Office of Inspector General

March 22, 2002
Audit Report No. 02-008

The FDIC's Efforts To Implement a Single Sign-on 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: March 22, 2002

MEMORANDUM TO: Carol M. Heindel, Acting 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: Final Report Entitled *The FDIC's Efforts To Implement a Single Sign-on Process* (Audit Report No. 02-008)

The Federal Deposit Insurance Corporation's (FDIC) Office of Inspector General (OIG) has completed an audit of the FDIC's limited efforts to implement a single sign-on (SSO) process for accessing the Corporation's information technology (IT) resources. The SSO process refers to an access method that allows users to access multiple systems using only one password. We initiated this audit to evaluate the internal controls over the FDIC's planning and implementation of the SSO process. The FDIC's Division of Information Resources Management (DIRM)[1] originally requested $4.1 million to implement a corporate-wide access control process. Year 2000 funding for the project was approved for $1.6 million.

In April 2000, DIRM initiated the development of SSO for its Extranet-accessible applications[2] as a pilot project for examining the feasibility of providing SSO capabilities. Our audit focused on
(1) the FDIC's planning and implementation of SSO for its Extranet-accessible applications and
(2) the Corporation's ability to make an informed decision regarding corporate-wide implementation of SSO based on the pilot project. A detailed discussion of the scope and methodology of our audit is included in Appendix I.

[1] DIRM has the responsibility of developing, maintaining, and providing security for the FDIC's information technology resources

[2] The Extranet-accessible applications involved are internal Division of Supervision mainframe applications that are available to the examiners for the state and other federal financial regulatory agencies based on permissions granted by the FDIC. The applications are the *Non-Deposit Investment Products System,* the *Statistical CAMELS Off-site Rating,* the E*xaminer Download System,* the *Custom Download*, the *Performance Reports Online,* and the *Community Contacts*.

BACKGROUND

Before beginning the development of a corporate-wide access control process, the Corporation had difficulty in documenting and controlling system access because of the many users, both internal and external, with access to multiple systems. The FDIC required that some external users obtain as many as three passwords to access a system. The General Accounting Office (GAO) had identified the need for better controls over user access during the audit of the FDIC's 1999 financial statements. To streamline the user access process and partially address GAO's user access concerns, the FDIC began planning to implement an SSO process.

DIRM originally requested $4.1 million to develop and implement a corporate-wide access control process. DIRM's original purpose in developing such a control process was to eliminate the redundant sign-on procedures for a user to access multiple applications and to streamline password management. Year 2000 funding of $1.6 million was approved to initiate the corporate-wide access control project.

In April 2000, DIRM initiated an SSO pilot project for Extranet users to determine the feasibility of and methods for effectively implementing SSO for the entire Corporation. Before the implementation of SSO, Extranet users were required at a minimum to have a user ID, valid certificate,[3] and two passwords to access specified FDIC applications. With SSO in place, Extranet users could now access these resources with a user ID, valid certificate, and a single password. DIRM expected that the implementation of SSO for all of its applications would reduce the number of user ID and password combinations managed corporate-wide.

DIRM used the services of a contractor to develop and implement SSO for the Extranet-accessible applications. The SSO pilot was placed in production in March 2001. SSO project costs through the issuance date of this report were approximately $1.4 million.

The September 1999 SSO project plan was developed by DIRM's Information Security Section for a corporate-wide implementation of SSO and included two basic functional requirements: (1) an efficient, reliable, and centrally-managed user access process for all of the FDIC's computing environments and (2) a secure and reliable Extranet and internal system access process using a single log-on transaction. The plan described the benefits of SSO as (1) enhanced usability and reliability of the FDIC Extranet, (2) improved corporate capability to control user access privilege assignments, (3) standardized access controls across all the FDIC's environments, and (4) reduced costs of operating multiple access control systems. The project plan also included a description of the access control environment in place at the time and a comparative analysis of the capabilities of three SSO vendor products. The SSO project team did not tailor the original SSO project plan to take into account that a pilot project was being conducted to determine whether a corporate-wide SSO solution should be pursued. The SSO project team instead prepared a project schedule using Microsoft Project[4] to manage the tasks to be performed during the implementation of the pilot SSO process. The project schedule described the tasks to be performed and the staff responsible for those tasks. DIRM

[3] A certificate is an electronic document used to identify an individual, company, or entity.

[4] Microsoft Project is an application that provides a project manager with the ability to schedule, organize, and analyze tasks, deadlines, and resources.

representatives also prepared a separate document that identified the budget for the pilot SSO project.

RESULTS OF AUDIT

Project planning for the SSO pilot was not adequate. Specifically, DIRM did not integrate into one document pertinent factors associated with the project, develop the methodology or measures needed to effectively assess the project team's implementation of the project, evaluate the outcome of the project, or identify lessons learned. DIRM also did not establish a process to obtain corporate-wide agreement from all FDIC divisions and offices that the SSO process would be the standard access method for use of the FDIC's computing environment.

The SSO project team did not prepare an analysis of alternatives based on the benefit-cost of available system access methods or perform a post-implementation assessment to determine whether the selected SSO solution was the most appropriate method for addressing the FDIC's IT access security needs. Without an analysis of alternatives, the SSO project team was unable to justify that the system access process that the team implemented was the most cost effective.

SSO PROJECT PLANNING

DIRM implemented the SSO pilot project before developing the pertinent information related to the project and documenting that information. Specifically, DIRM did not integrate into one document the key factors associated with the project, including IT resource requirements, the amount of funds budgeted, and the relationships to other IT systems and initiatives. Additionally, DIRM did not develop the methodology or measures needed to effectively assess the project team's implementation of the pilot project, evaluate the outcome of the project, or identify lessons learned. Finally, DIRM did not establish a process, before committing funds to the development of the SSO pilot, to obtain agreement that SSO would serve as the standard system access method. The lack of project documentation occurred because the SSO project team did not follow all the planning requirements for information technology projects outlined in Office of Management and Budget (OMB) circulars and FDIC directives. Rather, the SSO project team believed that the use of Microsoft Project was sufficient for project planning purposes. As a result, the SSO team was unable to justify the SSO method implemented, determine whether the actual results of the SSO pilot project met the expected results, and determine whether the SSO process should be expanded corporate-wide.

SSO Project Documentation

OMB Circular A-130, *Management of Federal Information Resources*, (OMB Circular A-130) promotes an integrated approach to IT planning. The circular states that agencies should integrate planning for information systems with plans for resource allocation, including budgeting, acquisition, and use of information technology. In addition, agencies must establish and maintain an investment control process that links mission needs, information, and information technology in an effective and efficient manner. Agencies must use a performance

based management system that provides timely information regarding the progress of an information technology investment. The system must also measure progress towards milestones in an independently verifiable basis, in terms of cost, capability of the investment to meet specified requirements, timeliness, and quality.

The SSO project team did not integrate into one document the pertinent factors associated with the pilot project, such as IT requirements, amount of funds budgeted, and relationships to other IT systems and initiatives. Specifically, the SSO project team did not develop or maintain the information needed to (1) describe the total resources required to develop, implement, and maintain the SSO process over the entire life cycle of SSO application, (2) ensure the benefit-cost of the project selected exceeded the benefit-cost of maintaining the status quo or other available SSO alternatives, (3) establish and measure the achievement of performance goals for implementing SSO consistent with OMB Circular A-130 and FDIC directives, (4) ensure that the SSO access process would become the corporate standard method for system access, and (5) determine whether expanded implementation of the current pilot SSO process was justified. The lack of documentation occurred because the SSO project team did not develop the planning documents required by corporate policy and OMB Circular A-130 before initiating the SSO implementation.

Without a complete, comprehensive and documented set of information supporting the project, the SSO project team could not properly select from among alternatives or control and evaluate the system access approach that was pursued. The required documentation was not developed or maintained because the SSO project team believed that the use of Microsoft Project was a sufficient means of monitoring the development and implementation of the SSO pilot process. Although Microsoft Project can assist the project manager in monitoring a project's schedule, a more comprehensive means of measuring costs and schedules for IT investment projects is a performance based management system required by OMB Circular A-130. Without the required documentation, DIRM had a limited basis for measuring the effectiveness of the pilot implementation or for determining whether and how to expand the SSO process corporate-wide. During our audit, the SSO project team agreed that the Extranet SSO plan could have been better documented. At DIRM's request, we provided the SSO team with a list of documents that would improve the future planning for SSO.

Performance Measurement

OMB Circular A-130 requires that agencies establish a capital planning and investment control process that links mission needs, information needs, and IT in an effective and efficient manner. The use of performance goals and indicators is a control method that measures an agency's progress in achieving its mission and goals. To accomplish the control objective, the FDIC must develop performance plans that (1) establish the performance indicators to be used in measuring or assessing the relevant outputs, service levels, and outcomes of each program and (2) provide a basis for capturing actual program results through the establishment of performance goals.

DIRM did not develop the performance goals and indicators needed to gauge DIRM's progress in managing and monitoring the pilot SSO project. The performance measures were not developed because the SSO project team again believed that the use of Microsoft Project was a

sufficient means of monitoring the performance of the SSO process. As stated above in our discussion of project documentation, although Microsoft Project does provide a means for the project manager to monitor a project's schedule, it does not provide the performance data required by OMB Circular A-130. More specific performance measures are needed to ensure that DIRM develops its IT resources effectively and efficiently. Without instituting the performance measures and management processes needed to monitor actual performance as compared to expected results, DIRM was not able to evaluate and control the SSO development process. The SSO project team did not have the information needed to measure the project's progress in terms of cost or the capability of the investment to meet specified requirements, timeliness, and quality. Most important, the SSO project team did not implement the performance measures needed to assess whether the results of the pilot project justified a corporate-wide implementation. As a result, DIRM could not determine whether the SSO pilot project, as implemented, met the requirement for an efficient, reliable, secure, and centrally managed SSO access process for all of the FDIC's internal and external computing environments as originally envisioned.

In addition, DIRM had no means to determine whether the original functional requirements would be satisfied and the FDIC would benefit from the SSO process through (1) enhanced usability and reliability of the Extranet, (2) improved corporate control of user access privilege assignments, (3) standardized access controls across all FDIC computer environments, and (4) reduced costs derived from operating fewer multiple access control systems. Finally, the FDIC could not demonstrate that the implementation of the SSO process would address the GAO's concerns related to the FDIC's management of system access, even though doing so was one of DIRM's justifications for implementing the SSO process.[5]

Corporate-Wide SSO Use by Divisions and Offices

The SSO project team did not establish a process to obtain agreement that the proposed SSO process would serve as the Corporation's standard system access method. The agreement was needed to ensure that all corporate applications and systems use the same sign-on process. Without obtaining the agreement of all directors of divisions and offices to use the same process for accessing systems, a corporate-wide SSO may not be attainable, and the implementation of the SSO process may not prove cost-beneficial if additional access methods continue to be used.

FDIC Circular 1240.1, *Corporate Perspective in Information Technology Systems Development* established policies, roles, responsibilities, and procedures to ensure a corporate perspective in creating information systems. The circular applies to the development of major information technology projects that are estimated to cost more than $400,000 in 1 year or $2 million within 5 years. The circular requires the development of a high-level impact analysis that identifies other parts of the Corporation affected by the implementation of the system. When the project is

[5] GAO's management letter entitled, *Financial Audit: Weaknesses in FDIC's Information System Controls*, July 17, 2000 and based on financial statement work performed in 1999 stated that the FDIC's access control process did not adequately protect resources. Part of the FDIC's response to GAO's finding was to implement SSO to improve the Corporation's access controls.

funded, a more detailed impact analysis is required for the project definition report (PDR).[6] The Directors of all affected divisions and offices must signify approval before any major project continues. Provisions of this circular were not in effect when the SSO pilot project was initiated. However, the circular will apply if the implementation of the SSO process is expanded corporate-wide.

Recommendation

We recommend that the Acting Director, DIRM,

(1) require that before initiating the corporate-wide SSO process, the SSO project team prepare a comprehensive project plan that contains the following:

- all documentation required by OMB Circular A-130 for the selection, control, and evaluation components of the capital planning and investment control process,
- performance goals and indicators to gauge the FDIC's progress in implementing the SSO project plan, and
- a mechanism for obtaining agreement from all directors of FDIC divisions and offices to use the SSO process.

ANALYSIS OF SSO ALTERNATIVES

The SSO pilot project plan did not (1) provide an explanation as to how the SSO project team determined that the SSO solution selected was the most appropriate method for addressing the FDIC's IT security concerns, (2) include a benefit-cost analysis (BCA), or (3) quantify the benefits to be achieved based on the measurement of the future improvements in program outputs. The lack of an analysis of alternatives occurred because the SSO project team did not follow the applicable IT planning circulars and directives issued by OMB and the FDIC. As a result, the SSO project team could not provide adequate justification for the system access method that was implemented.

OMB Circular A-130 requires that agencies demonstrate a projected return on investment that is clearly equal to or better than alternative uses of available public resources. Return on investment should, where appropriate, reflect actual returns observed through pilot projects and prototypes. The selection component of the circular also requires that BCAs be prepared and updated for each information system throughout its life cycle. The BCA should provide a level of detail proportionate to the size of the investment, rely on systemic measures of mission performance, and be consistent with the methodology described in OMB Circular A-94, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs.*

[6] A PDR is a deliverable of the FDIC's system development life cycle and addresses business needs; high-level functional, data, security, and performance requirements; project scope; technical feasibility; evaluation of alternatives; and the recommended alternative.

FDIC Circular 4310.1, *Utilizing Cost Benefit Analysis Methodology for the Purchase or Development of Capital A*ssets, dated July 17, 1998 was issued to promote efficient resource allocation through well-informed decision-making and to provide guidance for conducting a BCA. The circular also defines a capital asset to include land, structures, equipment, and intellectual property (including software) that have an estimated useful life of 1 year or more and costing more than $3 million. A DIRM policy memorandum entitled *Instructions for Performing Cost Benefit Analyses*, dated April 25, 2001 was also issued to ensure that more realistic BCAs are performed for future IT projects.

The SSO project team did not develop a BCA and perform an analysis of alternatives before initiating the SSO pilot project as required by OMB Circular A-130 and FDIC Circular 4310.1. Specifically, the SSO project team did not consider other alternatives for accomplishing the FDIC's system access needs before opting to pursue SSO. Some of the system access methods that were not considered before initiating the SSO project included: maintaining the present system access method with improved internal controls; password synchronization,[7] also know as same sign-on; and SSO with the FDIC's in-house public key infrastructure (PKI)[8] software.

Although the SSO project plan stated that implementing SSO would reduce the costs of operating multiple access control processes, the plan did not quantify the benefits to be achieved through the implementation of the SSO process. Because it did not perform a BCA and analysis of alternatives, the FDIC cannot determine if it is making the best use of its investment funding or determine with any certainty whether SSO is the best alternative for meeting the Corporation's system access needs.

Recommendation

We recommend before proceeding to a corporate-wide SSO process, the Acting Director, DIRM,

(2) require the SSO project team to develop a BCA for all available alternatives that meet the FDIC's system access needs and select the alternative that provides the best use of the Corporation's funds.

SSO POST-IMPLEMENTATION ASSESSMENT

The SSO project team did not develop the benchmarks and goals needed to measure the benefits achieved through the implementation of the SSO process for the Extranet users of the five DOS systems. As a result, the project team was unable to perform a post-implementation assessment to determine whether DIRM should expand the use of the SSO process corporate-wide.

---

[7] Password synchronization ensures that a user accesses all systems with the same ID and password.

[8] A public key infrastructure is a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances that are important in protecting sensitive communications and transactions.

OMB Circular A-130 requires post-implementation reviews of information systems as part of the evaluation component of the capital planning process. The purpose of these reviews is to validate estimated benefits and costs and to document effective management practices for broader use.

The project team's lack of performance measures occurred because the SSO project team did not develop or maintain an SSO performance plan to measure benefits achieved with the SSO process. Because the Corporation has not yet decided upon the future course of the SSO effort, the SSO project team would be well served to collect system access data, statistics, and costs related to both the pre- and post- pilot SSO implementation. With such information, the SSO project team could prepare a lessons learned analysis and perform a post-implementation review of the SSO process for the Extranet accessible applications. These two analyses would be of particular use in determining whether SSO should be implemented corporate-wide.

Recommendation

We recommend that the Acting Director, DIRM,

(3) require that the SSO project team perform a lessons learned analysis based on a post-implementation assessment of the SSO pilot project to determine whether a corporate-wide implementation of the SSO process is justified.

CORPORATION COMMENTS AND OIG EVALUATION

On March 14, 2002, the Acting Director of DIRM provided a written response to the draft report. Management's response, without the attachment suggesting editorial changes, is presented in Appendix II to this report. We made several of DIRM's suggested editorial changes to clarify our discussion. DIRM stated that plans to implement a corporate-wide SSO process have been deferred. The Corporation has partially concurred with recommendations 1 through 3. However, management's comments indicate that the proper corrective action will be taken should DIRM initiate SSO again. Accordingly, we consider management's comments to be responsive to recommendations 1 through 3. Because there are no current plans to extend the SSO process corporate-wide, we consider these recommendations to be resolved, dispositioned, and closed.

APPENDIX I

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to evaluate the internal controls over the planning and implementation of the FDIC's pilot project to provide SSO for Extranet users. To accomplish the audit objective, we interviewed DIRM and Division of Supervision (DOS) employees and evaluated the SSO implementation plan to determine if the plan complied with:

- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources* ;[9]

- FDIC Circular 1240.1, *Corporate Perspective in Information Technology Systems Development*, dated April 4, 2001;

- FDIC Circular 4310.1, *Utilizing Cost Benefit Analysis Methodology for the Purchase or Development of Capital Assets*, dated July 17, 1998; and

- DIRM's policy memorandum, *Instructions for Performing Cost Benefit Analyses*, dated April 25, 2001.

We also researched the Internet and audit work performed by other organizations to identify alternative technology that could potentially address the FDIC's SSO needs. We reviewed all available SSO planning documents and interviewed DIRM and DOS personnel to determine (1) the feasibility of the SSO process, (2) the testing methodology, and (3) whether the stated goals of the SSO process had been achieved.

We also determined the security impact of use of the SSO process by external users. We observed the operation of the SSO process and reviewed the SSO scripts to ensure that access was provided only to required resources. We performed the audit between January and October 2001 in accordance with generally accepted government auditing standards.

[9] We used OMB Circular A-130 as our primary criteria either because the FDIC is required to follow certain provisions or because in our judgment it would be prudent for the FDIC to voluntarily adopt the nonobligatory provisions.

FDIC

Federal Deposit Insurance Corporation

CORPORATION COMMENTS

March 14, 2002

MEMORANDUM TO: Russell A. Rau
Assistant Inspector General for Audits
Office of Inspector General

FROM: Carol M. Heindel, Acting Director [Electronically produced version; original signed by Carol Heindel]
Division of Information Resources Management

SUBJECT: Revised Response To OIG Draft Audit Report Number 2001-904
FDIC's Efforts to Implement a Single Sign-on Process

The Division of Information Resources Management (DIRM) has reviewed the subject draft audit report and we have attached a full copy with several wording changes we are requesting. In addition, we are offering general comments as well as specific management decisions regarding the individual recommendations made in the draft audit report.

General

DIRM's perspective regarding the Single Sign-On (SSO) initiative was one of investigating a new security software tool for potential introduction to the Corporation, not as a systems application developed under the requirements of the FDIC System Development Life Cycle (SDLC). While we agree that better documentation could have been maintained for all aspects of the project, DIRM did:

- issue a policy memorandum on April 25, 2001, entitled, *Instructions for Performing Cost Benefit Analyses*, to improve and ensure that more realistic cost benefit analyses (CBAs) are performed for future IT projects.

- develop separate project documentation including project plans using the Corporate standard project planning tool,

- conduct a review of multiple alternative vendor products based on both product functionality and the current FDIC infrastructure,

- develop lessons learned documents, as well as,

- submitted and processed all required project documentation for the IT budget formulation, review and approval process in place at the time of the pilot effort. This included presentation and ranking of the initiative by the FDIC IT Technical Committee.

The pilot for FDIC's Extranet did prove beneficial to the FDIC Extranet users from the state banks, eliminating duplicative id's and passwords. The overall decision not to proceed to any further implementation of SSO for the Corporation included several factors. First, the cost to apply SSO across all platforms in the FDIC was prohibitive. Second, at the time of the pilot, success in implementing SSO in both the public and private sector was virtually non-existent due to the cost and complexity of implementation. Finally, at the time of the pilot, FDIC was beginning its effort to plan for the conversion of its network and desktop operating environments to the Windows 2000 and subsequently Microsoft XP environments. The timing and impact of this conversion on any SSO implementation would be significant.

The draft audit report makes reference to DIRM's anticipated use of SSO to address GAO access control issues. The report states that, "… the FDIC could not demonstrate that the implementation of the SSO process would address the GAO's concerns related to the FDIC's management of system access, even though doing so was one of DIRM's justifications for implementing the SSO process." It should be noted that the SSO effort was only one of several efforts underway by DIRM to address GAO's concerns. These included other successful activities such as the implementation of the Information Security Manager program and the associated access control procedures for that program. SSO was not to be a "silver bullet" for all GAO access control issues. The fact that the pilot results ended in the termination of any expansion effort beyond the FDIC Extranet, in no way minimizes DIRM's efforts to address GAO's access control concerns.

Management Decision Regarding Specific Recommendations

We recommend that the Acting Director, DIRM,

(1) require that before initiating the corporate-wide SSO process, the SSO project team prepare a comprehensive project plan that contains the following:

- all documentation required by OMB Circular A-130 for the selection, control, and evaluation components of the capital planning and investment control process,
- performance goals and indicators to gauge the FDIC's progress in implementing the SSO project plan, and
- a mechanism for obtaining agreement from all directors of FDIC divisions and offices to use the SSO process.

Response: We partially concur with the recommendation. As previously mentioned in our general comments, prior to any recommendations or results from this audit, DIRM had already recognized the need for more stringent cost benefit policy and procedures during the time of the pilot SSO implementation. To that end, the CIO issued Policy Memorandum 02-2001 Instructions for Performing Cost Benefit Analyses on April 25, 2001 to improve these policies and procedures. Should DIRM decide to evaluate SSO again, these audit findings will be taken into consideration and applied to the SSO project according to the applicable corporate investment planning, control and measurement process that FDIC has in place at that time. This

will include applicable policy and procedures associated with the communication and agreement amongst FDIC divisions and offices.

(2) Require the SSO project team to develop a BCA (Benefit Cost Analysis) for all available alternatives that meet the FDIC's system access needs and select the alternative that provides the best use of the Corporation's funds.

Response: We partially concur with the recommendation. Since the April 25, 2001 issuance of Policy Memorandum 02-2001, DIRM has procedures in place to address CBA's for all major IT development/initiative projects in a thorough and comprehensive manner. This would include a project like SSO which occurred under older, generally less stringent DIRM policies. At this time, there are no current plans to re-evaluate SSO or to proceed with further SSO expansion. If DIRM initiates a SSO effort again, the SSO project team will do a CBA against the available alternatives in selecting a product or tool and will follow all applicable Corporate cost-benefit guidance.

(3) Require that the SSO project team perform a lessons learned analysis based on a post-implementation assessment of the SSO pilot project to determine whether a corporate-wide implementation of the SSO process is justified.

Response: We partially concur with this recommendation. Based on the pilot, the determination has already been made not to proceed with further SSO expansion as stated in our general comments. As such, no additional resources will be expended on the completed pilot for any further assessment. DIRM did prepare a lessons learned document following the pilot on May 17, 2001. This document is attached. If DIRM initiates a SSO effort again, the SSO project team will perform a lessons learned analysis based on their documented post-implementation assessment of the project.

If you have any questions concerning this response, please contact Rack Campbell, Chief ITES on 516-1422.

Attachments

cc: Vijay G. Deshpande, Director, OICM
Janet W. Roberson, Deputy Director, DIRM
Rack Campbell, Chief, DIRM
Ned Goldberg, Assistant Director, DIRM