FOLLOW-ON AUDIT OF FDIC'S GENERAL EXAMINATION SYSTEM (GENESYS) DEVELOPMENT PROJECT

Audit Report No. 99-020
March 31, 1999

OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

TABLE OF CONTENTS

FDIC

Federal Deposit Insurance Corporation Office of Audits
Washington, D.C. 20434 Office of Inspector General

DATE: March 31, 1999

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

James Sexton, Director
Division of Supervision

FROM: David H. Loewenstein
Assistant Inspector General

SUBJECT: Report Entitled *Follow-on Audit of FDIC's General Examination System Development Project*
(Audit Report No. 99-020)

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) has completed a follow-on audit of the FDIC's General Examination System (GENESYS) development project. This follow-on audit focused on evaluating whether developers were adhering to the FDIC's system development policies and procedures. Prior to this audit, the OIG issued an audit report entitled *Audit of the General Examination System (GENESYS) Development Project* dated June 5, 1997 that contained five findings and recommendations designed to improve the FDIC's system development practices relative to GENESYS.

Division of Information Resources Management (DIRM) and Division of Supervision (DOS) management had taken some steps to improve the development practices for GENESYS following our initial audit. However, DIRM repeated its practice of performing detailed design and development work before user requirements had been completely defined or a project work plan had been formally approved. In addition, senior DIRM and DOS management approvals of the GENESYS project work plan, functional requirements document (FRD), and system design document came after significant investments had been made in development work. We also noted that despite significant changes in the project's scope, cost, and schedule that should have required a formal re-evaluation of alternatives, the FDIC continued with their initial plan without evaluating alternatives.

BACKGROUND

GENESYS represents the FDIC's most comprehensive initiative to apply technology to the bank safety and soundness examination process. GENESYS will replace the FDIC's Automated

Report of Examination (C-ARE) and WordPerfect® templates used by DOS examiners to generate the Report of Examination (ROE). GENESYS is intended to improve the quality of the ROE and the efficiency of the report preparation process by leveraging time saving and data integration features of Windows® 95 and Microsoft® Office 97 software. In addition, GENESYS permits the electronic capture and analysis of key bank safety and soundness examination information, such as Call Report and Uniform Bank Performance Report data.

Data analysis and query tools contained within GENESYS are intended to assist examiners in more effectively analyzing liquidity risk, interest rate risk, and other risks against which bank operations can be assessed. In addition, by expanding the amount of timely and relevant data available to examiners prior to on-site examinations, examiners will be better able to identify the specific risk areas that should be addressed during an examination. GENESYS will also allow examiners to perform additional work off site and should facilitate the work that must be performed on site, thereby reducing the burden of examinations to the industry.

DIRM developed GENESYS using Microsoft Visual Basic® version 5.0 software and various add-on tools, including Formula One™ and First Impression®. Microsoft Access ‘97® was used to develop the GENESYS database, and Structured Query Language (SQL) program code was used to provide functionality to the GENESYS screens. GENESYS operates on a Pentium-based laptop computer.

The FDIC initiated the GENESYS project in December 1995. In January 1997, the Board of Governors of the Federal Reserve System (FRS) and the Conference of State Bank Supervisors (CSBS) joined the project as part of an interagency effort to develop a single bank safety and soundness examination system. Throughout the project, the FDIC's DIRM assumed the lead role in developing, testing, and implementing the system. DOS planned to use GENESYS on all new safety and soundness examinations when fully implemented. Approximately 30 state banking departments planned to begin using GENESYS with the FDIC in 1998, and the majority of the remaining state banking departments, along with FRS, planned to implement GENESYS in March 1999.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of the audit were to determine whether: (1) development was adhering to established and generally accepted System Development Life Cycle (SDLC) procedures, (2) requirements had been adequately defined and satisfied user needs, and (3) cost and benefit information had been adequately documented and tracked. Because of the time-sensitive nature of the GENESYS development project, we met with DIRM and DOS personnel throughout the audit to discuss our preliminary recommendations.

To accomplish our audit objectives, we interviewed headquarters DIRM and DOS personnel as well as regional and field office bank examiners who were involved with the project. We also interviewed representatives of the U.S. General Accounting Office (GAO), FRS, CSBS, and the Alabama State Banking Department. In addition, we reviewed key SDLC deliverable products, including the GENESYS project work plan, FRD, and system design document. We also reviewed DIRM client information technology (IT) plans, contractor status reports, examiner training evaluation reports, and other key reports and documents prepared during the GENESYS development process. We also evaluated DIRM and DOS plans and activities relating to System Qualification Testing (SQT) and User Acceptance Testing (UAT) of GENESYS. Finally, we reviewed the FDIC's SDLC policies and procedures.

Our audit work was limited to the FDIC's development of version 1.0 of GENESYS. We did not review development plans or work relating to ongoing or planned GENESYS enhancements. We conducted our audit between September 1997 and October 1998 in accordance with generally accepted government auditing standards.

RESULTS OF AUDIT

Although DIRM and DOS management had taken some steps to improve the development practices for GENESYS following our initial audit, GENESYS development practices continued to deviate from the structured approach prescribed by the FDIC’s SDLC process. Specifically, DIRM employed an evolutionary prototyping process to develop GENESYS wherein development work was performed before requirements definition and design work were substantially complete. DIRM also initiated a SQT of GENESYS before system development and integration testing had been completed. In addition, DIRM deviated from the FDIC's SDLC process by not evaluating the feasibility or cost-benefit of alternative solutions to the development of GENESYS or finalizing critical SDLC deliverables and obtaining senior management approvals prior to initiating subsequent SDLC phases.

DIRM decided to deviate from the FDIC's prescribed SDLC procedures in an attempt to meet an aggressive development schedule for GENESYS. However, these deviations caused several inefficiencies in the GENESYS development process and required the FDIC to assume unnecessary risk. For example, ongoing changes to the functionality of GENESYS during the SQT process required testers to continually revalidate and update test procedures and ultimately prevented the testers from completing a SQT for GENESYS. DIRM also experienced inefficiencies and delays in the testing process by providing SQT testers with outdated GENESYS design specifications. This resulted in the development of erroneous test procedures that had to be revised or eliminated during the SQT process. Inadequate system qualification testing also allowed security weaknesses and numerous software bugs in GENESYS to go undetected until after DIRM and DOS began training the FDIC and state examiners on use of the software.

Examiners that we spoke with during our audit field work stated that GENESYS would generally satisfy their requirements for generating a safety and soundness ROE. However, feedback from examiners following GENESYS training indicated that the software contained numerous programming bugs and was not ready for training or production implementation when FDIC initiated its national training on the system. In our opinion, DIRM and DOS could have limited its risk by postponing GENESYS training and implementation until the software had been thoroughly tested and the programming bugs corrected.

In addition, we observed that there was no formal agreement between the FDIC and FRS regarding resources to satisfy unique FRS requirements. The FDIC assumed unnecessary risk by performing detailed design and development work without any formal FRS approvals of the GENESYS project work plan, FRD, or system design document. A less-than-expected level of FRS examiner support during the GENESYS design phase and FRS' decision to temporarily withdraw from the project on two separate occasions in May 1997 and November 1997 caused inefficiencies during the development process and contributed to delays to the project schedule. We believe that the FDIC can improve its interagency coordination on the many planned enhancements to GENESYS by formalizing up-front interagency development agreements and adhering more closely to generally accepted SDLC procedures.

Significant turnover of DOS examiners assigned to the project impeded both requirements definition and design and resulted in unnecessary delays to the GENESYS development schedule. In addition, we found that GENESYS security features that were designed to prevent the unauthorized disclosure of confidential bank examination information needed to be improved. Finally, we found that there was a need to track and report more complete and up-to-date cost-benefit information on GENESYS throughout its life cycle.

Prior OIG audit reports have identified repeated instances where DIRM has deviated from the structured development approach required by the FDIC's SDLC process. For example, in our review of the FDIC's Time and Attendance Processing System (TAPS) development project, we noted that DIRM and Division of Administration (DOA) management did not formally evaluate the feasibility or cost-benefit of alternative solutions to TAPS. In addition, DIRM and DOA proceeded with design and development work before fully defining user requirements. We also noted that TAPS suffered from a high turnover of project staff.

Reports and guidelines issued in past years by such organizations as GAO and the Office of Management and Budget (OMB) have identified similar causes for unsuccessful IT and systems development efforts. These causes include an inadequate evaluation of system alternatives, lack of senior management involvement, incomplete knowledge of customer needs, and turnover of key project staff. Because the referenced SDLC deviations continue to recur on DIRM's SDLC projects, we are re-addressing several recommendations to DIRM that have been made in past OIG audit reports. In addition, we are making several new recommendations to improve DIRM's development practices on future IT initiatives.

GENESYS DID NOT FOLLOW THE FDIC'S STRUCTURED DEVELOPMENT METHODOLOGY

DIRM and DOS management had taken some steps to improve the development practices for GENESYS following our initial audit. For example, DIRM assigned a quality assurance specialist to GENESYS and DOS improved the documentation of GENESYS requirements. However, GENESYS development practices continued to deviate from the structured approach required by the FDIC’s SDLC process. Specifically, DIRM deviated from the FDIC's SDLC process by (1) not evaluating the feasibility or cost-benefit of alternative solutions to the development of GENESYS,

(2) using an evolutionary prototyping methodology wherein development work was performed before requirements definition and design work were substantially complete, and (3) not finalizing critical SDLC deliverables and obtaining formal senior management approvals prior to making significant investments in subsequent SDLC phases.

DIRM decided to deviate from the FDIC's prescribed SDLC procedures in an attempt to meet an aggressive development schedule for GENESYS. However, these deviations caused several inefficiencies in the GENESYS development process and exposed the project to unnecessary risk. For example, DIRM's decision to deviate from the phased testing procedures prescribed by the FDIC's SDLC process resulted in a testing process that was ineffective, costly, and in some cases, redundant.

DIRM initiated a SQT of GENESYS before the system had been completely developed. Ongoing development of GENESYS during the SQT process prevented testers from finalizing a SQT plan and required ongoing revalidation and updating of SQT procedures to ensure that new or modified functionality that was being built into GENESYS would be properly tested. In addition, outdated GENESYS design specifications provided to the SQT testers prior to the start of SQT resulted in the development of many erroneous test procedures that subsequently had to be revised or eliminated. We noted that the FDIC paid a contractor $491,037 to perform the SQT.

We advised DIRM and DOS officials of the risks associated with performing a SQT before development and integration testing was completed. However, the DIRM and DOS officials indicated that they recognized the risks of performing concurrent testing and proceeded with the SQT. The lack of a fully integrated GENESYS system prevented testers from completing a SQT for GENESYS. Inadequate system qualification testing also allowed security weaknesses and numerous software bugs in GENESYS to go undetected until after DIRM and DOS began training the FDIC and state examiners on use of the software.

Examiners that we spoke with during our audit field work stated that GENESYS would generally satisfy their requirements for generating a safety and soundness report of examination. However, feedback from examiners following GENESYS training indicated that the software contained numerous programming bugs and was not ready for training or production implementation when the FDIC initiated its national training on the system in August 1998. In our opinion, DIRM should have delayed GENESYS training and implementation until the software had been thoroughly tested and the programming bugs corrected. Initial impressions of a new software product are lasting ones and can have a significant impact on acceptance of the software within the user community. Given the complexity of the GENESYS software, DIRM could have further limited the risk of an unsuccessful implementation by ensuring that programming bugs were corrected before examiners were trained on the system.

Feasibility and Cost-Benefit of Alternative Solutions Not Evaluated

Earlier in the GENESYS development process, DIRM and DOS did not formally evaluate the feasibility or cost-benefit of alternative solutions to GENESYS. DIRM and DOS developed an analysis of the projected costs and benefits of developing GENESYS in September 1996. DIRM also maintained and reported annual cost data throughout most of the project's life cycle as changes occurred in the project's scope. However, the September 1996 analysis did not address alternative solutions. Additionally, despite significant changes in the project's scope, cost, and schedule in January 1997 that should have required a formal re-evaluation of alternatives, the FDIC continued with their initial plan to develop an in-house system without formally evaluating alternatives.

Although DIRM officials informed us that they informally considered alternatives to GENESYS, they did not formally evaluate or document the cost-benefit of alternative solutions because they did not consider it necessary to do so. DIRM and DOS also did not provide senior management with information that compared actual project cost, schedule, and scope to original projections.

FRS raised concern about the need to evaluate alternative solutions to GENESYS in April 1997 and cited this as one of its reasons for a less than full commitment to the project at that time. Alternative solutions should be considered up-front during the project planning phase of a system initiative. Also, when major changes occur that affect the project's cost, scope, risks, or timeframes for implementation, alternative solutions should be revisited in order to validate the approach being followed.

The purpose of a feasibility study is to provide senior management with: (1) an analysis of the project's objectives, requirements, and system concepts; (2) an evaluation of alternative approaches; and (3) a recommended approach. The purpose of a cost-benefit analysis (CBA) is to provide management with adequate cost and benefit information to analyze and evaluate alternative approaches. A CBA should help to determine whether commercial off-the-shelf software is available to address project requirements or whether other technical and functional alternatives, such as enhancing or re-engineering existing systems or modifying an existing system developed by another federal entity, are feasible. Because the structures of feasibility studies and CBAs are so similar, the FDIC's SDLC Manual allows them to be combined.

The FDIC's SDLC Manual requires a feasibility study and CBA to be completed for major IT projects before committing full life cycle resources. Federal guidelines also stress the importance of feasibility studies and CBAs. For example, *Evaluating Information Technology Investments*, a practical guide issued jointly by OMB and GAO in November 1995, recommends that management evaluate the cost-benefits and risks of IT projects before making significant investments in those projects. Changes proposed by DIRM to the FDIC's SDLC Manual would require that CBAs be updated and approved when significant changes occur in a project's scope, estimated resources, or timeframes. Updating CBAs throughout a project's life cycle is consistent with sound business practices and guidelines, including *OMB Circular A-130*, which prescribes that CBAs be refreshed throughout the life cycle process with up-to-date information to ensure the continued viability of systems prior to and during implementation.

In a subsequent section of this report, we identify opportunities for DIRM and DOS to improve the tracking and reporting of GENESYS cost and benefit information. Tracking accurate, current, and complete life cycle cost data is critical to measuring performance and making cost-effective decisions on complex IT investments. Full life cycle cost data is also essential for evaluating alternatives when significant changes occur in an IT project's cost, scope, or schedule. In addition, without current and up-to-date cost-benefit information, DIRM is unable to conduct effective post-implementation reviews to validate estimated benefits and document effective management practices for broader use.

Recommendations

We recommend that the Director, Division of Information Resources Management:

(1) Formally evaluate and document the feasibility and cost-benefit of alternative solutions for systems development projects, including major enhancements to GENESYS, using the guidelines in the FDIC's SDLC Manual before committing significant life cycle resources to a particular alternative.

(2) Revisit alternative solutions when significant scope, cost, risk, or schedule changes occur on future information technology projects.

(3) Revise the FDIC's SDLC Manual to require that as significant changes occur in a project's scope, risk, estimated resources, or timeframes, that these changes be approved by the IT Council.

Use of Evolutionary Prototyping

DIRM employed an evolutionary prototyping methodology to develop GENESYS that significantly deviated from the phased development methodology prescribed by the FDIC’s SDLC process. The evolutionary prototyping methodology used for GENESYS was one in which development work was performed before requirements definition and design work were substantially complete. DIRM's development approach also involved initiating a SQT of GENESYS before system development and integration testing had been completed. In addition, although the GENESYS project team had developed several draft versions of critical SDLC deliverable products, these deliverables were not approved by senior management before significant investments had been made in subsequent life cycle phases. The FDIC's SDLC process requires that critical SDLC deliverable products be approved by senior management before making significant investments in subsequent life cycle phases. DIRM decided to deviate from the FDIC's prescribed SDLC process in an attempt to meet an aggressive development schedule for GENESYS. However, these deviations caused several inefficiencies in the GENESYS development process and required the FDIC to assume unnecessary risk.

We spoke with members of the GENESYS development team and learned that the phased development approach prescribed by the FDIC's SDLC process was not being followed because of the amount of time required to complete work in one phase before proceeding with work in a subsequent phase. The GENESYS developers adopted a streamlined development process for GENESYS in an attempt to meet an aggressive development schedule for the project. The

GENESYS project work plan states: "This project is schedule-driven; the highest priority identified is to deliver a product on time. Therefore, risk areas that adversely impact project schedule will be given the highest priority. Other risk areas, such as product content and quality, and project cost, will be considered secondary."

The evolutionary prototyping methodology used to develop GENESYS was one in which programmers periodically met with examiners to present specific screens and demonstrate functionality. Some program code was developed as part of this process to display information on the screen and demonstrate functionality. Based on their meetings with the examiners, the programmers made adjustments and enhancements to the GENESYS screens. Code reviews were also performed to ensure that detailed design and development work adhered to agreed upon standards. This process was repeated until the user was satisfied with the functionality of the screen. Once the user was satisfied, the DIRM and program office project managers formally approved the requirements and design of the screen and any coding work remaining for the screen was completed. The prototype screen was then integrated into a working version of the application and later tested in preparation for production implementation.

The FDIC’s SDLC Manual describes a prototyping technique that can be used by system developers for requirements gathering or for proof-of-concept purposes. According to the FDIC's SDLC methodology, a prototype of the proposed system is developed based on user requirements and refined based on user input. Once the user is satisfied that the prototype has the required features, the prototype requirements are documented in a FRD and design continues in the traditional, phased manner. The prototyping methodology described in the FDIC's SDLC Manual has been advocated as a useful software engineering tool because it lends itself to intense interaction between users and developers, resulting in early validation of requirements. Validation of requirements early in a system's life cycle development is important because failure to validate requirements can result in frequent and expensive changes in later life cycle phases.

While it may be necessary to perform a certain level of design and development work to produce a working model or prototype, the design and development work performed on GENESYS was more extensive for some business functions than required to validate user requirements and elicit feedback on the look and feel of the user interface. For example, programmers were developing and testing program code for GENESYS screen functionality, performing detailed design and development work on the GENESYS database, and developing program code to populate tables in certain GENESYS modules.

GENESYS design and development work was performed before required SDLC deliverable products had been approved. We noted that DIRM and DOS had invested significant corporate resources in the GENESYS project before obtaining senior DIRM and DOS management approval of a FRD or project work plan describing the scope, resources, and time schedules required to develop the system. The FDIC’s SDLC Manual prescribes that a project work plan and FRD be completed and approved before proceeding with detailed design and development work.

We believe that DIRM's use of evolutionary prototyping to develop GENESYS caused certain inefficiencies in the GENESYS development process and required the FDIC to assume unnecessary risk. For example, in the following section of this report, we explain that DIRM lost valuable resources by proceeding with a SQT of GENESYS before system development and integration testing had been completed. The FDIC's SDLC Manual prescribes a phased approach for systems development wherein development is completed before testing begins. In addition, a major risk in developing significant functionality into a prototype is that if business requirements change or do not receive management approval, the investment in the design and development of prototype modules may not benefit the project or the Corporation.

DIRM's use of evolutionary prototyping also made the project sensitive to personnel turnover. DIRM relied on extensive developer/user interaction to build requirements and design into a working software prototype while placing less emphasis on maintaining up-to-date requirements and design documentation than prescribed by the FDIC's SDLC process. As a result, as examiners left the GENESYS project, so did much of the knowledge and rationale underlying why decisions relating to GENESYS requirements and design were made. Although DOS examination staff improved GENESYS user documentation during late 1997 and early 1998, in part, to mitigate the impact of examiner departures, temporary assignments of examination staff to the GENESYS project continued through the close of our audit field work.

In our opinion, the evolutionary prototyping methodology used to develop GENESYS should not be used on the FDIC's large, complex systems initiatives, such as GENESYS. In addition, we believe that prototyping techniques should be strictly limited to the requirements gathering phase of IT projects as prescribed by the FDIC's SDLC Manual. Evolutionary prototyping that extends beyond the requirements definition phase, similar to the methodology used on GENESYS, may be useful on FDIC's small, non-complex systems initiatives that involve short development schedules. If DIRM determines that an evolutionary prototyping methodology similar to the one used on GENESYS is appropriate for select, small scale IT initiatives, then the FDIC's SDLC Manual should be amended to describe the evolutionary prototyping methodology that will be used. The Manual should also include specific criteria for determining when evolutionary prototyping development such as the one used for GENESYS is appropriate. The criteria restricting when this method can be used should address the estimated life cycle cost of the system, time frames for development, project complexity, scope, and risk.

Recommendations

We recommend that the Director, Division of Information Resources Management:

(4) Require the GENESYS development team to follow the phased development process prescribed by the FDIC's SDLC Manual for systems development projects, including any major enhancements to GENESYS.

(5) Determine whether evolutionary prototyping could benefit FDIC's small, non-complex systems initiatives that involve short development schedules. If DIRM determines that evolutionary prototyping is appropriate for select, small scale IT initiatives, then the FDIC's

SDLC Manual should be amended to describe the type of methodology that will be used and specific criteria governing its use.

GENESYS Testing Was Inefficient, Costly, and Not Always Effective

DIRM did not follow an efficient or effective method of testing GENESYS prior to its implementation. As a result, valuable system development resources may have been wasted. For example, developers initiated a SQT of GENESYS before system development and integration testing was completed. Although the FDIC paid a contractor $491,037 to perform a SQT for GENESYS, ongoing changes to the functionality of GENESYS during the SQT process required testers to continually revalidate and update test procedures. As a result, the SQT was not completed.

DIRM experienced additional inefficiencies in the SQT process by providing testers with outdated GENESYS design specifications. This resulted in the development of erroneous test procedures that had to be revised or eliminated during the SQT process. A lack of effective communication and coordination between the SQT testers and members of the GENESYS development and examination teams during the SQT process exacerbated the SQT shortcomings. Inadequate system qualification testing allowed security weaknesses and numerous software bugs in GENESYS to go undetected until after DIRM and DOS began training the FDIC and state examiners on the software.

DIRM assumed additional risk during the testing process by performing a SQT, user acceptance test (UAT), and pilot test of GENESYS concurrently. DIRM deviated from the phased testing approach prescribed by the FDIC's SDLC process in an attempt to meet an aggressive development schedule for GENESYS. We advised DIRM and DOS officials of the risks associated with parallel testing in writing via an e-mail that was sent on May 1, 1998. We also met with DIRM and DOS officials on May 8, 1998 to discuss our concerns regarding parallel testing in greater detail. However, DIRM and DOS officials indicated that they recognized the risks of performing parallel testing and proceeded with the SQT, UAT, and pilot tests of GENESYS as planned.

In September 1997, FDIC awarded a contract to provide Independent Verification and Validation (IV&V) technical support to the GENESYS project. The contract was valued at $622,149 and ran through December 31, 1998. The contract required the IV&V contractor to analyze the GENESYS functional requirements and design, prepare a SQT plan and related test procedures, conduct a SQT, and report the results to DIRM. The GENESYS SQT was intended to consist of three 2-week test cycles. The first SQT cycle was intended to validate whether the GENESYS functional requirements were met, ensure that all system capabilities functioned as designed, and ensure that the GENESYS user guide was adequate. The second SQT cycle was intended to focus on exception testing to determine how GENESYS would handle abnormal conditions and error processing. The third SQT cycle was intended to repeat the first two SQT cycles using a different set of input data to ensure that there were no data dependencies within the system.

The IV&V contractor developed its initial test procedures based on a review of the approved GENESYS FRD and system design document. However, many of the requirements and design specifications contained within these documents had not been updated to reflect changes that had been made to the software's functionality pursuant to the evolutionary prototyping process that DIRM was using to develop GENESYS. As a result, many of the test procedures that the contractor developed were erroneous or inaccurate and had to be revised and revalidated. A lack of effective communication and coordination between the SQT testers and members of the GENESYS development and examination teams during the SQT process prevented the testers from identifying erroneous test procedures. Resources devoted to identifying and revising erroneous test procedures introduced significant inefficiencies to the GENESYS testing process.

The contractor initiated the first SQT cycle of GENESYS on January 20, 1998. However, the lack of a fully integrated GENESYS system and the development of erroneous test procedures referenced above impeded the testing process. We noted that the IV&V contractor was only able to successfully execute approximately 14 percent (66 of 471) of the test procedures that had been prepared for the first SQT cycle of GENESYS. We also noted that the contractor developed 344 findings as a result of the first 2-week SQT cycle for GENESYS. The contractor testers cited the lack of a GENESYS user guide, the lack of documentation that explained proper operation of the system, and an incomplete GENESYS data dictionary as further impediments to the SQT process.

Ongoing changes to the functionality of GENESYS during the SQT process introduced additional inefficiencies by requiring testers to continually revalidate and update test procedures. In an effort to address this impediment, contractor testers were directed by DIRM on February 3, 1998 to modify their test procedures based on input from the DOS examiners. Contractor testers were also directed to contact the examiners whenever differences were noted between the GENESYS software and documented requirements and design. During their discussions with examiners, the contractor testers identified new GENESYS requirements and functionality that had been neither documented nor coded into the GENESYS software. The examiners indicated that many of these new requirements were needed for an initial release of GENESYS. These new requirements were provided to the GENESYS developers for programming and incorporation into the application.

Although the GENESYS SQT process was scheduled to be completed within 6 weeks of its initiation, SQT testing activities continued for 17 weeks and were not completed. In May 1998, DIRM discontinued the GENESYS SQT and directed the IV&V contractor to prepare a test analysis report. The SQT test analysis report, dated June 8, 1998 states: "At the time of this report a fully integrated system has not been made available. The testing conducted by the IV&V team might more appropriately be referred to as a combination of unit and integration testing." The test analysis report recommended that the DIRM project manager for GENESYS complete unit and integration testing of the software and then subject the system to a formal SQT. However, at the close of our field work, a formal SQT, as defined by the FDIC's SDLC Manual, had not been performed for GENESYS.

The purpose of a SQT is to validate that functional requirements are satisfied by the developed system and that there are no adverse effects on the overall process or other existing systems. The FDIC's SDLC Manual describes a SQT as "a comprehensive verification and validation process conducted to ensure that all capabilities and requirements of the system are exercised under both normal and stress conditions." SQT procedures cover all facets of a newly developed system, including screen functionality, database updates, user documentation, and security. In addition, there are certain pre-requisites for conducting an effective SQT. These include a fully integrated software system and completion of unit and integration testing.

The lack of a formal SQT for GENESYS allowed security weaknesses and numerous software bugs in GENESYS to go undetected until after DIRM and DOS began training the FDIC and state examiners on the software. Feedback from examiner training evaluation forms indicated that GENESYS was not ready for training or production implementation when DIRM and DOS initiated GENESYS training in August 1998 because the software contained run-time errors and numerous programming bugs. Some examiners suggested in their training evaluation forms that the implementation of GENESYS should be delayed to address the programming bugs that were identified during their training sessions.

In our opinion, DIRM should have delayed GENESYS training and implementation until the software had been thoroughly tested. Emphasis on meeting the GENESYS development schedule should not have obviated requirements to follow prescribed SDLC procedures. Initial impressions of a new software product are lasting ones and can have a significant impact on acceptance of the software within the user community. Training examiners on a software product that has not been completely tested and still had errors in it presented unnecessary risk to the successful implementation of GENESYS.

DIRM assumed additional risk by deviating from the phased testing approach prescribed by the FDIC's SDLC process. Specifically, DIRM performed a SQT, UAT, and pilot test of GENESYS in parallel. DIRM deviated from the phased testing approach prescribed by the FDIC's SDLC process in an attempt to meet an aggressive development schedule for GENESYS. However, the FDIC's SDLC Manual states that the SQT, UAT, and pilot tests are to be performed in a phased manner, starting with the SQT. The SDLC Manual also states that the UAT is the final test of the system and the SQT should be completed before the system is delivered to the UAT team.

Phased testing, as described in the FDIC's SDLC Manual, is designed to prevent the inefficiencies that are inherent in parallel testing, such as SQT and UAT testers performing identical test procedures on the same piece of software. In addition, because a SQT had not been completed for GENESYS, UAT testers experienced software problems that should have been identified and corrected during the SQT. Although a phased testing approach would most likely have required an extension to the GENESYS delivery date, potential efficiencies could have been significant.

We advised DIRM and DOS officials of the risks associated with concurrent testing on May 1, 1998. We pointed out that the FDIC's SDLC Manual prescribes a phased testing approach for newly developed systems and that a phased approach would help to ensure a successful implementation of GENESYS and acceptance within the user community. We also indicated that, in our opinion, there was unnecessary risk in proceeding with a pilot test of GENESYS, then scheduled to begin May 11, 1998, without first completing the SQT, followed by the UAT. Despite the concerns expressed by our office, DIRM and DOS officials indicated that they recognized the risks of performing concurrent tests and proceeded with the SQT, UAT, and pilot tests as planned.

Recommendation

We recommend that the Director, Division of Information Resources Management:

(6) Follow the phased testing approach prescribed by the FDIC's SDLC Manual for all future systems development projects and enhancements to existing systems.

BETTER INTERAGENCY COORDINATION NEEDED FOR FUTURE GENESYS AUTOMATION EFFORTS

Although the FDIC and FRS entered into a memorandum of understanding (MOU) establishing a sound framework for the development of GENESYS, a lack of adherence to the MOU caused inefficiencies and delays in the development process. Specifically, senior FDIC and FRS management did not formally approve a project work plan or other agreement defining the responsibilities of each agency on the project or the time and resources to be committed by each agency to GENESYS. We noted that the referenced MOU provided for the joint development and approval of a project work plan for GENESYS. Generally accepted SDLC principles also require a project work plan to be completed and approved before investing significant resources in life cycle development. The lack of an approved project work plan contributed to delays and inefficiencies during the GENESYS design phase when FRS provided a less than expected level of examiner support and temporarily withdrew from the project. Additional delays and inefficiencies were experienced during the development phase when FRS temporarily withdrew from the GENESYS project for a second time.

The FDIC also assumed unnecessary risk by proceeding with detailed design and development of FRS-specific requirements for GENESYS without FRS approvals of a project work plan, FRD or system design document. Although senior FDIC and FRS management were generally aware of the project's scope and objectives through high level briefings, generally accepted SDLC procedures require that critical SDLC deliverable products be completed and formally approved by key project participants before making significant investments in subsequent life cycle phases. We believe that the FDIC can improve its interagency coordination on the many planned enhancements to GENESYS by formalizing up-front interagency development agreements and adhering more closely to generally accepted SDLC procedures.

In January 1997, the FDIC and FRS entered into a MOU establishing a framework for the development of an interagency bank safety and soundness examination system. The agreement established an interagency task force comprised of FDIC, FRS, and state examiners for the purposes of (1) specifying a set of joint requirements for the system, (2) estimating the time and resources required to develop the system, and (3) proposing a development approach. The agreement also provided for regular involvement of senior FDIC and FRS management. Specifically, the MOU stated: “Final approval of all work products and recommendations of the examination team and IS support staff will be granted jointly by the FRS Director of Bank Supervision and Regulation and the FDIC Director of Supervision within two weeks of submission of project deliverables.”

In May 1997, the FDIC's DIRM and DOS completed a draft project work plan that contained a proposed approach for developing GENESYS and an estimate of the time and resources that the FDIC would dedicate to the development effort. However, the project work plan did not address the tasks or responsibilities of other agencies involved with the project, such as FRS or CSBS. The draft project work plan also did not address the resource commitments that those agencies would make to the project. Although the draft project work plan was subsequently approved by senior FDIC management, it was never approved by FRS management. We spoke with representatives of FRS and CSBS and learned that their agencies did not develop separate project work plans for GENESYS. The FRS and CSBS representatives informed us that they were relying on the FDIC to plan for the development of GENESYS.

In addition, no effort was made to quantify the level or source of resources that would be needed to address FRS-specific requirements that were not related to the FDIC's safety and soundness examination responsibilities. We noted that the FDIC was providing programming resources to satisfy FRS specific requirements and that the FDIC had made informal commitments to provide resources for FRS examiner training and software maintenance. In our opinion, DIRM and DOS management should obtain FDIC Board of Director approval prior to investing significant FDIC resources to satisfy non-FDIC requirements.

According to the FDIC's SDLC Manual, the purpose of a project work plan is to formally capture and document agreements among project participants regarding project scope, tasks, schedule, allocated resources, and interrelationships with other projects. The Manual states: "the Project Work Plan will make clear the responsibility and accountability of the various parties." By securing an informed agreement up-front, and revisiting the agreement throughout the project's life cycle, developers can better prevent cost and schedule overruns and ensure that the project will meet expected results. Obtaining formal, senior management approval of a project work plan also ensures that management has the information necessary to make informed decisions on the project and that changes in the project's scope, costs, and time schedules are adequately controlled.

In May 1997, the interagency task force completed a high level, 6-page requirements analysis for GENESYS. The analysis was approved by FDIC, FRS, and CSBS project managers for GENESYS. However, the analysis was not formally approved by senior FDIC and FRS management as required by the interagency MOU. Senior FDIC management approved a more detailed GENESYS FRD and system design document in August 1997 and October 1997, respectively. However, these documents were not approved by FRS management, as required by the MOU and generally accepted SDLC principles.

The FDIC's SDLC Manual states that user requirements must be defined, documented, and approved in a FRD before making significant investments in detailed design and development work. The SDLC Manual states that the FRD "serves as the foundation for system design and development." The SDLC Manual also states that detailed design specifications for a proposed system are to be documented and approved before making significant investments in development work. These principles are basic to the SDLC methodology.

FRS approval of the GENESYS FRD and system design document would have helped ensure that GENESYS met their needs and reflected a more clear indication of their level of commitment to the project. We noted that FRS raised several concerns regarding the GENESYS project in April 1997. These concerns included the amount of time and cost required to develop GENESYS, the lack of an interagency cost-benefit analysis, and the lack of risk-focused examination support proposed for the system. These concerns were a contributing factor in FRS' less than full commitment to the project during the design and development phases of GENESYS and their decision to temporarily withdraw from the project in May 1997 and November 1997. DIRM officials indicated that FRS' lack of commitment to the GENESYS project during 1997 caused significant disruption and delays to the project.

We believe the FDIC can more effectively evaluate the commitment of other organizations to joint development efforts by requiring those agencies to formally approve critical SDLC deliverable products before investing significant resources in subsequent SDLC phases. Joint approval of SDLC deliverable products will allow senior managers of participating agencies to better understand their role and responsibilities on IT projects, as well as the resources that are needed by each participant to complete the effort. Joint approval of SDLC deliverable products will also help ensure that system requirements and design meet agencies' needs.

Recommendations

We recommend that the Directors, Division of Information Resources Management and Division of Supervision:

(7) Formally document and obtain interagency approval of the scope, tasks, schedule, and resources associated with any major enhancement to GENESYS.

(8) Obtain formal, interagency approval of all SDLC deliverable products required by the FDIC's SDLC process for major planned GENESYS enhancements.

(9) Obtain FDIC Board of Director approval prior to investing significant FDIC resources to satisfy non-FDIC requirements on GENESYS.

NEED FOR CONTINUITY OF EXAMINATION STAFF

A high turnover of DOS examination staff assigned to the GENESYS project impeded critical development activities, including requirements definition and system design, and introduced unnecessary delays to the project schedule. We noted that four different DOS program managers were assigned to the GENESYS project during its 2 1/2-year development cycle. In addition, DOS examination staff assigned to work on the GENESYS project were replaced every 120 days.

The high turnover of examiners assigned to the GENESYS project resulted in differing perspectives on the design of the GENESYS modules and screens, resulting in changes to ongoing design and development efforts. In addition, because senior DOS and DIRM management had not formally approved a functional requirements or system design document until after development of GENESYS had begun, controls over design changes made by rotating examination staff were diminished. The inefficiencies and delays caused by the high turnover of DOS examination staff were exacerbated by an equally high turnover of FRS and state examiners working on the project and DIRM's use of an evolutionary prototyping approach for development.

Although work on an initial release of GENESYS was completed in August 1998, FDIC has already planned major enhancements to the system. We believe that DOS and DIRM can achieve significant time savings and efficiencies when addressing these planned GENESYS enhancements by appointing a permanent DOS program manager and maintaining a core staff of key personnel that are committed to the project until its completion.

The GENESYS developers recognized early in the project's life cycle that the high turnover of DOS examiners was affecting the efficiency and timeliness of the GENESYS development process. The GENESYS project work plan states: "All efforts required to bring new team members up to speed as existing team members depart and are replaced are essentially non-productive hours and will introduce delays in the schedule. Project experience to date has demonstrated that as new team members are brought on, significant team time is required to familiarize them with the project, their roles and their assignments, and to explain why certain decisions were made; resolved issues again become topics of debate and second-guessing. Loss of continuity becomes a problem, particularly when an assigned deliverable has a long development or delivery time, e.g., training materials or user manuals."

While some staff turnover on projects with long development schedules should be expected, sound business practices suggest that a program manager and a core group of program team members be maintained throughout a project's development life cycle. *Project Management for Mission Critical Systems*, a handbook developed by the Information Technology Resources Board (ITRB) in October 1997,[1] stresses the importance of keeping the core development team members together. The handbook recommends that management maintain a commitment to the integrity of key project players, including program office officials, from project conception through implementation. Senior DIRM and DOA management identified a high turnover of project staff as a contributing factor in the FDIC's recent decision to terminate another major corporate automation effort, TAPS. In addition, GAO has cited frequent turnover of project managers and other key development personnel as a common cause of system failures in the federal government.

The inefficiencies and delays caused by the high turnover of DOS examination staff were exacerbated by an equally high turnover of FRS and state examiners assigned to the project. We noted that FRS had assigned three different project managers to the GENESYS project and that CSBS had assigned four different project managers to the GENESYS project during 1997 and 1998. We also noted that FRS and CSBS examination staff turned over about every 30 to 90 days. In

[1] ITRB was created in July 1996 pursuant to Executive Order 13011. ITRB performs peer reviews of major systems initiatives in the federal government and publicizes the resulting lessons learned and promising practices. ITRB consists of IT, acquisition, and program professionals with significant experience in developing, acquiring, and managing information systems in the federal government.

addition, DIRM's decision to use an evolutionary prototyping approach for GENESYS development made the project more sensitive to personnel turnover. DIRM's evolutionary prototyping approach involved extensive developer/user interaction to build requirements and design specifications into a working software prototype. Developers placed less emphasis on maintaining up-to-date requirements and design documentation than prescribed by the FDIC's SDLC process. As a result, as examiners left the GENESYS project, so did much of the knowledge and rationale underlying why decisions relating to GENESYS requirements and design were made.

The DOS program manager for GENESYS informed us that some steps had been taken in late 1997 and 1998 to mitigate the impact of examiner turnover. For example, DOS examination staff improved GENESYS user documentation. However, the DOS program manager also indicated that in addition to the personal and professional disruption of being away from their duty station for an extended period, there were financial disadvantages for examiners on detail for more than 120 days.

We believe that DOS management should explore alternatives to detailing key examination staff to the GENESYS project for short periods of time. In our opinion, a core group of DOS staff should be assigned to development projects and planned enhancements to GENESYS from initiation through implementation. We recognize that the FDIC cannot direct the staff assignments of other organizations. However, the FDIC can significantly reduce its exposure to cost and schedule overruns on future systems development projects and planned enhancements to GENESYS by ensuring greater continuity of its assigned staff. The continuity associated with reduced examiner turnover should allow the FDIC to more efficiently address its role as the lead banking agency for the maintenance and development of the planned enhancements to GENESYS.

Recommendations

We recommend that the Director, Division of Supervision:

(10) Evaluate the feasibility of establishing a permanent staff to manage the development, operation, and maintenance of major DOS systems including GENESYS.

(11) Ensure that a core group of staff is assigned to future systems development or enhancement projects until the project is completed.

IMPROVED SAFEGUARDS NEEDED TO PROTECT CONFIDENTIAL BANK EXAMINATION DATA

GENESYS security features that were designed to prevent the unauthorized disclosure of confidential bank examination information need to be improved. Specifically, GENESYS uses a compression program called addZIP Compression Libraries (addZIP) to encrypt confidential bank examination data processed by GENESYS. However, addZIP does not encrypt sensitive files that are created and permanently stored on the laptop's hard drive each time users utilize the print function in GENESYS. When a user prints information in GENESYS, such as a report of examination page, GENESYS creates a copy of the printed information and stores it in plain text on the laptop's hard drive. Because printed information is stored outside of GENESYS, it is neither encrypted nor protected by the application's login ID and password.

In addition, a file containing GENESYS login IDs and passwords is saved to the laptop's hard drive in plain text whenever a user fails to exit the application properly. Examples of when a user would fail to exit the application properly include power disruptions, software errors requiring users to reboot the laptop, or users simply turning the laptop power off without first exiting GENESYS. Although the examiner laptops have power-on passwords that are intended to restrict access to any information contained on the laptop, these passwords can be circumvented by simply removing the laptop's battery.

Additionally, DIRM has not demonstrated that addZIP complies with Federal Information Processing Standards (FIPS) or broader industry standards governing the effective protection of sensitive data. We identified several Internet sites containing detailed descriptions of software programs capable of cracking addZIP's encryption algorithm. We obtained one such readily available freeware attack program from the Internet and successfully ran it against the GENESYS database. We were able to crack addZIP's encryption algorithm, obtain the passwords used to protect the database, and view confidential bank examination data. We noted that the passwords used by addZIP to protect the GENESYS database and data did not meet the corporate standards described in FDIC Circular 1360.10, *Corporate Password Standards*, including minimum length of passwords or use of alpha and numeric characters. We concluded that addZIP is not a reliable means of protecting sensitive data.

DIRM and DOS defined the information security requirements for GENESYS in the FRD and system design document. The FRD states: "GENESYS will contain volumes of institution specific financial information including detailed listings of the institution's loan customers. There will be several subjective comments concerning management and the institution's loan customers. This information is highly confidential…" The FRD identifies several security features that DIRM planned to implement to significantly reduce the likelihood of unauthorized access to GENESYS data, including the encryption of the application's database and the use of passwords to restrict access to the application. The FRD also states that GENESYS information security should comply with FIPS and the law.

DOS derived its information security requirements for GENESYS, in part, from Part 309 of FDIC's Rules and Regulations, which strictly prohibit the public disclosure of any information contained in a report of examination. FRS, as well as individual state banking regulators who will be using GENESYS, have similar legal restrictions over the public disclosure of bank examination findings and ratings. In addition, federal statutes protect the confidentiality of information pertaining to individual loan customers.

DIRM initially planned to ensure the confidentiality of sensitive GENESYS data using cryptographic security products developed by Entrust Technologies, Inc. Entrust Technologies has implemented in Entrust a cryptographic module which has been validated by the National Institute of Standards and Technology (NIST) and meets the Level 1 requirements of the standard. In addition, the GENESYS project work plan states that Entrust had been selected by FDIC as a corporate standard for data protection, encryption, and session security support. However, reservations expressed by FRS about the complexity of implementing and maintaining Entrust and emphasis on meeting the GENESYS development schedule delayed implementation of Entrust with GENESYS.

In May 1998, we learned that DIRM and DOS had proceeded with a live pilot implementation of GENESYS in four banks without any data encryption. We immediately discussed the FDIC's plans regarding the security of GENESYS data with DIRM and DOS officials and, in June 1998, DIRM decided to encrypt GENESYS data using addZIP. We were informed that addZIP would serve as an interim solution to GENESYS' encryption requirements until a permanent solution could be identified.

We researched and tested the data encryption capabilities of addZIP and identified several limitations:

- The GENESYS FRD states that one of the GENESYS security requirements is to comply with FIPS and the law. However, DIRM has not demonstrated that addZIP complies with NIST FIPS or broader industry standards governing the effective protection of sensitive data.

- There are several readily available software attack programs on the Internet capable of cracking addZIP's encryption algorithm. We successfully ran one such attack program against the GENESYS database and were able to crack addZIP's encryption algorithm and obtain the passwords used to protect the GENESYS database.

- Passwords used by addZIP to protect the GENESYS database did not meet the corporate standards described in FDIC Circular 1360.10, *Corporate Password Standards,* or broader industry standards, regarding length of passwords or use of alpha and numeric characters.

- AddZIP is compatible with PKzip[2], a widely used data compression program on personal computers. Data files compressed and encrypted using addZIP can also be decompressed and decrypted using PKzip. As a result, data could be read by unauthorized individuals with access to examiner laptop computers.

- Although a password can be used to protect data that is encrypted by addZIP, the password is not "hashed" (i.e., scrambled using an initializer to reduce the likelihood of it being deciphered by an attacker). Hashing is a basic tenet of modern encryption.

Security weaknesses, such as those discussed above, are typically detected and corrected during an application's SQT. The FDIC's SDLC Manual states that the purpose of a SQT is to validate that functional requirements, including security, are satisfied by the developed system and that there are

[2] PKzip is a registered trademark of PKWARE, Inc.

no adverse effects on the overall process or other existing systems. However, as discussed in an earlier section of this report, a formal SQT was not performed for GENESYS, despite concerns expressed by our office to senior DIRM and DOS management in May 1998. We advised the DIRM and DOS project managers for GENESYS of our findings regarding the limitations of GENESYS security on September 10, 1998 so that they could take appropriate actions in as timely a manner as possible. At the close of our field work, DIRM was researching the possibility of replacing addZIP with Entrust.

Applying new technologies to the bank examination process offers examiners significant advantages over traditional manual examination techniques. For example, GENESYS will improve the amount and timeliness of bank examination data available to examiners during examinations. Data query and analysis tools contained within GENESYS will also offer examiners a number of advantages over traditional manual examination techniques. However, advanced technology also presents new and potentially more serious security threats, such as the unauthorized disclosure of confidential bank examination information or the undetected alteration of sensitive data reported by or relating to a bank. Protecting sensitive bank examination information is an important element of public trust and confidence in bank supervision and regulation. While the measures taken to protect sensitive data should be commensurate with the security levels of the data being protected, we believe that improved safeguards are needed to ensure that confidential GENESYS data is adequately protected from unauthorized disclosure or alteration.

Recommendations

We recommend that the Director, Division of Information Resources Management:

(12) Incorporate security features into GENESYS that will adequately address the security requirements contained in the functional requirements document and that will provide reasonable assurance that confidential bank examination information will be adequately protected against unauthorized disclosure or alteration.

(13) Direct DIRM's Information Security Section to perform a security review of GENESYS to ensure compliance with corporate security standards and guidelines and to ensure that the application has adequate security.

TRACKING AND REPORTING OF GENESYS COST-BENEFIT INFORMATION CAN BE IMPROVED

Generally, DIRM and DOS needed to maintain more complete and up-to-date cost-benefit information on GENESYS throughout its life cycle. Although DIRM had an established process for tracking and reporting its expenditures on GENESYS, the process did not track or report significant program office costs incurred by DOS examiners and others assigned to the project. DIRM's process also did not track or report full life cycle (i.e., inception to date) costs for GENESYS. Program office and life cycle cost information are basic tenets of any successful IT investment decision making process.

In addition, we observed that GENESYS cost-benefit information had not been continually evaluated throughout the life cycle of GENESYS as material changes occurred from earlier projections. Tracking program office and life cycle costs on GENESYS enhancements will provide management with more accurate and complete IT cost data with which to measure performance and make critical investment decisions. Improved project information will also allow managers to better measure project performance by comparing cost data to original projections.

DIRM implemented the DIRM Budget Support System (DBSS) in 1997 to track the division's expenditures and commitments against approved budgets for each of its IT projects. DBSS tracked DIRM's expenditures and commitments on IT activities by allocating DIRM expenses, such as employee salaries, travel, and contractor billings, to specific IT projects. DIRM maintained this information in a centralized Lotus Notes[3] database. Periodic cost reports identifying budgets and related expenditures for selected IT projects were provided to the FDIC's IT Technical Committee and IT project managers for their consideration in making management decisions. Additional, high level cost-benefit information was developed for GENESYS as part of DIRM's annual planning and budgeting for new and ongoing IT projects and provided to the FDIC's IT Technical Committee.

While DBSS provided management with valuable financial information about GENESYS, the system did not account for significant DOS personnel and travel costs incurred on the project. The DOS program manager for GENESYS indicated that examiners began recording their hours spent on GENESYS in the Scheduling Hours and Reporting Package (SHARP) in January 1998. SHARP is a computerized hours tracking system used by DOS examiners to allocate their time spent on specific tasks. However, DIRM and DOS project personnel were not tracking or comparing DOS costs to projected cost estimates.

Although DOS personnel and travel costs were not being tracked or reported, the DIRM and DOS project managers for GENESYS indicated that significant DOS resources were being expended on the project. For example, the GENESYS project work plan, approved August 28, 1997 estimated that DOS would expend approximately $2.6 million in personnel resources on the project during the period of June 1, 1997 through December 31, 1998. We noted that the $2.6 million figure did not include DOS travel expenses or significant DOS personnel resources expended on the project prior to June 1, 1997.

OMB Circulars No. A-109, *Major Systems Acquisitions*, and No. A-11, *Planning, Budgeting, and Acquisition of Capital Assets*, require federal agencies to monitor the full life cycle costs of their IT investments, including all costs incurred to bring the investment to a form and location suitable for its intended use. For example, program office costs should be tracked as life cycle costs and compared to estimates and cost-benefit analyses throughout a project’s life cycle. Sound business practices also dictate that significant costs associated with system development projects be tracked and reported to management.

[3] Lotus Notes is a registered trademark of Lotus Development Corporation.

DIRM also did not track life cycle (i.e., inception to date) costs for GENESYS. We noted that DBSS contained only current year cost data and that the system was used primarily to ensure that DIRM's annual budget for GENESYS was not exceeded. The DIRM project manager for GENESYS indicated that, while not readily available, full life cycle cost data could be reconstructed for GENESYS by researching the project files. However, any reconstructed life cycle data would not be complete because program office costs were not being maintained. Further, unless full life cycle cost data is tracked, analyzed, and reported, it cannot benefit the FDIC's management decision making process.

We concluded that, as of the close of our field work, DIRM and DOS system development staff had not provided senior FDIC management with a full life cycle cost estimate for GENESYS that was reviewed and approved. The GENESYS project work plan, which was approved by senior DIRM and DOS management on August 28, 1997 estimated the cost to design, develop, and implement GENESYS to be approximately $7.4 million. This same estimate was also provided to the FDIC's Board of Directors in a formal request for expenditure authority dated July 15, 1997. However, the $7.4 million estimate significantly underestimated the total life cycle cost to the FDIC for developing and implementing GENESYS. Specifically, the $7.4 million figure did not include several million dollars[4] in DIRM and DOS personnel, contractor, travel, hardware, software and other costs incurred on the project from December 1995, when the project was initiated, through May 31, 1997. The $7.4 million estimate also did not include approximately $2.9 million in software support, maintenance, and enhancement costs that DIRM estimated would be incurred on the project during the period 1999 through 2002.

The DIRM project manager for GENESYS indicated that DOS program office and life cycle cost data were not being tracked or reported for GENESYS because the FDIC had no requirement to do so and because management had not requested this information. OMB Circulars No. A-11, *Planning, Budgeting, and Acquisition of Capital Assets*, and A-109, *Major System Acquisitions*, require federal agencies to monitor the full life cycle costs of their IT investments. Without periodic comparisons of original estimates and cost-benefit analyses to actual results, agencies cannot determine whether their IT investments will deliver promised benefits within cost and risk limitations. Government oversight agencies, such as OMB and GAO, have also stressed the need for current, accurate, and complete cost information on which to base IT investment decisions in publications, such as GAO’s February 1997 guide, *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies’ IT Investment Decision-making*.

In an OIG report, *Audit of FDIC Resource and Cost Tracking Systems for Information Systems Projects*, dated March 6, 1998 we recommended that DIRM and DOF work with representatives of the FDIC's business units to develop a capability to track and report total costs associated with IT projects, including program office costs. We also recommended that DIRM begin tracking and reporting full life cycle costs on IT projects. In addition, we recommended that DIRM develop policies and procedures that would require IT project managers to routinely review actual life cycle

[4] We were unable to quantify the exact amount of expenditures incurred by DIRM and DOS on the GENESYS project between December 1995 and May 31, 1997 because IT expenditures were not tracked and reported during this entire period. We estimated the total costs incurred by DIRM and DOS during this period using DIRM estimates and actual costs, where available.

information on project costs to date, expected benefits, estimated timelines for implementation, and risks and to compare that information with the information that was relied upon by senior management at the outset of the project. Because DIRM and DOF management agreed to implement actions that were responsive to our recommendations, we are making no recommendations in this report at this time.

CORPORATION COMMENTS AND OIG EVALUATION

On March 15, 1999 the Directors, DIRM and DOS, provided a written response to the draft report. The response is presented in Appendix I of this report. A summary of management's responses to the recommendations contained in this report follows.

The Director, DIRM, stated that DIRM recognizes the problems in the project management process. As stated in its previous response to the OIG's report entitled *Audit of the Time and Attendance Processing System Development Project (II),* dated February 22, 1999, DIRM has strengthened existing processes and established new mechanisms to address this overall problem. Specifically, the Director, DIRM, stated that DIRM had developed more complete and robust IT plans for all projects, implemented internal controls designed to ensure that developers adhere to required SDLC procedures, established new management reporting, and implemented a post implementation review program for new systems. DIRM has also established procedures to ensure that significant changes in major projects are brought to the IT Technical Committee for review and approval. In addition, DIRM implemented new procedures for conducting cost-benefit analyses (CBA) which will be formally published with the next release of the SDLC Manual, currently scheduled to be completed by April 30, 1999.

For recommendations 1-3, the Director, DIRM, stated that a formal CBA format and a $3 million threshold for performing CBAs exists for DIRM projects, but that these procedures were not in place when GENESYS was initiated. Subsequent to management's written response to our report, the Director, DIRM, and the IT Technical Committee decided to eliminate the $3 million CBA threshold. Beginning March 24, 1999, a specific dollar threshold will no longer be used for determining whether a CBA is required for IT projects. The IT Technical Committee planned to review all 1999 IT development projects to determine which projects require a CBA by March 30, 1999.

In addition, the Director, DIRM, will issue a memorandum to all DIRM project managers by March 31, 1999 re-emphasizing the new CBA guidelines. The DIRM memorandum will remind DIRM project managers to alert senior management to significant changes in cost-benefit information, timelines, or increased risk. The DIRM memorandum will also communicate new policy requiring project managers to formally revisit alternative solutions when significant scope, cost, risk, or schedule changes occur on IT projects. The Director, DIRM, stated, that significant cost deviations will be defined as over-runs of 20 percent or more and significant schedule slips as deviations of more than 60 days. However, subsequent to management's written response to our report, the IT Technical Committee decided to review any IT project that has been flagged with variances in DIRM's IT Plan Database. After reviewing these projects, the IT Technical

Committee will request briefings from the DIRM project manager and client sponsor on projects considered significant. If the impact of the variance warrants, the IT Technical Committee will recommend IT Council review. Procedures for performing, updating, and maintaining CBAs will be formally published in the next release of FDIC's SDLC Manual.

For recommendations 4-6, the Director, DIRM, will issue a memorandum to all DIRM project managers by March 31, 1999 re-emphasizing existing requirements that prerequisite SDLC phases be substantially completed and approved before proceeding with subsequent phases. This requirement will be highlighted in the upcoming SDLC revision. The referenced memorandum will also remind project managers to adhere to the phased testing approach prescribed by FDIC's SDLC Manual for all future systems development projects and enhancements. In addition, DIRM will make an assessment as to whether deviations from FDIC's SDLC process, similar to the evolutionary prototyping methodology used to develop GENESYS, may benefit FDIC's small, non-complex systems initiatives that involve short development schedules. An initial assessment of evolutionary prototyping will be completed by June 30, 1999, with a schedule for updating FDIC's SDLC Manual to be developed no later than July 30, 1999.

For recommendations 7-9, the Directors, DIRM and DOS, stated that an interagency steering committee had been established to oversee the development and enhancement of interagency bank examination tools, including GENESYS. The steering committee will formally approve all SDLC deliverable products required for any major GENESYS enhancement, including an interagency project work plan describing life cycle scope, tasks, schedule and resource estimates. In addition, DIRM and DOS will explicitly identify and present any significant resources for non-FDIC GENESYS requirements to the FDIC Board of Directors as part of the annual budget process. Any significant resources required for non-FDIC GENESYS requirements that were not approved as part of the annual budget process will also be presented to the FDIC Board of Directors for approval.

For recommendations 10 and 11, the Director, DOS, stated that a permanent Examination Specialist position had been created to manage DOS' bank examination software development, including GENESYS, and that 3 field examiners had been appointed for one-year detail assignments.

For recommendations 12 and 13, the Director, DIRM, stated that discussions were ongoing with representatives from the FRS and CSBS to identify a security solution for GENESYS. Once identified, the solution will be incorporated into the system with the implementation of GENESYS version 1.2, currently scheduled for release in the fourth quarter of 1999. In addition, DIRM has appointed an Information Security Section staff member to the project team who will be responsible for conducting appropriate reviews and other actions to ensure that GENESYS version 1.2 is in full compliance with corporate security standards.

The Corporation's response to the draft report provides the elements necessary for management decisions on each of the report's recommendations. Accordingly, no further response to this report is required. However, we are providing additional comments below regarding management's response to recommendations 3, 4, 5 and 9. Appendix II presents management's proposed actions on our recommendations and shows that there are management decisions for each recommendation in this report.

We state in Recommendation 3 that the Director, DIRM, revise the FDIC's SDLC Manual to require that as significant changes occur in a project's scope, risk, estimated resources, or timeframes, that these changes be approved by the IT Council. The OIG made a similar recommendation in a recently issued report entitled *Audit of the Time and Attendance Processing System Development Project II*, dated February 22, 1999. In its response to the TAPS report, recommendation 3 of this report, and subsequent correspondence, DIRM indicated that significant scope, cost, risk, and schedule changes would be presented to the IT Technical Committee for approval and that the IT Technical Committee would report significant issues to the IT Council.

On March 10, 1999 representatives of our office met with members of the IT Technical Committee and advised them that, in our opinion, the charters of the IT Technical Committee and IT Council place authority for approval of IT projects and related changes with the IT Council. In response to our discussion, the IT Technical Committee decided to review its charter and recommend modifications to the IT Council that would delegate responsibility for project review to the IT Technical Committee. As we indicated in the referenced March 10, 1999 meeting, we believe that responsibilities for reviewing and approving IT projects should remain with the IT Council.

In response to recommendations 4 and 5, the Director, DIRM, stated that DIRM project managers may continue to propose different development methodologies than the phased approach prescribed by FDIC's SDLC Manual when justified by business needs and circumstances. The Director, DIRM, added that proposals to utilize significantly different approaches to phased development will be considered on a case-by-case basis and approved or denied in writing by senior DIRM management after a review of the probable risks and benefits of the proposed approach. As stated in the body of this report, we believe that FDIC's large, complex systems initiatives, such as GENESYS, should follow the phased development methodology prescribed by FDIC’s SDLC process. In addition, we believe that prototyping techniques should be strictly limited to the requirements gathering phase of IT projects as prescribed by the FDIC's SDLC Manual. However, we recognize that evolutionary prototyping that extends beyond the requirements definition phase, similar to the methodology used on GENESYS, may be useful on FDIC's small, non-complex systems initiatives that involve short development schedules.

Any proposal to significantly deviate from the phased development approach prescribed by FDIC's SDLC process should include a formal written analysis of the risks and benefits associated with the alternative approach. In addition, proposals to significantly deviate from FDIC's SDLC process should, at a minimum, be approved in writing by the Director, DIRM, and the program office Director. Alternative development approachs should also be provided the IT Council for review and approval. As with any development effort, alternative approaches should require the completion and approval of all critical SDLC deliverable products prescribed by FDIC's SDLC Manual.

In response to recommendation 9, the Directors, DIRM and DOS, stated that their divisions will begin identifying and presenting any significant resources for non-FDIC GENESYS requirements to the FDIC Board of Directors as part of the annual budget process. Any significant resources required for non-FDIC GENESYS requirements that are not approved as part of the annual budget process will also be presented to the FDIC Board of Directors for approval. In our opinion, significant cost deviations associated with non-FDIC requirements should be presented to the IT Technical Committee for approval, just as significant cost deviations associated with FDIC requirements must be approved by the IT Technical Committee.

FDIC

Federal Deposit Insurance Corporation

3501 North Fairfax Drive, Arlington, VA 22226 Division of Information Resources Management

March 15, 1999

MEMORANDUM TO: David H. Loewenstein
Assistant Inspector General

FROM: Donald C. Demitros
Director, DIRM

James L. Sexton
Director, DOS

SUBJECT: Response to Draft Report Entitled *Follow-on Audit of the General Examination System (GENESYS) Development Project*

The Division of Information Resources Management (DIRM) and the Division of Supervision (DOS) appreciate the opportunity to formally respond to the recommendations contained in the subject report. In general, the recommendations in this report focus on breakdowns in the project management process and not on the quality of the product, with the exception of identified security weaknesses. In fact, the report states that that "GENESYS would generally satisfy their [the DOS examiners'] requirements for generating a safety and soundness ROE." DIRM recognizes the problems in the project management process and, as previously stated in its response to TAPS audit, has strengthened existing processes and established new mechanisms to address this overall problem. These include: more complete and robust IT plans for all projects; new management reporting; new guidelines for cost benefit analysis; post implementation reviews; and internal controls which tie to the steps in the SDLC.

Currently, each project that exceeds $200,000 has an IT Plan established at its inception along with the appointment of a project owner from the requesting division or office. New information is now being captured in the IT Plan including early warning, overall project issues, budget issues, project justification, milestones, budget, and expenditures. This information is being used to produce a new management report highlighting budget variances, project slippage, and project risks such as poor customer participation, project scope creep, technical challenges, staffing issues, contractor performance/management. Strict adherence is placed on cost and schedule. Expenditures for these projects are automatically updated via a direct tie to the DIRM budget system and requests to change completion dates for major project milestones require Branch Chief approval or higher for key projects. In addition, during the annual budget formulation process, the funding and justification of the project is reviewed by the requesting division's line management, the IT Technical Committee, and the IT Council. Procedures have been established to insure that any significant changes in major projects are brought before the IT Technical Committee for review and approval.

New procedures for conducting a cost benefit analysis, based on OMB and DOF guidelines, have been published and are being used on projects such as ETVS and CHRIS. These procedures will be formally published with the next release of the Systems Development Life Cycle Manual SDLC. DIRM is now conducting post implementation reviews, which include a level of review to assess a project at the time of design, as well as looking at a project after its implementation.

Also, our new internal controls are now tied to the specific SDLC processes to ensure that we are adhering to our development methodology. Following approval of the new management control plan for systems development, a copy will be provided to the OIG.

For recommendations 1-4 DIRM will reemphasize specific requirements and responsibilities to all project managers by March 31, 1999. This will be accomplished through the issuance of a memorandum from the Director of DIRM to all project managers clearly communicating the policies referenced in this response. For recommendations 5-8, DIRM will review and strengthen its SDLC, which it plans to revise by April 30, 1999, with later revisions as required. DIRM has previously complied with Recommendation 9, which entails obtaining Board of Director approval for significant investments in non-FDIC GENESYS requirements. No additional investments of this type are planned in 1999 or 2000. DOS has already started to establish permanent core staff to manage major systems development efforts as suggested in recommendations 10 and 11. Recommendations 12 and 13 entail the strengthening of GENESYS security, which is planned for future releases.

DIRM and DOS believe that the above actions will address the overall recommendations included in this report. The following outlines the corrective actions already taken or planned (including anticipated due dates) in response to each individual recommendation.

Recommendation 1 (DIRM)

> **Formally evaluate and document the feasibility and cost-benefit of alternative solutions for systems development projects, including major enhancements to GENESYS, using the guidelines in the FDIC's SDLC Manual before committing significant life cycle resources to a particular alternative.**

Corrective Action

> The SDLC currently requires a project budget package, including a formal evaluation of alternatives, be prepared for all corporate projects expected to exceed the IT Dollar threshold. This threshold, currently set at $3 million, and a new formal CBA format now exist but were not in place when GENESYS was initiated. These new guidelines and IT

dollar threshold, which are consistent with the DOF Directive on Cost Benefit Analysis Methodology for the Purchase or Development of Capital Assets (Circular 4310.1), have been used for recent projects, such as: the Structure Information Management System; Electronic Travel Voucher Processing System (ETVPS); and other non-application projects. Also, IT Plans are required for all projects exceeding $200,000 and, for any of these projects that are new, a cost justification must be developed which includes the full life cycle costs and benefits for the proposed alternative. These procedures and the IT Dollar thresholds will be formally published with the next release of the SDLC, which will clearly state the requirement for performing CBA's. DIRM, with the IT Committee, will, by April 30, 1999, also review the current dollar threshold to determine whether it warrants adjustment. As an interim measure, the new guidelines and IT dollar threshold will be reemphasized and formally communicated to all project managers by March 31, 1999.

DIRM will reinforce its efforts to review project progress with clients, ensuring their clear understanding and obtaining their approval of both original cost-benefit analyses, and changes that modify the results of those analyses. DIRM also will present the initial CBA and any updates for projects over $3 M to the IT Technical Committee. The IT Technical Committee will report any project issues to the IT Council.

Recommendation 2 (DIRM)

Revisit alternative solutions when significant scope, cost, risk, or schedule changes occur on future information technology projects.

Corrective Action

DIRM agrees that alternative solutions should be revisited when significant scope, cost, risk, or schedule changes occur on information technology projects. Alternative solutions will be revisited when CBAs are revised, which will occur when significant scope, cost, risk, or schedule changes occur on projects over the $3m threshold. Significant scope and risk determinations will be made by management from DIRM and the sponsoring FDIC division(s). Significant costs will be defined as projected over-runs of 20% or more, and significant schedule slips will defined as greater than 60 days. These procedures and the IT Dollar thresholds will be formally published with the next release of the SDLC, which will clearly state the requirement for performing CBA's. As an interim measure, the new guidelines and IT dollar threshold will be reemphasized and formally communicated to all project managers by March 31, 1999.

Recommendation 3 (DIRM)

Revise the FDIC's SDLC Manual to require that as significant changes occur in a project's scope, risk, estimated resources, or timeframes, that these changes be approved by the IT Council.

Corrective Action

Alerting senior management to significant deviations in cost-benefit information, timelines, or increased risk is now required of all DIRM project managers. Corrective actions already have been taken to ensure that such do not reoccur. IT plans, required for all projects exceeding $200,000 in expenditures, have warning flags automatically set to alert senior management when completion dates for major project milestones are slipping (Refer to Attachment 2). These flags are reviewed monthly and project managers are required to report to DIRM senior management to explain the issues and obstacles causing the warning flags. Changes to schedules and projected cost expenditures are tightly controlled. A Branch Chief must approve changes to schedules on all projects. The expenditures are automatically updated, and therefore controlled via the budget system. These requirements will be formally reemphasized and communicated to all project managers by March 31, 1999.

The IT Council provides the approval authority for the initiation of IT systems development projects. It is the responsibility of project managers and, if appropriate, Steering Committees, to ensure projects are reviewed and reevaluated at critical management checkpoints during the life cycle of the systems development effort. In addition, schedule slippage of more than 60 days or projected cost overruns of more than 20 percent for any major project will be presented to the IT Technical Committee for management action. The IT Committee will report these project issues to the IT Council. DIRM will arrange, by March 31, 1999, for the OIG to meet with the IT Committee to discuss the OIG proposal to change the charters of the IT Committee or IT Council to approve such deviations to project schedules or costs.

Recommendation 4 (DIRM)

Require the GENESYS development team to follow the phased development process prescribed by the FDIC's SDLC Manual for systems development projects, including any major enhancements to GENESYS.

Corrective Action

All DIRM project managers are responsible for ensuring that prerequisite SDLC phases are substantially complete and approved prior to proceeding with subsequent SDLC phases. This process is in place but was not regularly adhered to during the initial GENESYS systems development effort. Corrective actions have been taken to address these problems. The current GENESYS version 1.2 project is being closely monitored by management to ensure compliance with SDLC procedures.

The requirement to ensure that prerequisite SDLC phases are substantially complete and approved prior to proceeding with subsequent SDLC phases will be highlighted in the next SDLC revision. This requirement will be formally reemphasized and communicated to all project managers by March 31, 1999.

DIRM project managers may continue to propose different approaches to phased development than dictated in the SDLC as justified by business needs and circumstances. Any proposals to utilize significantly different approaches to phased development will be considered on a case-by-case basis, and approved or denied in writing by senior DIRM management after a review of the probable risks and benefits of the proposed approach.

Recommendation 5 (DIRM)

Determine whether evolutionary prototyping could benefit FDIC's small, non-complex systems initiatives that involve short development schedules. If DIRM determines that evolutionary prototyping is appropriate for select, small scale IT initiatives, then the FDIC's SDLC Manual should be amended to describe the type of methodology that will be used and specific criteria governing its use.

Corrective Action

The current FDIC SDLC methodology allows the use of prototyping in the Requirements Definition Phase to elicit customer feedback on screen layouts and basic system features. The prototype is developed and reviewed in an iterative process that continues until the customer is satisfied with the basic features and screen designs, which are then documented in the Functional Requirements Document. This prototyping methodology is often described as throwaway prototyping.

The GENESYS project made extensive use of this technique during the Requirements Definition Phase, building a prototype, however, that was not thrown away, but retained and ultimately adopted as the starting point for development of the fully featured and completely functional final system. As modules of GENESYS were completed in the Development Phase, screens and functionality were reviewed with examiners to confirm that the requirements and design had been effectively translated into working software. Often changes were requested by the examiners and then incorporated into the software. This iterative process, which lasted throughout the development phase and into the testing phase, can be viewed as a form of evolutionary prototyping.

DIRM will make an assessment of whether the evolutionary prototyping methodology could benefit FDIC's small, non-complex systems initiatives that involve short development schedules. If DIRM determines that evolutionary prototyping is appropriate for select, small scale IT initiatives, then the FDIC's SDLC Manual will be amended to describe the type of methodology that will be used and specific criteria governing its use. The initial assessment of the evolutionary prototyping methodology will be completed by June 30, 1999. A schedule for updating the SDLC Manual will be developed after the assessment is complete, but no later than July 30, 1999.

DIRM continues to retain the latitude to incorporate additional systems development practices into projects as required to supplement its standard SDLC methodology. If significant variations or supplements to the SDLC are contemplated for a project, the project managers are required to include them in their Project Work Plan deliverable, which is subject to management review and approval. Techniques such as Joint Application Design and Staged Delivery have been effectively incorporated into projects even though they are not explicitly referenced in the SDLC. DIRM believes that the ability to continue to utilize common software development methods in selected projects is a productive management practice.

Recommendation 6 (DIRM)

Follow the phased testing approach prescribed by the FDIC's SDLC Manual for all future systems development projects and enhancements to existing systems.

Corrective Action

DIRM agrees that a phased approach to comprehensive system testing, including unit and integration testing, system qualification testing and user acceptance testing, should and will be followed for all major system development and enhancement efforts, as prescribed by the SDLC. Pilot testing may be included or not, for a given project, based on the judgement of the project team and the desires, goals and objectives of the sponsoring agencies' management.

All development and enhancement projects will conduct appropriate testing, including unit and integration testing, system qualification testing and user acceptance testing, per the SDLC. Also per the SDLC, the project and program managers will exercise judgement in determining the length, intensity, number and location of participants, and other relevant testing factors for each test phase to conduct an overall testing activity that is appropriate in scale and duration to the system or modification being tested.

Recommendation 7 (DIRM/DOS)

Formally document and obtain interagency approval of the scope, tasks, schedule, and resources associated with any major enhancement to GENESYS.

Corrective Action

An interagency steering committee that will oversee development and enhancement of interagency bank examination tools, including GENESYS, has been formed. This committee includes management representatives from the FDIC, the Federal Reserve System and the Conference of State Bank Supervisors, which represents the state regulators. This committee provides high level direction for and oversight of the development and enhancement of interagency bank examination tools. All such development or enhancement cycles will begin with a planning phase, to include a detailed interagency project plan as a deliverable; this project plan will include cycle scope, tasks, schedule and resource estimates, and will be presented to the members of this committee for formal approval.

Recommendation 8 (DIRM/DOS)

Obtain formal, interagency approval of all SDLC deliverable products required by the FDIC's SDLC process for major planned GENESYS enhancements.

Corrective Action

As indicated in the response to Recommendation 7 above, an interagency steering committee has been formed to oversee development and enhancement of interagency bank examination tools, including GENESYS. All SDLC deliverable products required for any major GENESYS enhancement will require formal approval from this interagency committee.

Recommendation 9 (DIRM/DOS)

Obtain FDIC Board of Director approval prior to investing significant FDIC resources to satisfy non-FDIC requirements on GENESYS.

Corrective Action

The FDIC Board of Directors did approve a total of $7.3 million dollars for the development and support of GENESYS and related examination software through the year 2000 as part of a July 1997 Board Case to acquire contractor services for DOS information systems projects. Included within this Board Case was a GENESYS Project Work Plan, which noted that as a result of interagency discussion, FDIC would "assume the role of the primary development agency, with the participation of FDIC, FRS, and CSBS supervisory staff as needed."

DIRM annually presents a comprehensive budget request to the FDIC Board of Directors for approval. Any significant resources required for non-FDIC GENESYS requirements, beyond what has already been approved, will be explicitly identified and presented to the Board of Directors for approval via the annual budget request for the year in which these expenses are expected to be realized. Any significant resources required for non-FDIC GENESYS requirements that were not approved via the annual budget request would also be presented to the Board of Directors for approval.

Recommendation 10 (DOS)

Evaluate the feasibility of establishing a permanent staff to manage the development, operation, and maintenance of major DOS systems including GENESYS.

Corrective Action

DOS recognizes the need for a more permanent staff to oversee software development. However, to ensure the software satisfies the needs of the field staff, it is necessary that field staff be used as subject matter experts to oversee product development. Examination standards and policies are constantly changing and permanent Washington staff soon lose the knowledge necessary to be effective in examination software development. In an effort to provide continuity to project management, DOS Washington Policy Section established an Examination Specialist position to head software development; however, additional staffing will continue to be provided by field staff on detail assignments. For current GENESYS development, DOS has recruited three field examiners for one year details who will report directly to the Program Manager. Additional staffing will be provided from short-term details as needed. The Federal Reserve Board has also provided permanent staffing for developmental needs.

Recommendation 11 (DOS)

Ensure that a core group of staff is assigned to future systems development or enhancement projects until the project is completed.

Corrective Action

A problem that DOS faces regarding permanent staffing is recruiting field examiners to volunteer for extended assignments. We agree it is difficult to maintain continuity for application development when the subject matter experts are replaced every 120 days. However, if the detail assignment extends beyond 120 days, the detailee must change travel status to Category II as required by the General Travel Regulations. Examiners are reluctant to volunteer for these extended details because of personal and financial drawbacks of such assignments. Not only do the extended detail assignments to Washington take detailees away from families, but the loss of potential income can be significant. Additionally, examiners believe that long-term details can hurt career advancement opportunities because of lost examination experience while on the extended detail. However, as indicated above, we believe the steps already taken will provide the necessary continuity for the project going forward.

Recommendation 12 (DIRM)

Incorporate security features into GENESYS that will adequately address the security requirements contained in the functional requirements document and that will provide reasonable assurance that confidential bank examination information will be adequately protected against unauthorized disclosure or alteration.

Corrective Action

DIRM is committed to strengthening the security features contained within GENESYS to protect sensitive and confidential data contained in the system database. As explained in the audit report, the measures that are currently in place are interim measures that afforded some degree of protection while more robust and permanent measures could be identified and incorporated.

The GENESYS project team sought and acquired a waiver of the corporate policy requiring Entrust in order to release GENESYS as developed. One of the conditions of that waiver was conversion from the interim security solution to a more permanent solution during the version 1.2 enhancement cycle. DIRM has initiated this enhancement cycle, and discussions are in progress with the Federal Reserve and the Conference of State Bank Supervisors to identify a security solution that will be acceptable to all parties. Once identified, this solution will be incorporated into the product for implementation with the v1.2 release of the system.

Recommendation 13 (DIRM)

Direct DIRM's Information Security Section to perform a security review of GENESYS to ensure compliance with corporate security standards and guidelines and to ensure that the application has adequate security.

Corrective Action

DIRM proposes to address this recommendation in conjunction with the version 1.2 enhancement cycle for the GENESYS product. A security review of the current product will likely find the same weaknesses that have been identified in this audit report and would therefore be of little value. As noted in DIRM’s response to Recommendation 12, DIRM has already initiated the v1.2 enhancement cycle for the GENESYS product, and this cycle will include action to strengthen the security components of the GENESYS product. DIRM has appointed an Information Security Section staff member to the project team, and will conduct appropriate reviews and other actions to ensure that the v1.2 release of GENESYS is in full compliance with corporate security standards. DIRM proposes to deliver the v1.2 release of GENESYS during the fourth quarter of 1999.

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 and subsequent discussions with management representatives.

APPENDIX II

MANAGEMENT RESPONSES TO RECOMMENDATIONS

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 Corporation agreed with the recommendation. The IT Technical Committee will review all 1999 IT development projects to determine which projects require a CBA by March 30, 1999. DIRM will issue a memorandum to its project managers re-emphasizing SDLC policy regarding CBAs.	March 31, 1999	March 24, 1999 DIRM memorandum to OIG and DIRM memorandum to project managers.	None	Yes
2	The Corporation agreed with the recommendation. DIRM will issue a memorandum to its project managers reminding them to alert senior management to significant changes in cost-benefit information, timelines, or increased risk. The DIRM memorandum will also communicate new policy requiring project managers to formally revisit alternative solutions when significant scope, cost, risk, or schedule changes occur on IT projects.	March 31, 1999	DIRM memorandum to project managers	None	Yes
3	The Corporation agreed with the recommendation. DIRM will present significant scope, cost, risk, and schedule changes to the IT Technical Committee for approval. The IT Technical Committee will report this information to the IT Council. The IT Technical Committee will review any IT project that has been flagged with variances in DIRM's IT Plan Database. After reviewing these projects, the IT Technical Committee will request briefings from the DIRM project manager and client sponsor on projects considered significant. If the impact of the variance warrants, the IT Technical Committee will recommend IT Council review. Procedures for performing, updating, and maintaining CBAs will be formally published in the next release of FDIC's SDLC Manual.	March 24, 1999	Revision to the IT Technical Committee Charter or documentation indicating that the IT Council is reviewing IT projects.	None	Yes

APPENDIX II

MANAGEMENT RESPONSES TO RECOMMENDATIONS

4	The Corporation agreed with the recommendation. DIRM will issue a memorandum to all DIRM project managers re-emphasizing existing requirements that prerequisite SDLC phases be substantially completed and approved before proceeding with subsequent phases. This requirement will be highlighted in the upcoming SDLC revision, currently planned for April 30, 1999, with later revisions as required.	March 31, 1999	DIRM memorandum to project managers.	None	Yes
5	The Corporation agreed with the recommendation. DIRM will make an assessment as to whether deviations from FDIC's SDLC process, similar to the evolutionary prototyping methodology used to develop GENESYS, may benefit FDIC's small, non-complex systems initiatives that involve short development schedules. An initial assessment will be completed by June 30, 1999, with a schedule for updating FDIC's SDLC Manual to be developed no later than July 30, 1999.	July 30, 1999	DIRM assessment document and specific changes to the SDLC Manual.	None	Yes
6	The Corporation agreed with the recommendation. DIRM will issue a memorandum reminding its project managers to adhere to the phased testing approach prescribed by FDIC's SDLC Manual for all future systems development projects and enhancements.	March 31, 1999	DIRM memorandum to project managers.	None	Yes
7	The Corporation agreed with the recommendation. An interagency steering committee has been established to oversee the development and enhancement of interagency bank examination software, including GENESYS. The steering committee will formally approve an interagency project work plan describing life cycle scope, tasks, schedule and resource estimates for any major GENESYS enhancement.	October 6, 1998	DOS Regional Director Memorandum 98-097 and approved project work plan.	None	Yes
8	The Corporation agreed with the recommendation. An interagency steering committee has been established to oversee the development and enhancement of interagency bank examination software, including GENESYS. The steering committee will formally approve all SDLC deliverable products required for any major GENESYS enhancement.	October 6, 1998	DOS Regional Director Memorandum 98-097 and approved SDLC deliverable products.	None	Yes
9	The Corporation agreed with the recommendation. DIRM and DOS will explicitly identify and present any significant resources for non-FDIC GENESYS requirements to the FDIC Board of Directors as part of the annual budget process. Any significant resources required for non-FDIC GENESYS requirements that were not approved as part of the annual budget process will also be presented to the FDIC Board of Directors for approval.	March 15, 1999	DIRM and DOS budget documentation.	None	Yes

APPENDIX II

MANAGEMENT RESPONSES TO RECOMMENDATIONS

10	The Corporation agreed with the recommendation. A permanent Examination Specialist position has been created to manage DOS' bank examination software development, including GENESYS. In addition, 3 field examiners have been appointed to support the development of DOS' bank examination software for a period of one year.	January 4, 1999	Approved organization chart	None	Yes
11	The Corporation agreed with the recommendation. A permanent Examination Specialist position has been created to manage DOS' bank examination software development, including GENESYS. In addition, 3 field examiners have been appointed to support the development of DOS' bank examination software for a period of one year.	January 4, 1999	Approved organizational chart	None	Yes
12	The Corporation agreed with the recommendation. Discussions are ongoing with representatives of the FRS and CSBS to identify a security solution for GENESYS. Once identified, the solution will be incorporated into the system with the implementation of GENESYS version 1.2.	December 31, 1999	GENESYS system documentation	None	Yes
13	The Corporation agreed with the recommendation. DIRM appointed an Information Security Section staff member to the GENESYS project who will be responsible for conducting appropriate reviews to ensure that GENESYS version 1.2 is in full compliance with corporate security standards.	December 31, 1999	Document from DIRM Information Security Section indicating that GENESYS complies with corporate security standards.	None	Yes