirements, (2) the ISR team and user agreeing to the scope of the review being either application-specific or based on functions or processes, and (3) the ISR team and user signing a MOU that summarizes the agreements. The MOU should also include an agreement on the extent of user involvement in the planning and completing of ISR review steps.

(5) Modify the ISR process such that findings outside the control of the user should still be listed in the ISR but clearly identified as to the original ISR and the unit responsible for the corrective actions.

IMPROVED CONTRACTOR OVERSIGHT CAN ENHANCE THE ISR PROCESS

We noted opportunities to improve contractor oversight for the ISR process. The conclusions and review activities contained in contractor-performed ISRs were not adequately supported by working papers. Also, DIRM was not adequately reviewing the support for contractor conclusions or invoice documentation. To determine the adequacy of workpapers, we requested workpapers that would support findings and conclusions for the two 1999 ISRs that we reviewed for the audit. The contractor's workpapers contained only emails and did not include schedules, calculations, or other documentation that would normally be expected to document conclusions reached and work performed. The risk management program manager stated in interviews that he did not review contractor workpapers because of lack of time and resources. The manager also stated he did not review contractor invoices again because of time and resource constraints. Workpapers should be reviewed by the FDIC program manager to ensure that the appropriate procedures were completed and that support exists for potential conditions or areas found satisfactory. The manager should also review invoice documents to evaluate the propriety of staff assignments and the amount of time that reasonably should have been expended on these tasks. Considering the costs associated with performing ISRs, the sensitive nature of the contractor's work, and the impact of contractor conclusions on FDIC operations, effective oversight procedures are vital to ensure the viability and reliability of the FDIC’s risk management program.

DIRM and the OIG agreed that the reduction in the number of ISRs should assist in improving working paper reviews and other oversight factors. We suggested and DIRM agreed to implement control procedures to improve review and oversight activities. ISS stated that it will require invoice modifications to specifically identify that the staff and resources expended for each task conform to the contractual agreements and will develop procedures that will enhance confirmation of time and task statements. Additionally, ISS indicated that it will consult with the OIG on developing working paper standards that will be required to support findings and confirmation of important controls.

Recommendation

We recommend that the Director, DIRM, and CIO:

(6) Modify the ISR procedure manual to require that: (1) contractor tasks assignments state the requirement for adequate contractor workpapers that support findings and confirmation of major controls, (2) workpapers are timely reviewed and approved, and (3) invoices be reviewed to confirm the time and personnel that were used for the ISRs.

CORRECTIVE ACTION PROGRAM NEEDS TO BE IMPLEMENTED

Although DIRM had identified substantial security risks and developed recommended corrective actions to address these risks through its risk management program, it had not implemented a system to: (1) identify the corporate officials responsible for the corrective actions, (2) establish target dates for completing the actions, and (3) track resolution of the actions. In addition, the absence of an effective tracking system reduced DIRM's ability to identify redundant corrective actions. As a result, approximately 700 recommended ISR corrective actions remain unresolved as of the end of our fieldwork.

Many of the 700 unresolved corrective actions are duplicates. As described before, ISRs would include identical review steps that had been completed in previous ISRs. If the review step resulted in a finding, the identical finding and corrective action noted in a previous ISR would be included in the current ISR, thereby resulting in redundant issues. The number of duplicated corrective actions cannot be easily identified because DIRM does not employ an identifying number for the recommendation nor assign a specific FDIC manager to be responsible for the resolution.

The effectiveness of any audit or internal review program depends on the program's ability to resolve any weaknesses identified in a timely manner. If the issues are not resolved, the efforts to identify them are negated. An effective tracking system identifies the corrective actions needed, the officials responsible for the actions, and the milestones for achieving the corrective actions. During our audit DIRM obtained agreement from the Office of Internal Control Management (OICM) to use the Internal Review Information System (IRIS), OICM's system for tracking corrective actions related to OIG and GAO audits, to track corrective actions related to ISRs. DIRM began populating IRIS with ISR-recommended corrective actions in August 2000. This action will provide DIRM with enhanced abilities to ensure the timely implementation of needed corrective actions. Involving OICM and internal control liaisons (ICL) in tracking and implementation can further enhance the effectiveness of the process.

Our review of the ISR data loaded into IRIS as of September 2000 identified the existence of a significant number of duplicate corrective actions. However, we were unable to quantify the number of duplicate actions loaded because DIRM had not developed a coding system to identify related recommended actions. The use of such a code would ease DIRM efforts to cleanse the ISR data in IRIS and identify similar or redundant future corrective actions. This, in turn, will permit the Corporation to focus on and prioritize the actions needed to improve the FDIC's security posture and improve client perceptions regarding the viability of the program.

Recommendations

We recommend that the Director, DIRM, and CIO:

(7) Design and implement a tracking report that employs ISR corrective action numbers and identifies only one unit or individual responsible for resolution and the timeframes required.

(8) Modify ISR support procedures to require that OICM and internal control liaisons be involved in monitoring and resolving corrective actions. These corrective actions should be tracked, and results that are delayed should be communicated to the next level of management. If delays become excessive, DIRM should distribute a report of outstanding corrective actions and submit them to senior management, including the CFO, if the delays persist.

INVOLVEMENT OF ISS DURING APPLICATION DEVELOPMENT IS CRITICAL TO AN EFFECTIVE IT RISK MANAGEMENT PROGRAM

Because DIRM had not ensured the involvement of ISS during the development of application systems supporting corporate operations, it had not effectively identified security-related issues and solutions during the development process. FDIC Circular 1320.3 and *FDIC's System Development Life Cycle Manual* require that ISS be involved in assessing security requirements during development to ensure the development and implementation of adequate safeguards. OMB A-130 requires that, during the first part of the development phase, security requirements be developed at the same time as functional requirements for the application. However, DIRM officials advised that the goals associated with delivering system functionality to meet FDIC clients' operational requirements often caused this needed involvement to be overlooked.

By requiring ISS to review and approve the security architecture for an application during the development stage, DIRM can maximize the effectiveness of the risk management program. ISS can help ensure that developers identify major applications through the ISR and then complete the resulting security plans and management authorizations. Many of the shortfalls in meeting OMB A-130 security requirements could have been addressed during the application development process if DIRM had adhered to this required portion of its system development life cycle (SDLC). By strictly adhering to its SDLC requirement to involve ISS and consider security requirements during the development process, DIRM can ensure that application-specific security issues are addressed during application development and avoid future IT risk management issues.

Recommendation

We recommend that the Director, DIRM, and CIO:

(9) Modify policies to include requirements that ISS must approve the security design of major applications before an application can be placed into production. This review and approval should be required for the security design, security plan, and management authorization. Specifically, the procedures should: (1) require a security specialist to review the security design for adequacy during the development stage and (2) require ISS management to approve and sign off on the design prior to placing the application in production.

CONCLUSION

As described above, we believe that the FDIC’s risk management issues can be corrected by implementing management modifications. One outcome of these modifications, particularly the modifications related to the SAQ process, is that the number of required ISRs will likely be reduced and the costs of administering the program will be likewise reduced. This, combined with oversight and planning enhancements, should reduce overall costs, allow more resources to be committed to each ISR, particularly the general support systems and major applications. In addition, active client involvement should ensure enhanced ISR quality and increased client acceptance of ISR issues. Finally, DIRM actions to restrict applications from being implemented without ISS’s review should enhance overall security and increase the manageability of the IT risk management program.

CORPORATION COMMENTS AND OIG EVALUATION

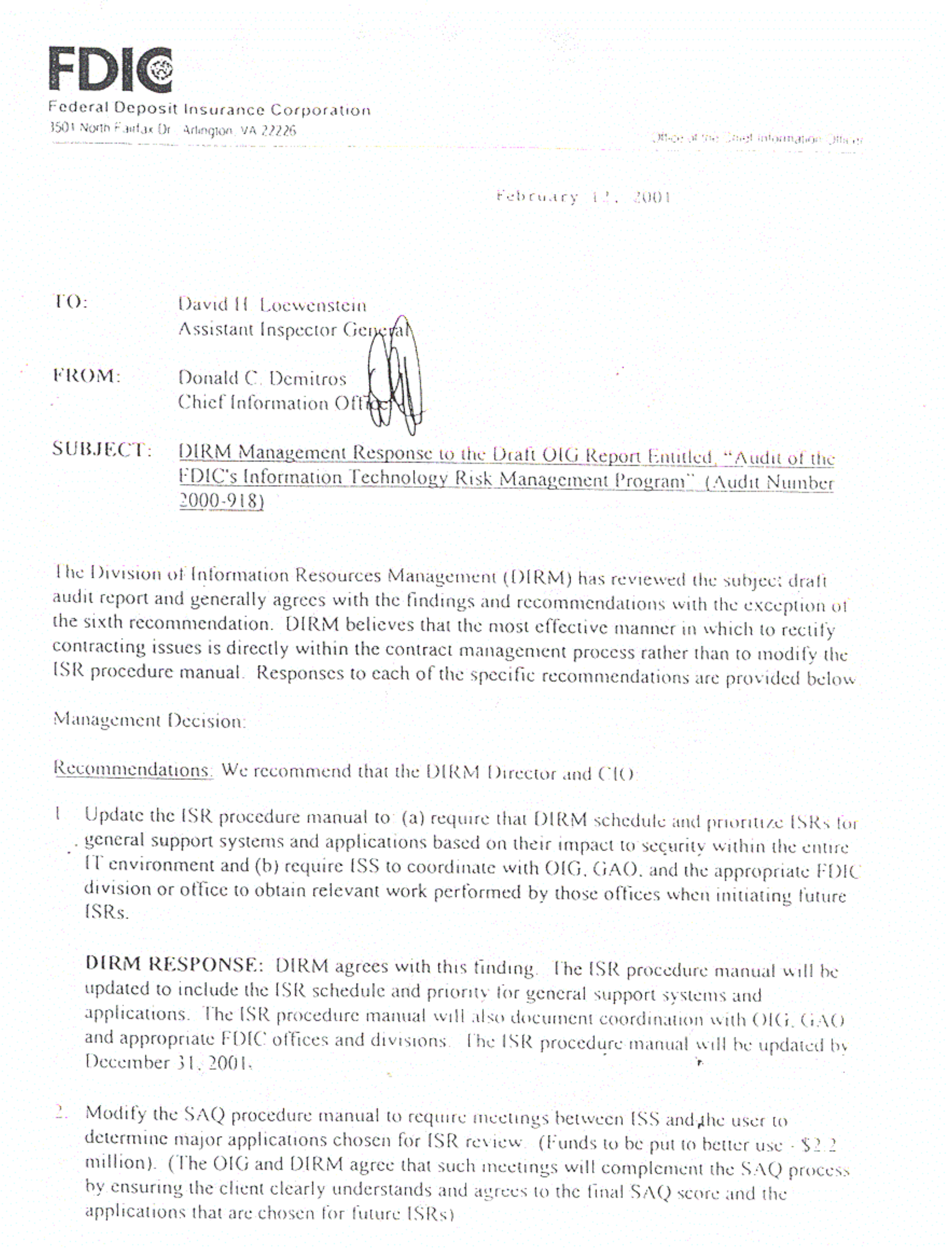
On February 12, 2001, the Director, DIRM, and CIO provided a written response to the draft audit report. The CIO and DIRM Director agreed with the report's findings and recommendations and provided the elements necessary for management decisions on all nine of the report's recommendations. DIRM's response is presented in its entirety in Appendix I of this report.

Regarding recommendation 6, the Director, DIRM and CIO indicated DIRM would prefer to address the finding and recommendation as a contract management issue rather than as an amendment to the ISR procedure manual. DIRM will ensure that the Oversight Manager for the contract will be reminded, in writing, of his responsibilities relative to the management of the contract. The Oversight Manager's supervisor will ensure that sound contract management and invoice review processes are in place and are being followed. We agree that these actions are responsive to our concerns and should resolve the weaknesses we noted concerning adequate review of invoices and working papers.

As a result of our audit, we will report funds put to better use of $2.2 million over 3 years in our *Semiannual Report to the Congress*.

APPENDIX I

CORPORATION COMMENTS



FDIC

Federal Deposit Insurance Corporation
3501 North Fairfax Dr., Arlington, VA 22226

Office of the Chief Information Officer

February 12, 2001

TO: David H. Loewenstein
Assistant Inspector General

FROM: Donald C. Demitros
Chief Information Officer

SUBJECT: DIRM Management Response to the Draft OIG Report Entitled, "Audit of the FDIC's Information Technology Risk Management Program" (Audit Number 2000-918)

The Division of Information Resources Management (DIRM) has reviewed the subject draft audit report and generally agrees with the findings and recommendations with the exception of the sixth recommendation. DIRM believes that the most effective manner in which to rectify contracting issues is directly within the contract management process rather than to modify the ISR procedure manual. Responses to each of the specific recommendations are provided below.

Management Decision:

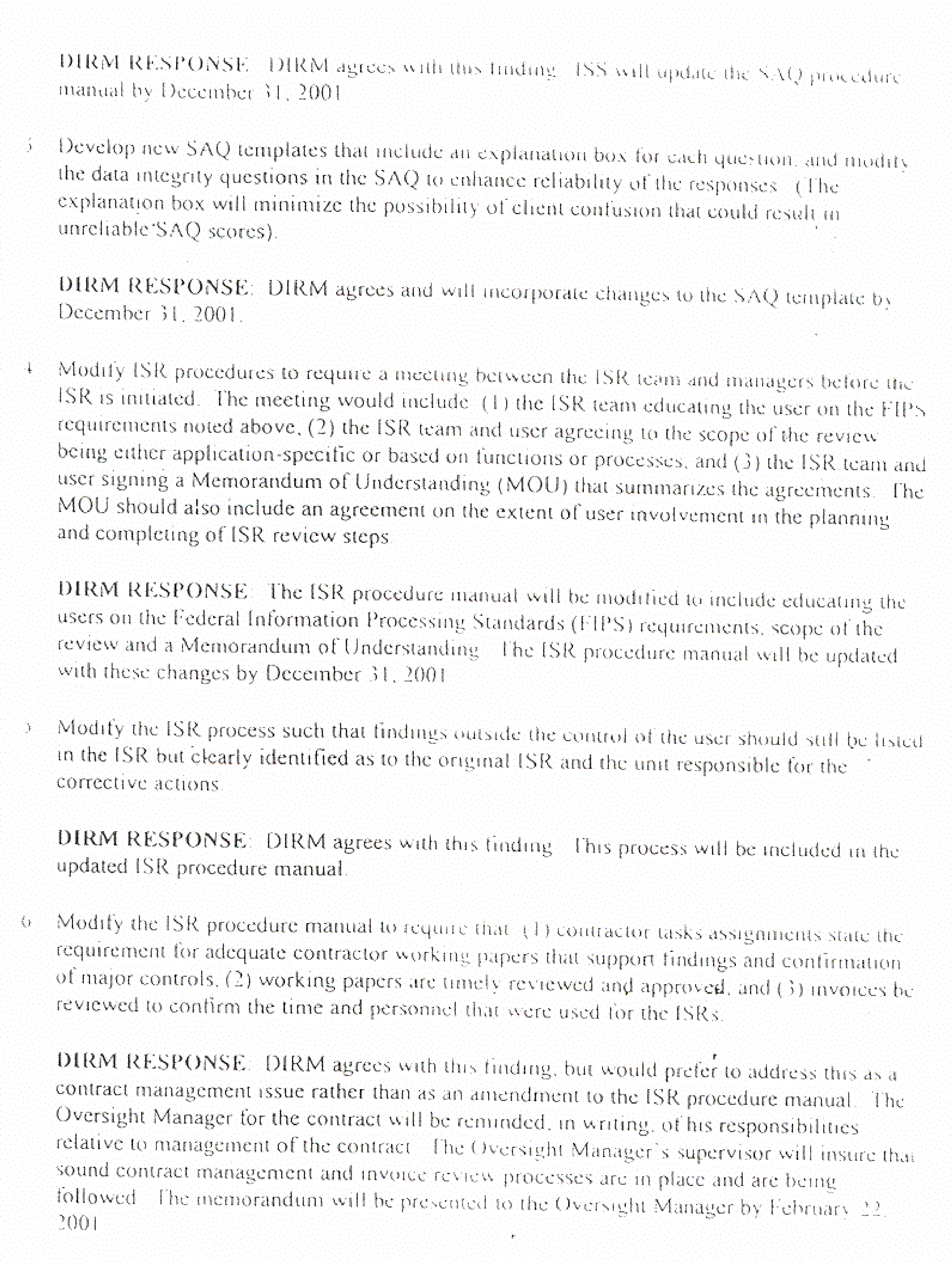
Recommendations: We recommend that the DIRM Director and CIO:

1. Update the ISR procedure manual to: (a) require that DIRM schedule and prioritize ISRs for general support systems and applications based on their impact to security within the entire IT environment and (b) require ISS to coordinate with OIG, GAO, and the appropriate FDIC division or office to obtain relevant work performed by those offices when initiating future ISRs.

   DIRM RESPONSE: DIRM agrees with this finding. The ISR procedure manual will be updated to include the ISR schedule and priority for general support systems and applications. The ISR procedure manual will also document coordination with OIG, GAO and appropriate FDIC offices and divisions. The ISR procedure manual will be updated by December 31, 2001.

2. Modify the SAQ procedure manual to require meetings between ISS and the user to determine major applications chosen for ISR review. (Funds to be put to better use - $2.2 million). (The OIG and DIRM agree that such meetings will complement the SAQ process by ensuring the client clearly understands and agrees to the final SAQ score and the applications that are chosen for future ISRs)

CORPORATION COMMENTS



DIRM RESPONSE: DIRM agrees with this finding. ISS will update the SAQ procedure manual by December 31, 2001.

3 Develop new SAQ templates that include an explanation box for each question, and modify the data integrity questions in the SAQ to enhance reliability of the responses. (The explanation box will minimize the possibility of client confusion that could result in unreliable SAQ scores).

DIRM RESPONSE: DIRM agrees and will incorporate changes to the SAQ template by December 31, 2001.

4 Modify ISR procedures to require a meeting between the ISR team and managers before the ISR is initiated. The meeting would include: (1) the ISR team educating the user on the FIPS requirements noted above, (2) the ISR team and user agreeing to the scope of the review being either application-specific or based on functions or processes, and (3) the ISR team and user signing a Memorandum of Understanding (MOU) that summarizes the agreements. The MOU should also include an agreement on the extent of user involvement in the planning and completing of ISR review steps.

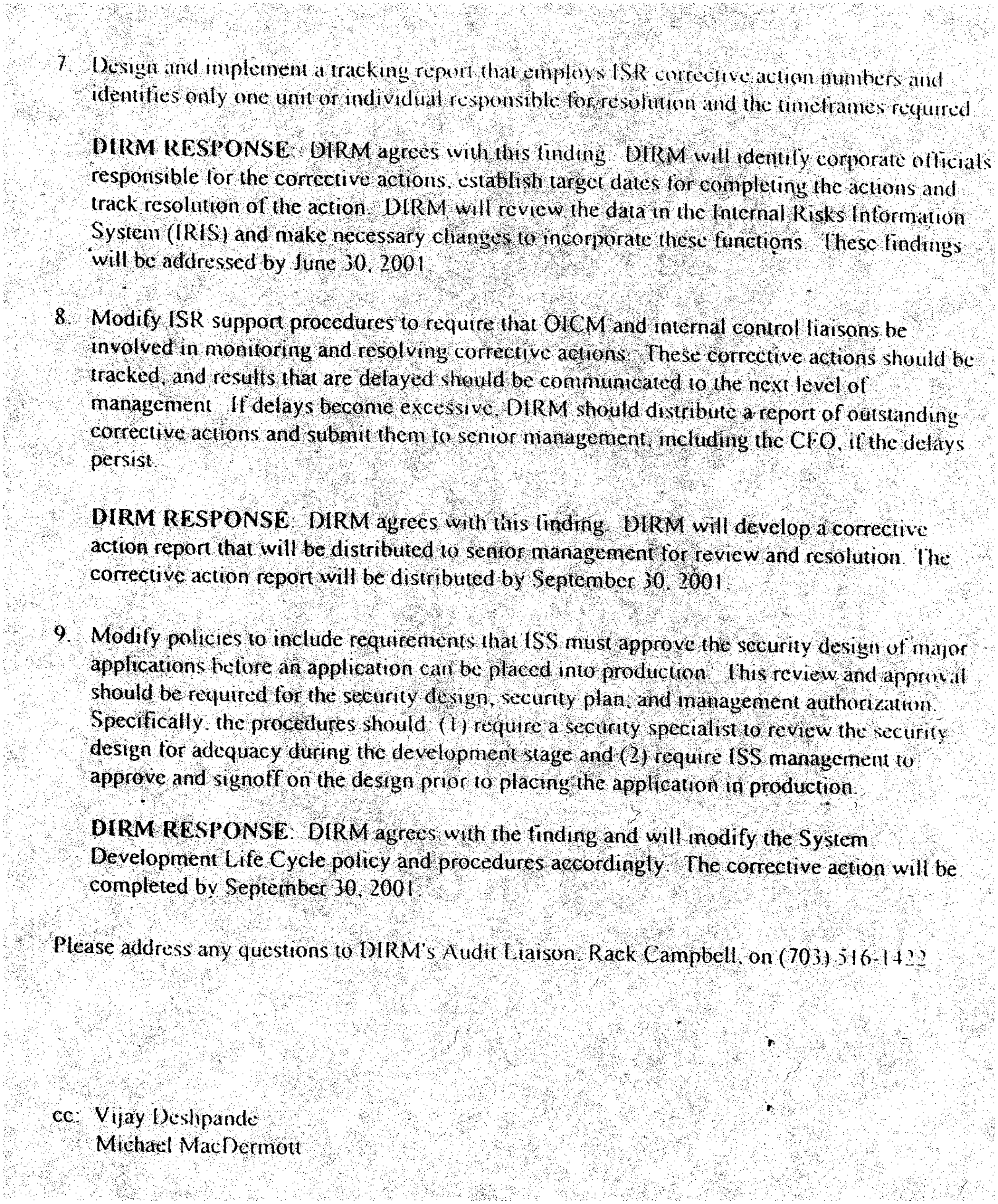
DIRM RESPONSE: The ISR procedure manual will be modified to include educating the users on the Federal Information Processing Standards (FIPS) requirements, scope of the review and a Memorandum of Understanding. The ISR procedure manual will be updated with these changes by December 31, 2001.

5 Modify the ISR process such that findings outside the control of the user should still be listed in the ISR but clearly identified as to the original ISR and the unit responsible for the corrective actions.

DIRM RESPONSE: DIRM agrees with this finding. This process will be included in the updated ISR procedure manual.

6 Modify the ISR procedure manual to require that: (1) contractor tasks assignments state the requirement for adequate contractor working papers that support findings and confirmation of major controls, (2) working papers are timely reviewed and approved, and (3) invoices be reviewed to confirm the time and personnel that were used for the ISRs.

DIRM RESPONSE: DIRM agrees with this finding, but would prefer to address this as a contract management issue rather than as an amendment to the ISR procedure manual. The Oversight Manager for the contract will be reminded, in writing, of his responsibilities relative to management of the contract. The Oversight Manager's supervisor will insure that sound contract management and invoice review processes are in place and are being followed. The memorandum will be presented to the Oversight Manager by February 22, 2001.



7. Design and implement a tracking report that employs ISR corrective action numbers and identifies only one unit or individual responsible for resolution and the timeframes required

   DIRM RESPONSE: DIRM agrees with this finding. DIRM will identify corporate officials responsible for the corrective actions, establish target dates for completing the actions and track resolution of the action. DIRM will review the data in the Internal Risks Information System (IRIS) and make necessary changes to incorporate these functions. These findings will be addressed by June 30, 2001.

8. Modify ISR support procedures to require that OICM and internal control liaisons be involved in monitoring and resolving corrective actions. These corrective actions should be tracked, and results that are delayed should be communicated to the next level of management. If delays become excessive, DIRM should distribute a report of outstanding corrective actions and submit them to senior management, including the CFO, if the delays persist.

   DIRM RESPONSE: DIRM agrees with this finding. DIRM will develop a corrective action report that will be distributed to senior management for review and resolution. The corrective action report will be distributed by September 30, 2001.

9. Modify policies to include requirements that ISS must approve the security design of major applications before an application can be placed into production. This review and approval should be required for the security design, security plan, and management authorization. Specifically, the procedures should: (1) require a security specialist to review the security design for adequacy during the development stage and (2) require ISS management to approve and signoff on the design prior to placing the application in production.

   DIRM RESPONSE: DIRM agrees with the finding and will modify the System Development Life Cycle policy and procedures accordingly. The corrective action will be completed by September 30, 2001.

Please address any questions to DIRM's Audit Liaison, Rack Campbell, on (703) 516-1422

cc: Vijay Deshpande
Michael MacDermott

APPENDIX II

MANAGEMENT RESPONSES TO RECOMMENDATIONS

The Inspector General Act of 1978, as amended, requires the OIG to report the status of management decisions on its recommendations in its semiannual reports to the Congress. To consider FDIC's responses as management decisions in accordance with the act and related guidance, several conditions are necessary. First, the response must describe for each recommendation

- the specific corrective actions already taken, if applicable;
- corrective actions to be taken together with the expected completion dates for their implementation; and
- documentation that will confirm completion of corrective actions.

If any recommendation identifies specific monetary benefits, FDIC management must state the amount agreed or disagreed with and the reasons for any disagreement. In the case of questioned costs, the amount FDIC plans to disallow must be included in management's response.

If management does not agree that a recommendation should be implemented, it must describe why the recommendation is not considered valid. Second, the OIG must determine that management's descriptions of (1) the course of action already taken or proposed and (2) the documentation confirming completion of corrective actions are responsive to its recommendations.

This table presents the management responses that have been made on recommendations in our report and the status of management decisions. The information for management decisions is based on management's written response to our report.

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Documentation That Will Confirm Final Action	Monetary Benefits	Management Decision: Yes or No
1	The ISR procedure manual will be updated to include the ISR schedule and priority for general support systems and applications. The ISR procedure manual will also document coordination with OIG, GAO, and appropriate FDIC offices and divisions.	December 31, 2001	Updated procedures in ISR procedure manual	N/A	Yes
2	ISS will update the SAQ procedure manual.	December 31, 2001	Updated procedures in SAQ procedure manual	$2.2 million over 3-year ISR cycle	Yes
3	ISS will modify SAQ template by: (1) including explanation box for each question and (2) modifying data integrity questions identified in the audit.	December 31, 2001	SAQ template	N/A	Yes

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Documentation That Will Confirm Final Action	Monetary Benefits	Management Decision: Yes or No
4	ISR procedure manual will be modified to include educating the users on the FIPS requirements, scope of the review, and MOU.	December 31, 2001	Updated procedures in ISR procedure manual	N/A	Yes
5	ISR procedure manual will be modified to require findings outside the control of the user to still be listed in the ISR but clearly identified as to the original ISR and the unit responsible for the corrective actions.	December 31, 2001	Updated procedures in ISR procedure manual	N/A	Yes
6	A memorandum will be developed and given to the Oversight Manager that will outline his responsibilities concerning workpaper and invoice reviews.	February 22, 2001	Memorandum to Oversight Manager	N/A	Yes
7	IRIS will include: (1) corporate officials responsible for the corrective actions, (2) target dates, and (3) tracking data relative to resolution of the corrective actions.	June 30, 2001	IRIS	N/A	Yes
8	Corrective Action Report will be developed and distributed to senior management for review and resolution.	September 30, 2001	Corrective Action Report	N/A	Yes
9	System Development Life Cycle Policy will be modified to require ISS approval of the security design of major applications before an application can be placed in production.	September 30, 2001	System Development Life Cycle Policy	N/A	Yes