Office of Inspector General

August 17, 2001
Audit Report No. 01-021

Improvements Can Be Made to the FDIC's Independent Security Review Process

OFFICE OF INSPECTOR GENERAL
DELIVERING QUALITY TIMELINESS VALUE
OFFICE OF AUDITS

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

Office of Audits
Office of Inspector General

DATE: August 17, 2001

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

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

SUBJECT: *Improvements Can Be Made to the FDIC's Independent Security Review Process*
(Audit Report Number 01-021)

During 2000, the Division of Information Resources Management (DIRM) requested that the Federal Deposit Insurance Corporation's (FDIC) Office of Inspector General (OIG) perform an independent security review (ISR) of the FDIC's mainframe computer system using the process and reporting guidance contained in DIRM's own draft *Risk Assessment/Independent Security Review and Management Authorization Program Guide*, dated August 25, 2000. We completed the review and provided our final report to DIRM on December 29, 2000.

At the time of the initial request, DIRM also asked that we comment on process-related improvement opportunities identified during our work on the ISR of the mainframe. Because we followed DIRM's ISR process in performing our mainframe review, we were able to identify improvements that would benefit DIRM's ISR program. These improvements are presented in this audit report.

The FDIC formalized its ISR process in 1997 with the initiation of the information technology risk management program, a program designed to identify and mitigate information technology risks and vulnerabilities. The OIG performed an audit of the FDIC's risk management program and issued a final report on March 14, 2001. In addition to recommendations for the overall risk management program, the report included recommendations addressing more specific ISR issues.
DIRM is currently reassessing its ISR approach and has agreed to take action on these recommendations and give serious consideration to more recent informal suggestions to improve the ISR program. DIRM has generally incorporated our recommendations and suggestions into its new processes and actively involved us in designing a new framework for the ISR program. Although DIRM has not formally documented these new processes, it has already taken action on several of the suggestions contained in this report and is in the process of implementing others.

BACKGROUND

The FDIC formalized its ISR program with the issuance of FDIC Circular 1310.3, *Information Technology Security Risk Management Program*, dated November 24, 1997. The ISR program was developed to address Office of Management and Budget Circular No. A-130, *Management of Federal Information Resources* (OMB A-130), which requires that independent security reviews of general support systems and major applications be performed every 3 years. Although the FDIC is an independent agency of the federal government, the FDIC determined that provisions of OMB A-130, Appendix III, establishing minimum controls for federal automated information security programs and linking agency automated information security programs and agency management control systems, are generally applicable to the FDIC.

ISRs are designed to identify risks and vulnerabilities in general support systems and major applications and to provide recommendations for mitigating those risks. The reviews focus on data integrity, confidentiality, and availability. OMB A-130 defines a major application as "an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application." OMB A-130 defines a general support system as "an interconnected set of information resources under the same direct management control which shares common functionality." The FDIC has identified 24 major applications and 8 general support systems (one of which is the FDIC's mainframe) to be reviewed during the 3-year cycle. DIRM spent more than $2 million in 2000 for its risk management and ISR program.

As described in DIRM's draft *Risk Assessment/Independent Security Review and Management Authorization Program Guide*, the ISR is a four-phase process that includes planning a system review, conducting a basic evaluation, conducting a detailed evaluation, and preparing an ISR evaluation report. During the system review planning phase, the ISR review team – an internal or contractor team – develops a technical description of the general support system or application and defines and documents review boundaries. The review team also identifies and documents security and integrity requirements – those related to the system or application under review and contained in federal and FDIC regulations and directives.

The team then performs a basic evaluation to verify that security controls have been implemented and a detailed evaluation to determine whether controls are functioning properly, cannot be circumvented, and satisfy performance criteria. The review team then summarizes the results in three separate reports: the System Evaluation Report (SER), the Control Matrix Report (CMR), and the ISR Evaluation Report. The report formats are standardized through reporting templates developed by a DIRM contractor hired to perform ISRs for the FDIC. The SER contains the review team's detailed findings along with recommended corrective actions. The SER also provides the reader with documents from the system planning phase, including the security and integrity requirements, the system description, and the independent review boundaries. Summary information on personnel interviewed, documents reviewed, tests conducted, and observations made is also presented in the SER.

The CMR contains a series of matrices that captures the related security and integrity requirements, the existing security and integrity control measures that fulfill these requirements, findings related to insufficient or nonexistent controls, and data security objectives that are answered by the control measures. The matrices summarize the threats that are mitigated by the identified security and control measures, summarize the sources used by the review team to verify the existence of the security and control measures (e.g. documentation, interviews, tests, and observations), and identify the security and integrity requirements not met by existing security and integrity control measures. For the requirements not met, the review team rates the likelihood of the vulnerability being exploited and the operational impact that may occur. The team also assigns a resulting priority value that helps FDIC management prioritize the vulnerabilities and allocate resources to address the identified vulnerabilities.

The final ISR Evaluation Report consolidates and summarizes the review findings, vulnerabilities, level of risk, and recommended corrective actions and once again presents the system description, review boundaries, and security and integrity requirements. The ISR Evaluation Report also contains a recommended Management Authorization Statement, authorizing use of the general support system or major application subject to certain conditions. FDIC management can opt to accept certain risks based on reasonable and documented operational necessity by considering the identified system vulnerabilities and the existence of compensating controls and/or complete the recommended corrective actions within agreed-upon timeframes.

The ISR reports are most useful to "clients" or system owners/users and FDIC management who need to be informed of risks and vulnerabilities associated with the FDIC's major applications and general support systems so that decisions can be made on authorizing the systems for use and taking corrective actions. The reports are also important to the oversight manager's evaluation of the ISR team's work and subsequent contractor billings, if any.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this report and our limited audit procedures was to identify and develop process-related observations and suggestions for improving the ISR program. We based our conclusions and suggestions on our experience while performing the ISR of the mainframe and our audit work related to the FDIC's information technology risk management program.

To further meet our objective, we held discussions with an OICM official responsible for monitoring a DIRM contractor's performance of the ISR of the Financial Information Management System General Ledger (FIMS-G/L) to obtain his observations on the process. Following those discussions, we analyzed the official's review notes and correspondence with the contractor and the FDIC oversight manager and the official's recommendations for changes to the ISR program. We drew conclusions based on our analysis of OICM's documentation and noted our concurrence with the official's concerns and conclusions.

We performed the additional audit procedures between January and April 2001 in accordance with generally accepted government auditing standards.

RESULTS OF REVIEW

The ISR program can be enhanced to better serve as an effective management tool for detecting security weaknesses. The following is a summation of those improvements as they relate to planning, performance, and reporting. An additional suggested improvement, obtaining client feedback, relates to all phases of the ISR.

- DIRM needs to further develop and enhance its ISR program policy.

- DIRM could improve the ISR program by ensuring that in subsequent review cycles, high-risk components of general support systems receive individual, more in-depth reviews.

- DIRM's point of contact needs to be more involved to ensure that the team develops an adequate test plan for confirming that controls are working as intended.

- DIRM could significantly improve reporting and management decision-making by streamlining the three ISR reports, consolidating them into one report, and developing separate formats for application and general support system reviews.

- DIRM needs to ensure that the ISR team obtains client input throughout the ISR process, most importantly as part of the team's efforts to develop an understanding of the client's environment.

- DIRM could also improve the ISR process by encouraging discussions between DIRM, the ISR team, and the client to reach a consensus and a clear understanding of the issues identified during the ISR.

During the course of our review, DIRM acknowledged weaknesses in its ISR program and draft ISR policy and began to address those weaknesses. The OIG and DIRM met informally on several occasions and exchanged ideas for redesigning the program. DIRM has also initiated corrective actions in response to recommendations presented in our risk management audit report. The suggestions within this report are intended to aid DIRM in its efforts to revamp the ISR program and move forward to formalize program policy. As part of its ISR program redesign efforts, DIRM decided to discontinue its use of contractors, who at one time performed the ISRs in their entirety.

THE ISR PLANNING PROCESS COULD BE IMPROVED

DIRM's ISR planning process could be improved by further developing policy for the ISR program, including sample documents, review procedures, and test requirements for general

support system ISRs. The draft policy could also be enhanced by requiring an evaluation of FDIC IT security policies and standards against applicable federal regulations to ensure that criteria used for the ISRs is consistent with governing regulations.

Sample Documents Should Be Developed for General Support System ISRs

DIRM had not developed sample documents that could be used during the system review planning phase to document the system description and the independent review boundaries for general support system ISRs. Although DIRM, in conjunction with the ISR of the mainframe, provided us with sample documents that would be helpful in planning a review of a major application, DIRM did not have sample documents available for the review of a general support system because an ISR of a general support system had not yet been completed. Because different language needs to be included in the planning documents for major applications and general support systems to comply with applicable federal regulations, it is important that DIRM develop sample documents to assist the review teams in their planning efforts.

OMB A-130 refers to National Institute of Standards and Technology (NIST) Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems,* dated December 1998. NIST, an entity within the United States Department of Commerce, is charged with developing generally accepted system security principles and practices for the federal government. NIST 800-18 contains descriptions of general support system operational and technical controls that should be included in general support system ISRs; thus, the controls should be referenced in the system review planning documents. For the ISR of the mainframe, the OIG review team had to make numerous revisions to the major application sample documents to incorporate the necessary general support system language and ensure compliance with NIST 800-18. Consequently, DIRM's development of sample system descriptions and review boundaries documents for general support system ISRs would benefit the ISR process in two ways. The sample documents would lessen the time required for the review teams to develop the proper documents and ensure compliance with the pertinent regulations.

Review Procedures and Test Requirements Should Be Developed for General Support System ISRs

DIRM had not developed ISR review procedures or test requirements that addressed security considerations applicable to general support systems. DIRM's draft policy was focused primarily on reviews of major applications, leaving the review teams with a need for specific guidance on general support systems. DIRM should develop specific guidance in the form of review procedures and test requirements that consider general support system controls and guide the review teams in performing general support system ISRs.

Because of the inherent differences between major applications and general support systems as defined previously, OMB A-130 and NIST 800-18 separately describe the security controls required for major application and general support system ISRs. DIRM's draft *Risk*

Assessment/Independent Security Review and Management Authorization Program Guide does not make that distinction, but rather combines the discussion of major application and general support system security controls and requirements, focusing primarily on major applications. DIRM needs to develop policies and procedures that will address those distinctions along with review procedures and test requirements that take into account general support system controls. By doing so, DIRM could ensure that the review teams do not improperly omit requirements that are specific to general support systems such as physical security, access and environmental controls, separation of duties, and continuity of operations – omissions that could negatively impact the quality and effectiveness of the review and compliance with OMB A-130 and NIST 800-18.

The ISR Process Should Include an Evaluation of FDIC IT Security Policies and Standards Against Governing Federal Regulations and Guidance

In planning the ISR, the review team establishes security and integrity requirements and criteria for the review by identifying FDIC IT security policies and standards and federal regulations applicable to the system under review. DIRM could improve this process by requiring an evaluation of FDIC IT security policies and standards against governing federal regulations to ensure that the FDIC's security policies and standards are adequate and consistent with federal regulations. After performing an initial full assessment, periodic assessments could be performed to ensure consistency with updated regulations and to reflect changes in the environment.

FDIC Circular 1310.3 mandates that general support systems and major applications undergo a periodic ISR. The method used for performing the ISR involves assessing the degree to which security and integrity requirements are satisfied for the system or application under review. ISR security and integrity requirements are formulated by drawing from applicable federal regulations, such as OMB A-130, and FDIC IT security policies and standards, such as FDIC Circular 1360.10, *Corporate Password Standards*. The draft *Risk Assessment/ Independent Security Review and Management Authorization Program Guide* and Circular 1310.3 provide for using FDIC IT security policies and standards to establish ISR security and integrity requirements but do not require an evaluation of the FDIC's IT security policies and standards against governing regulations to ensure consistency. Consequently, the existing ISR process may not provide full assurance that FDIC IT security policies and standards conform to continually evolving federal computer security laws, regulations, standards, and best practices. Ensuring that FDIC IT security policies and standards conform to federal laws, regulations, standards, and best practices is increasingly important because of the increased focus on security and the rapid changes in technology, related guidance, and best practices.

By first performing a full assessment of its IT security policies and standards and then performing periodic assessments to ensure consistency with updated regulations, standards, and best practices and to reflect changes in the environment, the FDIC can ensure that criteria used for the ISRs is consistent, relevant, and appropriate. Such an ISR process change will improve the effectiveness and efficiency of the FDIC ISR process by precluding the use of outdated and ineffective security and integrity requirements.

We suggest that the FDIC Chief Information Officer and DIRM Director ensure that DIRM's draft ISR policy is further developed, enhanced, and implemented for major applications and general support systems. In so doing, the FDIC Chief Information Officer and DIRM Director should ensure that:

(1) Sample documents are developed for general support system ISRs to ensure the efficiency of the ISR process and compliance with pertinent federal regulations.

(2) Review procedures and test requirements for use in performing general support system ISRs are developed to ensure the ISRs' compliance with OMB A-130 and NIST 800-18.

(3) For major applications and general support systems, an initial assessment and then periodic updates of FDIC IT security policies and standards are performed to ensure consistency with governing federal regulations, standards, and best practices.

DIRM COULD IMPROVE GENERAL SUPPORT SYSTEM ISRs AND INCREASE ISR OVERSIGHT

DIRM could improve the ISR program by ensuring that in subsequent review cycles, high-risk components of general support systems receive individual security reviews. DIRM could also improve the program by increasing oversight of the performance of the ISRs.

High-risk Components of a General Support System Should Have Individual Security Reviews

In our audit of the risk management program, we identified the need for DIRM to conduct ISRs of general support systems prior to performing ISRs of major applications. By doing so, DIRM could prevent the inclusion of redundant and non-application-specific findings and corrective actions in the various application ISRs and improve the ISRs' quality and effectiveness. Another method for improving quality and effectiveness (once general support system ISRs are completed and a baseline is established) is to segment ISRs of general support systems such as the mainframe into multiple reviews spread out over the 3-year review cycle.

DIRM's current ISR procedures of including all components of a general support system in a single review satisfy OMB A-130 requirements. OMB A-130 instructs agencies to "review the security controls in each system when significant modifications are made to the system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system." Performing subsequent reviews of individual components could be less burdensome, promote a more detailed and focused approach to completing the ISRs, and result in more in-depth reviews that provide better assurances about the security and integrity controls of high-risk components of the FDIC IT environment. Additionally, milestones for completing the ISRs could be set more realistically in line with the size of the component under review. DIRM indicated that it would consider this approach after its ISR program had matured, but felt that

resource constraints and the additional time needed to rank risks necessitated delaying a decision on this approach.

DIRM schedules ISRs for its general support systems at least once every 3 years in accordance with OMB A-130 requirements, commensurate with the acceptable level of risk for the system. The layered components of the mainframe, such as Computer Associates Access Control Facility2 (CA-ACF-2), database packages (DB2 and DATACOM)), Customer Interface Control System (CICS), and the operating system (OS/390), individually involve functions and transactions that pose a high level of risk to the FDIC IT environment and warrant in-depth individual reviews. OMB A-130 recognizes that the greatest security risk comes from authorized individuals engaging in improper activities, whether intentional or accidental. The layered components include technical, operational, and management controls that are used to prevent and detect these improper activities. Such controls are intended to ensure individual accountability, "least privilege," and separation of duties. OMB A-130 defines least privilege as "the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job."

The recently completed ISR of the mainframe included a security review of the OS/390 operating system and the layered products CA-ACF2, DB2, and DATACOM. If these components had been reviewed individually, the reviews could have been more in-depth and meaningful. Individual in-depth reviews could have provided better assurance that security and integrity controls of these high-risk components (1) were functioning properly, (2) satisfied performance criteria, and (3) were unable to be disarmed or circumvented.

Further Improvements Should Be Made to ISR Oversight

In our report on DIRM's risk management program, we noted improvements that could be made to oversight to enhance the ISR process. In particular, we recommended that DIRM modify the ISR procedure manual to require adequate working papers from contractors to support ISR findings and confirmation of major controls. We also recommended modifying the manual to require a timely review and approval of contractor working papers and invoices by the FDIC program or oversight manager. We identified additional oversight improvements that should be made based on our discussions with an OICM official and our review of OICM's documentation related to the ISR of FIMS-G/L.

Most notably, OICM's experience revealed the need for more involvement by DIRM's point of contact to ensure that the ISR team (internal or contractor team) develops an adequate test plan to confirm that controls are working as intended. The OICM official found that testing performed by the contractor was not always adequate and, in some cases, the contractor relied on information provided during discussions rather than performing actual testing. By obtaining a test plan from the ISR team and verifying its adequacy, DIRM could better ensure that the team's review will be sufficient to confirm that controls are working as intended. OICM's experience also reflected the need for a timeline from the team to ensure that adequate time has been allotted for (1) finalizing supporting working papers and draft deliverables, (2) reviewing working papers and deliverables and resolving reviewer comments, and (3) obtaining feedback from the clients and making appropriate report revisions. These oversight improvements could have a positive impact on the reliability and effectiveness of the ISRs by ensuring the adequacy and completeness of the ISR team's work.

OICM also documented concerns similar to those noted in our audit of DIRM's risk management program. Those concerns related to the need for obtaining adequate working papers from the contractor to support all ISR findings, conclusions, and tests of major controls; and performing a timely review of all supporting working papers prior to draft report issuance. In response to our audit of the risk management program, DIRM agreed with the need to obtain supporting working papers from the contractor and improve working paper reviews. DIRM also responded that it would consult with the OIG to develop working paper standards. DIRM's recent adoption of an audit-type approach for the ISRs should address the needed working paper improvements.

DIRM has indicated that it would use internal review teams in lieu of contractors to perform future ISRs. Such actions would be consistent with our prior informal suggestions to DIRM and suggestion number 11 of this audit report.

We suggest that the FDIC Chief Information Officer and DIRM Director ensure that:

(4) Changes are made to the ISR program after ISRs of general support systems are completed and a baseline is established so that: (a) general support system components that warrant individual reviews are planned and conducted individually to enhance their value; (b) individual support system components, particularly mainframe components that would warrant individual ISRs based on OMB A-130 guidelines, are identified, scheduled, and prioritized based on their relative risk to the Corporation; and (c) milestones for completing the ISRs are set based on the size of the component.

(5) Improvements are made to oversight to increase the involvement of DIRM's point of contact and ensure that the ISR team: (a) develops an adequate test plan for confirming that controls are working as intended and (b) provides a timeline that allows adequate time for finalizing supporting working papers and draft deliverables, reviewing working papers and deliverables and resolving reviewer comments, and obtaining feedback from the clients and making the appropriate report revisions. In its adoption of an audit-type approach for the ISRs, DIRM should continue its efforts to require adequate working papers to support all ISR findings, conclusions, and tests of major controls and to ensure a timely review of all working papers.

ISR REPORT FORMAT SHOULD BE MODIFIED TO IMPROVE CLARITY AND USEFULNESS

DIRM's ISR reporting process could be improved by streamlining the reports to benefit both the client and the review team and enhancing the reporting format to clearly identify the work performed and level of review.

The ISR Reporting Format Should Be Streamlined

In developing reports for the ISR of the mainframe, we noted that the current ISR reporting format resulted in a voluminous report containing redundancies and inconsistencies, making it difficult for the client to discern the important issues. The reporting format was also cumbersome and time-consuming for the review team to complete, a condition that may have increased billable time for contractor-prepared reports and could increase the cost of internal resources needed for future ISRs. Consequently, we believe the reporting format should be streamlined.

The three reporting vehicles – the CMR, the SER, and the ISR Evaluation Report – were developed by a DIRM contractor in an effort to comply with various federal regulations. The various reports restate review findings, recommended corrective actions, and other ISR information in different and similar formats. The reports contain repetitive executive summaries, review scopes, review methodologies, evaluation methodologies, system descriptions, independent review boundaries, and introductions. Among the three reports, findings and/or recommended corrective actions, security and integrity requirements and/or control measures, and tests conducted/vulnerabilities are presented numerous times in various formats.

The ISR reports are intended for use by "clients" or system owners/users, FDIC management, and the DIRM oversight manager. The reports should inform clients and FDIC management of risks and vulnerabilities associated with the FDIC's major applications and general support systems so that decisions can be made on authorizing the systems for use and taking corrective actions. The reports also are important to the oversight manager's evaluation of the team's work and subsequent billings should contractors be used for future ISRs. However, the voluminous and redundant nature of the reports makes it difficult for the various users to effectively use the information contained in them.

The redundancy of the three reports also creates problems with consistency. As noted by the OIG review team and OICM, a change made to the reports had to be made in several places, often resulting in errors to the draft reports when the change was not reflected throughout the three reports. For example, if a recommended corrective action was changed, the change had to be made six times – in three sections of the ISR Evaluation Report, two sections of the SER, and one section of the CMR. If all occurrences of the same information were not changed, conflicting and confusing information could have been conveyed to the client. During OICM's review of the final draft report for FIMS G/L, OICM's review notes indicated that the CMR included issues that had been deleted from the remainder of the report. These issues involved a potential heating and air conditioning (HVAC)-related exposure that was determined not to be a risk and a potential exposure involving the Virginia Square garage doors that was determined to be an acceptable risk with compensating controls in place.

By streamlining the three reports and consolidating them into one report, duplicate information can be eliminated thereby resolving the consistency issue. Additionally, because of the inherent differences between an application review and a general support system review, developing separate reporting formats for application and general support system reviews would also be an

important enhancement. Together, these enhancements could increase the ISR report's readability and effectiveness and lessen the report preparation time and associated costs.

The ISR Report Should Clearly Identify the Work Performed

The ISR report format did not provide a clear identification of the work performed for the ISR, the level of testing, or the sampling methodology. The format also promoted the presentation of information and conclusions on issues not specifically related to the system under review, a concern similar to one addressed in our audit of the risk management program. Providing the client with a clear indication of the level or depth of review is important for adding perspective to the ISR results and conclusions and for aiding the oversight manager in his/her review and approval of the team's work and subsequent contractor billings, if any. Because of DIRM's reliance on the ISR team's work and the impact of that work on FDIC operations, it is important that all parties have a clear understanding of the extent of the review.

The report format provides a list of tests performed for the ISR. However, the matrices and other reporting sections do not provide additional descriptive information, such as the level of testing performed, to confirm that controls are working as intended or the sampling approach and methodology used for testing. Consequently, such information is not conveyed to the client through the reports.

To compound this issue, the report format allows for issues or areas to be addressed that are not specific to the general support system or application under review, resulting in the inclusion of issues that were identified for other ISRs. Not only can this confuse the client and limit his/her understanding of the ISR, it may also make it more difficult for the oversight manager to identify the work that was actually performed for the ISR and determine whether the work and level of effort incurred by the team and/or billed by the contractor was reasonable.

We suggest that the FDIC Chief Information Officer and DIRM Director ensure that:

(6) The ISR reporting format is streamlined in a manner that will highlight the important issues, better serve the client, and expedite the reporting process.

(7) Two separate reporting formats are developed – one format for ISRs of major applications and a second format for ISRs of general support systems.

(8) The ISR report format is enhanced to clearly identify the work performed, level of testing, and sampling methodology.

(9) The ISR report format is revised to clearly present the security and integrity requirements, conclusions, corrective actions, and related information applicable to the major application or general support system under review.

ISRs SHOULD INCLUDE CLIENT FEEDBACK

The contractor hired by DIRM to perform ISRs did not always obtain the client's views or incorporate those views or comments into the various planning, performance, and reporting documents. According to the contractor, client feedback and concurrence was not always obtained or incorporated into the ISR documents because of the independent nature of the review. However, OMB A-130 states that "security controls may be reviewed by an independent audit or a self review. The type and rigor of review or audit should be commensurate with the acceptable level of risk that is established in the rules for the system and the likelihood of learning useful information to improve security."

We believe that client input should be obtained during all phases of the ISR, including the planning phase when the system description and independent review boundaries are determined and the evaluation and reporting phases when the results, conclusions, and corrective actions are drafted. Obtaining client involvement or feedback during the planning phase can assist the review team in gaining a thorough understanding of the user and the environment, identifying high-risk areas, and setting boundaries for the review, resulting in a more valuable and useful product for the client. During the evaluation and reporting phases, client feedback on results, conclusions, and proposed corrective actions can help ensure the accuracy of the ISR data and the usefulness of the corrective actions.

Obtaining client involvement can be accomplished through the use of a divisional or interdivisional review team to perform all or some phases of the ISR. Such a team could benefit the ISR program by eliminating or reducing contractor involvement and increasing the value and usefulness of the ISR to the client.

During our audit of the risk management program, we interviewed clients from divisions that recently were involved in the ISR process. Those divisions included the Division of Supervision, the Division of Finance, and the Division of Resolutions and Receiverships. Division managers expressed concerns that responsible division personnel were not contacted at any time during the ISR process. As a result, the managers believed that the contractor lacked an understanding of the user, the environment, and the high-risk areas, causing the ISR reports and corrective actions to be less than fully effective. Additionally, although most division managers acknowledged receipt of the draft reports, they stated that feedback or comments provided to the contractor on findings and corrective actions were not always included in the final reports. All in all, managers expressed a lack of confidence when signing the Management Authorization Statement.

For an ISR report to be an effective management tool, it should be complete, accurate, objective, convincing, clear, and concise. One of the most effective ways to accomplish this is to provide the client (i.e., responsible officials) with copies of the draft reports for their review and comment and include those comments in the final ISR report. The officials' comments should indicate their agreement or disagreement with the findings, corrective actions, and other information presented in the reports; the basis for the agreement/disagreement; and plans for resolution. The draft *Risk Assessment/Independent Security Review and Management Authorization Program Guide* allows for obtaining client feedback throughout the ISR process and instructs the team to provide the client with a draft SER, CMR, and ISR Evaluation Report for review and comment. The team is then to revise the reports and prepare a final ISR Evaluation Report incorporating the client comments. The guide also requires the team to submit various planning documents to the client for review and comment, including the system description, the independent review boundaries, and the security and integrity

control requirements.

Discussions between DIRM, the ISR team, and the client could also improve the process. Should the team disagree with the client's response, discussions could be held to reach a consensus or understanding of the issue and how it will be treated for reporting purposes. DIRM's point of contact could also ensure that disagreements with the ISR team, such as those related to findings, corrective actions, work performed, or other report information, are resolved prior to issuing the draft ISR reports. OICM noted that there is not a process or method in place to resolve disagreements between the point of contact and the ISR team. DIRM agreed that a resolution vehicle is needed and responded that with its new audit-type approach for the ISRs, OICM will now play the role of dispute mediator. Additionally, OICM commented that DIRM's actions in transferring responsibility for the ISR program to DIRM's Information Technology Evaluation Section resolve potential objectivity concerns that could arise between the DIRM Information Security Staff and the ISR team.

We suggest that the FDIC Chief Information Officer and DIRM Director ensure that:

(10) Client feedback is obtained and considered during all phases of the ISR.

(11) Consideration is given to using a divisional or interdivisional team to perform certain phases or all phases of the ISR.

(12) All ISR reports contain the views of responsible officials concerning conclusions, recommendations, and planned corrective actions.

(13) A process or method is developed for resolving disagreements between the point of contact and the ISR team.

CORPORATION COMMENTS AND OIG EVALUATION

On August 13, 2001, the FDIC's Chief Information Officer (CIO) and DIRM Director provided a written response to the suggestions contained in the draft report. The CIO and DIRM Director's response is presented in Appendix I of this report. The CIO and DIRM Director generally agreed with the information presented in the report with the exception of suggestion 4. With respect to suggestions 1 through 3 and 5 through 13, DIRM responded that it has begun to revise the ISR procedures manual, the ISR report format, and the ISR process to incorporate our suggested improvements.

A summary of the CIO and DIRM Director's response to suggestion 4 and our analysis follows.

Ensure changes are made to the ISR program after ISRs of general support systems are completed and a baseline is established so that: (a) general support system components that warrant individual reviews are planned and conducted individually to enhance their value; (b) individual support system components, particularly mainframe components that would warrant individual ISRs based on OMB A-130 guidelines, are identified, scheduled, and prioritized based on their relative risk to the Corporation; and (c) milestones for completing the ISRs are set based on the size of the component (suggestion 4): The CIO and DIRM Director disagreed with this suggestion. The CIO and DIRM Director stated that component reviews may provide more in-depth coverage but also would entail significant resources because of an increase in the number of reviews that would need to be conducted. The CIO and DIRM Director stated that the Sensitivity Assessment Questionnaire (SAQ) that measures the risk of major applications is undergoing revision as recommended in the OIG's Risk Management audit report (Audit Report No. 01-007). Further, the CIO and DIRM Director stated that he expects, although is not certain, that the revised SAQ will reduce the number of major applications and, thus, save money and resources and increase the quality of the remaining ISRs – all objectives of the OIG's Risk Management audit. The CIO and DIRM Director responded that it seems contrary to seek to reduce reviews in one area and increase them in another. The savings in cost, the reduction in resources, and the increased quality of the reviews would be lost.

The CIO and DIRM Director also responded that although these component reviews might be smaller if spread out, the burden on DIRM's internal clients will increase if component-based ISRs are performed in their program areas every year instead of once every three years. He also stated that these areas already receive audit coverage from the OIG and GAO. Further, the CIO and DIRM Director responded that recent general support system audits have not identified any significant threats to the Corporation. OMB A-130, Appendix III states that "the scope and frequency of the review should be commensurate with the acceptable level of risk for the system," and the "likelihood of learning useful information to improve security." The CIO and DIRM Director stated that at this time, DIRM believes that breaking general support systems into components for review would not significantly improve security for these systems.

Breaking general support systems into components for review allows DIRM to better focus on significant risks in those systems, and to provide greater assurance that security and integrity controls function properly, satisfy performance criteria, and are unable to be disarmed and circumvented. Accordingly, as DIRM officials indicated they would do during our review, we suggest the division reconsider its decision as the ISR process matures so there is more information and experience on which to make such a determination.

Because our report contained suggestions rather than formal recommendations, a management decision was not required.

In its response, DIRM referred to "confusion…as to the role of your staff when they are asked to participate in the design and development of a process." The OIG welcomes opportunities to work with management as it develops programs and systems, and anticipates we will continue to do so. We have flexibility in the manner in which we carry out our reporting responsibility under government auditing standards and make decisions in that regard on a case-by-case basis. Those decisions depend upon, among other things, the subject of our audit, the audit scope and methodology, and the significance of our findings. In this case, as we noted in our draft report transmittal, we believed the significance of independent security reviews warranted our providing management with an opportunity to review and comment on the findings and suggestions. Accordingly, we issued an "audit report" to provide management with a mechanism to do so and have included management's comments in their entirety as an appendix to this report.

Federal Deposit Insurance Corporation
3501 Fairfax Dr., Arlington, VA 22226
Office of the Chief Information Officer

August 9, 2001

TO: Stephen M. Beard
Deputy Assistant Inspector General

FROM: Donald C. Demitros [Electronically produced version; original signed by Donald C. Demitros]
Chief Information Officer

SUBJECT: Draft Report Entitled *Improvements Can Be Made to the FDIC's Independent Security Review Process*

The Division of Information Resources Management (DIRM) has reviewed the subject draft report and, with the exception of the fourth suggestion, generally agrees with the information presented. We appreciate the professional efforts of the Inspector General's (IG's) staff who have worked diligently with DIRM managers and provided valuable insights and suggestions throughout this effort. However, although your memo indicates that the report is not an audit, the second to last sentence of the memo calls it a "draft audit report". In addition, the first page of the report says improvements are presented in this "audit report". There already is an outstanding audit of this process; further, DIRM requested your staff's participation and comments on our process. There appears to be confusion as to the role of this document; but, more importantly, the role of your staff when they are asked to participate in the design and development of a process.

With regard to the fourth suggestion in this report, DIRM believes that increasing the number of independent security reviews (ISR) through component analysis for general support systems (GSS) is counterproductive in light of the recent OIG "Audit of the FDIC's Information Technology Risk Management Program" (Audit Number 2000-918). In that audit, the IG recommended reducing the number of ISRs performed to a more manageable number. DIRM agreed with that recommendation. At this time, DIRM believes that increasing the number of GSS reviews by examining their individual components will not substantially add to the "likelihood of learning useful information to improve security" as defined in OMB A-130, Appendix III. As our ISR process matures, we look forward to continuing our cooperative dialogue with the IG's staff to ensure that we identify any additional process improvements and potential best practices that could benefit our program. Our comments on each of the specific suggestions are provided below.

Suggestions: We suggest that the FDIC Chief Information Officer and DIRM Director ensure that DIRM's draft ISR policy is further developed, enhanced, and implemented for major applications and general support systems. In so doing, the FDIC Chief Information Officer and DIRM Director should ensure that:

1. Sample documents are developed for general support system ISRs to ensure the efficiency of the ISR process and compliance with pertinent federal regulations.

   DIRM Comment: DIRM agrees with this suggestion. The ISR procedure manual which is currently under revision will contain sample documents for general support systems (GSS) as well as for major applications (MA).

2. Review procedures and test requirements for use in performing general support system ISRs are developed to ensure the ISRs' compliance with OMB A-130 and NIST 800-18.

   DIRM Comment: DIRM agrees with this suggestion. The revised ISR procedure currently under revision will be based upon the review requirements contained in OMB A-130 and NIST 800-18.

3. For major applications and general support systems, an initial assessment and then periodic updates of FDIC IT security policies and standards are performed to ensure consistency with governing federal regulations, standards, and best practices.

   DIRM Comment: DIRM agrees with this suggestion. DIRM is conducting an evaluation of its IT security policies and standards against applicable federal regulations to ensure that criteria used for all ISRs continues to be consistent with governing regulations. Further, DIRM is updating its policy on IT Security Risk Management to ensure that it reflects the requirements of OMB A-130, Appendix III.

4. Changes are made to the ISR program after ISRs of general support systems are completed and a baseline is established so that: (a) general support system components that warrant individual reviews are planned and conducted individually to enhance their value; (b) individual support system components, particularly mainframe components that would warrant individual ISRs based on OMB A-130 guidelines, are identified, scheduled, and prioritized based on their relative risk to the Corporation; and (c) milestones for completing the ISRs are set based on the size of the component.

   DIRM Comment: Component reviews may provide more in-depth coverage but also would entail significant resources. The suggestion seems to imply that some type of sensitivity assessment questionnaire would have to be developed and implemented for GSS's that would identify components and component risks within the GSS. This would in turn increase the number of reviews that would need to be conducted. The Sensitivity Assessment Questionnaire (SAQ) that measures the risk of major applications is undergoing revision as recommended in the Risk Management Audit. It is expected, although not certain, that the revised SAQ will reduce the number of MAs and thus save money and resources and increase the quality of the remaining ISRs – all objectives of the former audit. It seems contrary to seek to reduce reviews in one area and increase them in another. The savings in cost, the reduction in resources and the increased quality of the reviews would be lost.

Although these component reviews might be smaller if spread out, the burden on our internal clients will increase if component-based ISRs are performed in their program areas every year instead of once every three years. These areas already receive audit coverage from the OIG and GAO. Recent GSS audits have not identified any significant threats to the Corporation. OMB A-130, Appendix III states that "the scope and frequency of the review should be commensurate with the acceptable level of risk for the system," and the "likelihood of learning useful information to improve security". At this time, DIRM believes that breaking GSSs into components for review would not significantly improve security for these systems.

5. Improvements are made to oversight to increase the involvement of DIRM's point of contact and ensure that the ISR team: (a) develops an adequate test plan for confirming that controls are working as intended and (b) provides a timeline that allows adequate time for finalizing supporting working papers and draft deliverables, reviewing working papers and deliverables and resolving reviewer comments, and obtaining feedback from the clients and making the appropriate report revisions. In its adoption of an audit-type approach for the ISRs, DIRM should continue its efforts to require adequate working papers to support all ISR findings, conclusions, and tests of major controls and to ensure a timely review of all working papers.

   DIRM Comment: DIRM agrees with this suggestion. Under the revised procedure, the ISR Team Leader will be responsible for oversight and development of an adequate test plan and a project plan that allows adequate time for all steps of the ISR to be performed and documented. The Team Leader will be responsible for reviewing work papers and assuring that they provide adequate support of the ISR findings, conclusions and tests. To improve oversight, the ISR program has been moved to the Information Technology Evaluation Section (ITES) and the ISR's themselves are being conducted by FDIC staff rather than contractors.

6. The ISR reporting format is streamlined in a manner that will highlight the important issues, better serve the client, and expedite the reporting process.

   DIRM Comment: DIRM agrees with this suggestion. The revised ISR report format will highlight important issues, better serve the client, and expedite the reporting process.

7. Two separate reporting formats are developed – one format for ISRs of major applications and a second format for ISRs of general support systems.

   DIRM Comment: DIRM agrees with this suggestion. The revised ISR report format will be customized to address those issues particular to major applications and those particular to general support systems.

8. The ISR report format is enhanced to clearly identify the work performed, level of testing, and sampling methodology.

   DIRM Comment: DIRM agrees with this suggestion. The revised ISR report format will clearly identify work performed, level of testing, and sampling methodology.

9. The ISR report format is revised to clearly present the security and integrity requirements, conclusions, corrective actions, and related information applicable to the major application or

general support system under review.

DIRM Comment: DIRM agrees with this suggestion. The revised ISR report format will clearly present the security and integrity requirements, conclusions, corrective actions, and related information applicable to the major application or general support system under review.

10. Client feedback is obtained and considered during all phases of the ISR.

    DIRM Comment: DIRM agrees with this suggestion. DIRM is using the OIG audit model as a best practice in revising the ISR process. The client will be involved and encouraged to give feedback throughout the ISR from the entrance conference, status meetings or notes to review and input of the draft report. The ISR Team will have members from the client organization actively involved in planning and conducting the ISR.

11. Consideration is given to using a divisional or interdivisional team to perform certain phases or all phases of the ISR.

    DIRM Comment: DIRM agrees with this suggestion. The ISR Team will consist of members from DIRM ITES, DIRM ISS, DIRM ASM, DIRM TIM, the client division and data stewards as appropriate to the review.

12. All ISR reports contain the views of responsible officials concerning conclusions, recommendations, and planned corrective actions.

    DIRM Comment: DIRM agrees with this suggestion. DIRM is using the OIG audit model as a best practice in revising the ISR process. The views of responsible officials concerning conclusions, recommendations and planned corrective actions will be obtained in a draft report and contained in the final ISR report.

13. A process or method is developed for resolving disagreements between the point of contact and the ISR team.

    DIRM Comment: DIRM agrees with this suggestion. DIRM is using the OIG audit model as a best practice in revising ISR process. OICM will play the same role as dispute mediator in the ISR process as it does in the audit process.

cc: Janet W. Roberson, Deputy Director, Information Technology Management
Rack D. Campbell, Chief, IT Evaluation Section