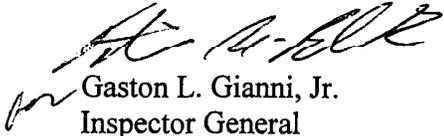




DATE: May 4, 2004

MEMORANDUM TO: Board of Directors
Audit Committce

FROM: 
Gaston L. Gianni, Jr.
Inspector General

SUBJECT: *Enhancements to the FDIC System Development Life Cycle
Methodology
(Report No. 04-019)*

Attached for your information is a copy of an audit report that the Office of Inspector General (OIG) recently issued. Also attached is a summary of the report.

This report presents the results of the OIG's audit of the Federal Deposit Insurance Corporation's (FDIC) system development life cycle (SDLC) methodology and control framework for the system development process. The objective of the audit was to determine whether the FDIC's SDLC methodology ensures the delivery of quality systems that satisfy corporate requirements in a timely and cost-effective manner.

We concluded that the FDIC had recently chosen a new SDLC methodology that was both risk-based and reflected industry and Federal government best practices. We also found that the FDIC had not developed an adequate control framework for system development to ensure that project management practices, performance assessment results, enterprise architecture alignment, funding decisions and cost-benefit analyses, and certification and accreditation guidance for security requirements were incorporated into development efforts. The report contains four recommendations to improve the system development control framework. The Corporation's response to this audit addressed the concerns we identified.

If you have any questions, please call me at (202) 416-2026 or Russell A. Rau, Assistant Inspector General for Audits, at (202) 416-2543.

Attachments



Office of Inspector General

April 30, 2004
Report No. 04-019

Enhancements to the FDIC System
Development Life Cycle Methodology

AUDIT REPORT



TABLE OF CONTENTS

BACKGROUND	1
RESULTS OF AUDIT	5
FINDING AND RECOMMENDATIONS	
Need for A Risk-Based SDLC Methodology and SDLC Control Framework	5
Risk-Based SDLC Methodology	5
SDLC Control Framework	7
ONGOING INITIATIVES	13
CONCLUSION AND RECOMMENDATIONS.....	13
Recommendations	14
CORPORATION COMMENTS AND OIG EVALUATION.....	14
APPENDIX I: OBJECTIVE, SCOPE, AND METHODOLOGY.....	16
APPENDIX II: WATERFALL AND ITERATIVE SYSTEM DEVELOPMENT MODELS.....	21
APPENDIX III: FEDERAL AGENCIES AND INDUSTRY ENTITIES THAT PROVIDED INFORMATION ON SDLC METHODOLOGY AND BEST PRACTICES	25
APPENDIX IV: PROJECT MANAGEMENT GUIDANCE	26
APPENDIX V: USEFUL BUSINESS MEASURES OF SYSTEM DEVELOPMENT PERFORMANCE	27
APPENDIX VI: CORPORATION COMMENTS.....	28
APPENDIX VII: MANAGEMENT RESPONSES TO RECOMMENDATIONS	31
FIGURES	
Figure 1: An Ideal SDLC Methodology and Control Framework.....	4
Figure 2: Waterfall Model of System Development.....	21
Figure 3: Spiral Software Development Life Cycle	22
Figure 4: COTS-Based Systems Approach.....	24



DATE: April 30, 2004

MEMORANDUM TO: Michael A. Bartell, Chief Information Officer and
Director, Division of Information Resources Management

FROM: Russell A. Rau
Assistant Inspector General for Audits

SUBJECT: *Enhancements to the FDIC System Development Life Cycle
Methodology*
(Report No. 04-019)

This report presents the results of our audit of the System Development Life Cycle (SDLC)¹ methodology at the Federal Deposit Insurance Corporation (FDIC).

We initiated this audit at the request of the former Acting Chief Information Officer to independently evaluate the existing SDLC methodology, in particular because the current methodology may need revisions to reflect current industry practices. In addition, recent Office of Inspector General (OIG) reports² indicated a need to improve the control framework for the system development process to adequately manage the scope, cost, and quality of information technology (IT) projects.

The objective of our audit was to determine whether the FDIC's SDLC methodology ensures the delivery of quality systems that satisfy corporate requirements in a timely and cost-effective manner. Appendix I describes in detail our objective, scope, and methodology.

BACKGROUND

The SDLC methodology is intended to guide the development and enhancement of information technology systems. An SDLC methodology includes those processes and practices reflected in an SDLC manual as well as other associated controls and activities used by developers to ensure system development efforts are well managed and meet user requirements. System development efforts budgeted for 2003 accounted for more than \$80 million, or 7 percent of the FDIC's 2003

¹ The SDLC is a multistage process (from establishing feasibility to carrying out post-implementation reviews) used to convert a management need into an application system that can be custom-developed, purchased, or a combination of both.

² The OIG recently issued two reports: *New Financial Environment Scope Management Controls* (Report No. 03-045), dated September 29, 2003; and *The New Financial Environment Project Control Framework* (Report No. 03-016), dated March 5, 2003.

annual operating budget; \$79 million is budgeted for 2004.³ The FDIC's Division of Information Resources Management (DIRM) is responsible for maintaining the SDLC methodology.

The *Systems Development Life Cycle Manual Version 3.0*, dated July 17, 1997, contains the FDIC's standard methodology for developing its automated information systems.⁴ The stated purpose of the FDIC's SDLC methodology is to provide a repeatable, uniform process to develop new FDIC automated information systems and enhance or maintain existing systems. The SDLC methodology applies to all IT projects,⁵ whether performed by the FDIC or through contract agreements.

The FDIC has identified the need to improve its SDLC methodology. This need was confirmed by the results of the recent DIRM Information Technology Program Assessment,⁶ which recommended that the SDLC methodology be modernized to adopt newer ways of doing business and best practices. DIRM selected a new SDLC methodology, Rational Unified Process^{®7} on February 20, 2004 and is in the process of engaging a contractor to tailor that methodology to the FDIC environment and ensure that it is scalable for various project sizes and types. DIRM plans to have the new methodology fully implemented by January 1, 2005.

Office of Management and Budget (OMB) Circular A-130⁸ requires the head of each federal agency to develop agency policies and procedures that provide for the timely acquisition of required information technology. Federal agency and industry best practice guidance related to an SDLC methodology is identified in various sources, including publications by the General Accounting Office (GAO), the Software Engineering Institute (SEI),⁹ and the Project Management Institute (PMI).¹⁰ These publications are discussed throughout this report.

Many methods and techniques can be used to direct system development life cycle processes, depending on the specific circumstances and risks of each development project. Two common system development models in industry and the federal government include the traditional linear sequential "waterfall" model and the more current iterative spiral model. Each phase of the

³ These amounts reflect budgeted expenditures for projects coded D (Development), E (Enhancement), P (Planning), and F (System Development Support projects).

⁴ Pursuant to FDIC Directive 1320.3, *Systems Development Life Cycle (SDLC) Version 3.0*, dated July 17, 1997.

⁵ An IT project is defined in FDIC Directive 1320.3 as the use of computer technology to automate the business process and practices of an organization. IT projects include a variety of initiatives, system development and maintenance projects, infrastructure projects, hardware and software acquisition projects, and IT planning projects.

⁶ In 2003, the FDIC contracted with Deloitte Consulting to conduct a comprehensive Information Technology Program Assessment (ITPA) with the objective of remaking the existing program into one that meets business needs effectively and efficiently. The recommendations from this program assessment are being implemented and include a new organizational structure, along with a variety of fundamental changes in the processes for managing IT.

⁷ Rational Unified Process[®] (RUP) is a risk-based program development methodology that establishes four phases of development. RUP is a registered trademark of Rational Software Corporation, which is a wholly owned subsidiary of International Business Machines Corporation.

⁸ OMB Circular No. A-130 Revised (Transmittal Memorandum No. 4), *Management of Federal Information Resources*.

⁹ Carnegie Mellon University's SEI is recognized for its experience in software development and acquisition processes. SEI has developed methods and models that can be used to define disciplined processes and determine whether an organization has implemented them. These methods and models are generally recognized as best business practices.

¹⁰ The PMI has conducted extensive research and analysis in the field of project management.

development process in the waterfall model is clearly defined and generally must be completed before moving to the next phase. A waterfall approach works well for projects with system requirements that can be defined and fixed early in the project. The spiral model is a risk-based iterative approach in which the overall project life cycle is composed of several sequential iterations or “mini-projects.” The spiral model works well when all project requirements are not known in advance, as is often the case with large, complex projects. Detailed descriptions of these system development models are provided in Appendix II.

The FDIC’s current SDLC methodology generally reflects a phased, waterfall-type model for systems development. Subsequent phase decisions, deliverables, and products are dependent on the decisions, deliverables, and products developed in prior phases. Unlike the classic waterfall model, the FDIC methodology does allow for development phases to be combined or overlapped, depending on the size and complexity of the project.

FDIC’s SDLC methodology has eight interdependent phases:

1. Planning
2. Requirements Definition
3. External Design
4. Internal Design
5. Development
6. Test
7. Implementation
8. Maintenance

The GAO *Standards for Internal Control in the Federal Government*¹¹ state that appropriate internal (management) control helps program managers improve operational processes and implement new technological developments. Management controls include both the day-to-day management of the project, such as scope, schedule, and cost controls, as well as controls that ensure the project is effectively coordinated with other related organizational projects. All of these controls collectively comprise a control framework to provide reasonable assurance of effective and efficient operations. An effective control framework for the SDLC methodology comprises:

- project management practices that are implemented to help the project meet cost, schedule, and performance goals;
- performance assessment practices, such as a post-implementation review¹² (PIR) feedback mechanism, that are used to provide continuous SDLC process improvement;
- investment management practices that ensure projects align with the agency Enterprise Architecture (EA)¹³ to avoid funding systems that are incompatible or provide redundant capability; and
- security management practices that ensure security requirements are addressed throughout the SDLC to cost-effectively reduce the risk of loss, misuse, or unauthorized access to or modification of information.

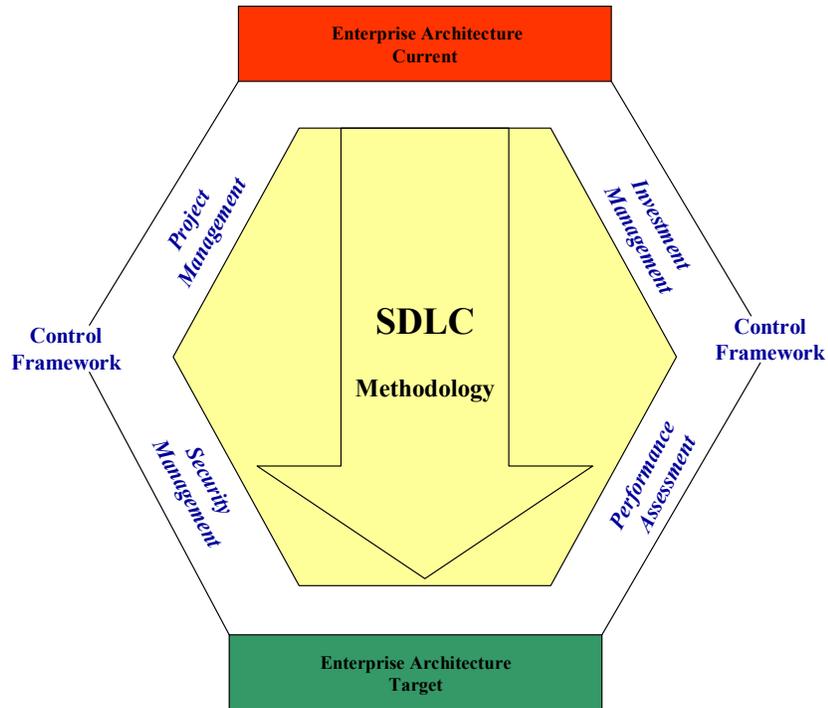
¹¹ GAO Publication GAO/AIMD-00-21-3.1, dated November 1999.

¹² Post-implementation reviews enable the FDIC to confirm the quality of system development projects and improve management over IT investments. The reviews provide "in process" feedback on the FDIC’s system development life cycle activities.

¹³ An EA is an institutional systems blueprint that defines in both business and technological terms an organization’s current and target operating environments (business and systems) and the way the organization will transition between the two. An EA is a requirement of OMB Circular A-130, based on the provisions of the Clinger-Cohen Act of 1996 (Public Law No. 104-106, codified throughout the U.S.C.). An EA is also a best practice of leading public and private-sector organizations.

Figure 1 depicts the ideal relationship between the SDLC methodology and its control framework.

Figure 1: An Ideal SDLC Methodology and Control Framework



Source: OIG analysis of federal agency and industry best practices.

RESULTS OF AUDIT

Consistent with DIRM concerns and the DIRM program assessment findings, we determined that the FDIC's existing SDLC methodology did not ensure the consistent delivery of quality systems that satisfy corporate requirements in a timely and cost-effective manner. Specifically, the existing SDLC methodology does not adequately reflect certain best practices, including a risk-based approach to system development and does not incorporate all the policies and procedures necessary to provide an effective SDLC control framework. Consequently, there is greater risk that projects will not meet cost, time, and performance goals and that the systems will not be consistent with the EA or incorporate adequate security requirements.

NEED FOR A RISK-BASED SDLC METHODOLOGY AND SDLC CONTROL FRAMEWORK

The FDIC's existing SDLC methodology does not provide for the use of an appropriate system development model based on risk¹⁴ considerations for each project. Further, the current SDLC control framework is not adequate to:

- integrate project management controls during the development process,
- assess project performance to ensure project success and provide feedback to continually improve the SDLC methodology,
- ensure consistency with the EA to avoid system incompatibility and duplication, and
- incorporate security management throughout the SDLC.

The FDIC's SDLC methodology has not been changed since 1997 and, therefore, does not reflect recent best practice guidance related to the use of risk-based system development models and procedures needed in a control framework.

Each component of this finding is discussed separately below.

Risk-Based SDLC Methodology

The FDIC's existing SDLC methodology recommends that the project manager consider the complexity and risk associated with a planned application in determining whether to use the current SDLC methodology for the project or whether to adapt the procedures and documentation required by the methodology. However, the FDIC's primary system development model is the linear sequential model, which is not the best model for all development projects. The SDLC methodology does not provide adequate guidance on the use of other development models, such as iterative models, that better address the specific risks of certain development efforts, especially those involving the use of commercial off-the-shelf (COTS) software. The FDIC's use of COTS software on two of its largest system development

¹⁴ Risks are situations or possible events that can cause a project to fail to meet its goals.

efforts, the New Financial Environment (NFE) and the Corporate Human Resources Information System (CHRIS),¹⁵ indicates that such guidance is needed to successfully complete those types of development efforts.

OMB Circular A-130 discusses an information system life cycle but does not define a preferred SDLC process model for use in the federal government. However, National Institute of Standards and Technology (NIST) guidance¹⁶ states that many methods exist that can be used by an organization to effectively develop an information system, including, among others, the traditional linear sequential, or waterfall model, and the spiral iterative model. NIST notes that the expected size and complexity of the system, development schedule, and length of a system's life will affect the decision on which the SDLC model will be used.

Best practice guidance issued by the Information Technology Resources Board (ITRB)¹⁷ indicates that an SDLC methodology should include a risk-based selection of a system development model. The ITRB Executive Handbook¹⁸ recommends that government agencies base selection of an appropriate development model on careful consideration of four project factors – cost, risk, complexity, and type. These four factors address:

- user requirements – the complexity of the desired system and when it is needed;
- resource requirements – the resources (human and monetary) available in comparison to those needed;

ITRB Executive Handbook factors for risk-based selection of an SDLC model.

Costs. Consider various development alternatives and estimate how they might contribute to project costs.

Risks. Consider how much risk the project faces from:

- High visibility due to public or political attention or requirements
- Highly compressed development time
- High uncertainty associated with the system's requirements, the technology that the system will employ, or the way that the system will affect business processes

Complexity. Consider the project to be complex if it:

- Affects many organizations or functional areas
- Results from business process reengineering, dramatically altering the use of information technology
- Requires new or rapidly advancing technology
- Requires a long time for development

Type. Consider the general type of the project:

- New development
- Modification of an existing system
- System integration

¹⁵ Both systems are being implemented with PeopleSoft® COTS software. PeopleSoft® is the second largest enterprise application software company in the world and the single largest vendor of mid-market solutions.

¹⁶ NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, dated October 2003.

¹⁷ The ITRB is a group of senior IT, acquisition, and program managers with significant experience developing, acquiring, and managing information systems in the federal government. Members are drawn from a cross section of agencies and are selected for their specific skills and knowledge. The ITRB provides, at no cost to agencies, peer reviews of major federal IT systems. Through these peer reviews, the ITRB identifies practical solutions to actual or potential problems.

¹⁸ ITRB publication *Project Management for Mission Critical Systems: A Handbook for Government Executives* (Executive Handbook), dated April 5, 2001.

- EA requirements – the desired system alignment with the current and target EA; and
- security requirements – what is the risk of system loss or negative publicity.

For example, an iterative model may be more appropriate for large and complex projects involving new technology that significantly affects the EA and for which there is a high level of uncertainty associated with the system’s requirements, such as security requirements. The waterfall model, however, may be appropriate for smaller projects requiring fewer resources with the purpose of modifying an existing system and for which there is limited impact on the EA.

The Department of Justice’s (DOJ) SDLC methodology considers the four factors noted above (project costs, risks, complexity, and type) and the mission criticality of the planned system when determining the system development model and level of work required. For example, DOJ’s methodology includes a “reduced effort” work pattern or model that combines some SDLC phases, eliminates some of the deliverables otherwise required, and combines some of the reviews to reduce project formality. This work pattern applies to any type of development, regardless of mission criticality, where the cost, risk, and complexity of the development project are low. The DOJ methodology also provides an iterative model suited to situations in which existing business processes will be altered considerably and the full set of detailed functional requirements cannot be reliably defined early in the development life cycle.

The SEI specifically recommends the use of the spiral iterative model for systems developed using COTS software to better address the risks of those projects. SEI notes that many organizations will find the transition to a risk-based spiral development approach one of the biggest challenges in implementing processes for COTS-based systems. Nonetheless, SEI stated that the change is needed because attempts to use traditional sequential processes are rarely successful.

SDLC Control Framework

Project Management

The FDIC has not incorporated all key project management¹⁹ practices for system development projects into its existing SDLC methodology. The methodology gives limited attention to project management practices aimed at controlling the development process with the goal of delivering quality systems within budget and time constraints. The methodology requires and provides some useful guidance on the preparation of key project management documents, such as a project (work) plan²⁰ and a work breakdown structure,²¹ but does not address other aspects of a project management control framework such as developing management plans (described later in this section of the report), conducting performance assessments, updating the project plan, and

¹⁹ Project management is the application of knowledge, skills, tools, and techniques to project activities to meet project requirements. Typically, project work, including system development efforts, involves coordination of competing demands affecting scope, time, cost, risk, and quality; stakeholders with differing needs and expectations; and identified requirements.

²⁰ The project plan is a formal, approved document or collection of documents used to manage project execution. The project plan should be expected to change over time as more information becomes available about the project.

²¹ A work breakdown structure organizes and defines the work within the scope of the project.

implementing corrective actions. In particular, the project plan guidance in the SDLC manual does not include the preparation of management plans, which are a major component of a project plan.

The PMI and project management experts have identified and developed the types of policies, procedures, and practices demonstrated to reduce development time and enhance effectiveness. The PMI's *A Guide to the Project Management Body of Knowledge* (PMBOK® Guide)²² identifies the importance of project management in managing and meeting project requirements. The PMBOK® Guide documents proven practices, tools, and techniques that have become generally accepted in the field of project management, including information systems development and implementation.

We primarily used the PMBOK® Guide, in conjunction with other government and industry guidance, as the primary criteria for reviewing the FDIC's SDLC methodology because the guide contains sound and prudent practices related to successful project management. The key project management activities identified in the PMBOK® Guide include preparing the project plan, preparing management plans for the PMBOK® knowledge areas, conducting performance assessment, updating the project plan, and implementing corrective action. Additional information about the PMBOK® Guide is included in Appendix IV of this report.

The PMBOK® Guide identifies nine distinct knowledge areas associated with successful project management:

- Integration
- Time
- Quality
- Communication
- Procurement management
- Scope
- Cost
- Human resources
- Risk

According to the PMBOK® Guide, a project plan should be prepared as part of project integration management. Also, management plans should be prepared for the areas of risk, scope, time/schedule, cost, quality, staffing, communications, and procurement. The management plans provide consideration for various contingencies and describe how each contingency will be managed. For example, the staffing management plan describes when and how human resources will be brought onto and taken off the project team. The cost management plan describes how cost variances will be managed (e.g., different responses to major variances than to minor ones.)

Another important management principle currently not incorporated in the SDLC methodology is an earned value management²³ system (EVMS). Performance measurement expressed in terms of earned value management is a tool to measure performance against the project plan. It integrates scope, cost, and schedule measures to help the project management team assess project performance. There are numerous benefits to an EVMS. First, it requires an adequate understanding of the work to be performed in order to assign a time-phased budget from the

²² The PMBOK® Guide was published in 2000 and is an approved standard of both the American National Standards Institute and the Institute of Electrical and Electronics Engineers.

²³ Earned value provides a valid method of measurement to compare planned project accomplishment to actual accomplishment. By comparing planned milestone completion against actual performance, project managers can estimate the amount of work remaining. The underlying concept of EVMS is that a project can be managed to reduce overall cost and schedule while delivering a quality product.

planned start through completion of the work. The performance management baseline established in this manner readily identifies problem areas such as underfunding, unrealistic schedules, and poor requirements or work content definition that can lead to later cost, schedule, and performance problems. An EVMS also serves as an excellent early warning system by identifying adverse variances in cost, schedule, and performance that may be driven by technical or business issues. Corrective actions based on an analysis of these variances can be more timely and the effects more visible than without an EVMS.

OMB Circular A-11²⁴ requires federal agencies to institute performance measures and management processes that monitor and compare actual performance to planned results. Agencies should use a performance-based acquisition management system, such as an EVMS, to obtain timely information on the progress of capital investments and to measure progress toward milestones in an independently verifiable basis in terms of cost, capability of the investment to meet specified requirements, timeliness, and quality. See Appendix V for the business measures GAO identified as useful for measuring system development performance.

OIG audits of the NFE and XBAT system development efforts²⁵ have identified a lack of project management practices for communication, risk, scope, time, and procurement management. However, the FDIC has not yet fully incorporated corrective actions in the SDLC methodology. Until these initiatives are in place and additional project management guidance is issued, the FDIC cannot be certain that it has addressed all of the risk factors that can undermine project success and there is greater potential for developing systems that exceed cost and schedule goals and do not meet users' needs.

In 2003, the FDIC identified the need for improved project management by commencing two initiatives in the project management arena. The first initiative was to begin formulating a Corporate Interdivisional Working Group for project management. The FDIC plans to offer training through the Corporate University to address identified corporate needs and expectations for project management. Additionally, DIRM has established an initiative to develop a program management office and has appointed an Assistant Director to establish the office. These initiatives are still in the planning stages and have not yet been implemented to improve the SDLC control framework.

Performance Assessment

The existing SDLC methodology incorporates performance measurement activities, such as quality assurance testing and a PIR process; however, DIRM has not always used the results of these activities to improve the existing SDLC methodology. Performance assessment is a critical function for measuring project progress and comparing it with established baselines. For maximum return on investment, the strategic value of IT projects should be documented before funding decisions are made and then verified after implementation. Common techniques for measuring performance include quality assurance testing and PIRs.

²⁴ OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, dated July 2003.

²⁵ *The New Financial Environment Project Control Framework* (Report No. 03-016), dated March 5, 2003; *New Financial Environment Scope Management Controls* (Report No. 03-045), dated September 29, 2003; and *XBAT Contracting and Project Management* (Report No. 04-014) dated March 26, 2004.

Quality Assurance Testing: The existing SDLC methodology identifies the need for quality assurance testing and refers to the FDIC Quality Assurance²⁶ program for guidance in the completion of this testing. The FDIC has performed quality assurance testing of selected recent system development efforts, but DIRM has not always used the results of that testing to improve the existing methodology. The FDIC issued Circular No. 1360.18, *FDIC Software Quality Assurance Policy*, on August 6, 2003 to provide direction on the independent testing and assessment of FDIC applications throughout their life cycle. The testing, such as independent verification and validation, helps answer the questions of “was the system built correctly?” and “was the correct system built?” The answers to these questions should be used to improve not only the performance of individual projects but also the adequacy of the overall SDLC methodology.

PIR Process: The existing SDLC methodology includes reference to the PIR process, which is now managed by the DIRM Information Technology Evaluation Section. The PIR process includes review of the SDLC documentation and interviews with the project team 6 months after a system is implemented. Recent PIRs have identified corrective actions needed for continual SDLC process improvement. However, not all corrective actions needed to improve the SDLC methodology have been implemented. Until December 2003, DIRM had not formally tracked PIR recommendations to determine the status of the recommended corrective actions.

The objectives of the FDIC’s PIR process are to:

- Assess management and end user satisfaction with the product.
- Determine how well the project met time schedules, implementation dates, and life-cycle cost projections.
- Identify best practices, lessons learned, and other improvements to project management activities.
- Identify the tangible and intangible benefits achieved.

OMB Circular A-130 requires that agencies conduct PIRs of information systems and information resource management processes to validate estimated benefits and costs and to document effective management practices for broader use. Agencies are to complete an evaluation of information systems once they are operational to validate projected savings, changes in practices, and effectiveness in serving stakeholders. These PIRs may also serve as the basis for agency-wide lessons learned on effective management practices.

Enterprise Architecture and Investment Management

The existing SDLC methodology acknowledges the importance of considering the FDIC’s EA²⁷ during a system development effort and refers to DIRM’s Strategic Planning Section (SPS) for guidance in using EA information in evaluating individual projects for alignment. The SPS has developed an EA Blueprint defining, at a high level, the FDIC’s current and target business and IT architectures. Additionally, the FDIC recently issued an EA policy, newsletter, and other general guidance indicating that information technology projects should align with the FDIC’s EA. However, the SPS has not issued detailed guidance on how compliance with this important EA control activity is to be accomplished. For example, current guidance does not describe how

²⁶ Quality assurance is the technical and administrative process to ensure the complete and accurate specification, implementation, and verification of all FDIC application requirements.

²⁷ Referred to throughout the existing methodology as an information architecture.

to use the EA Blueprint and repository information to evaluate alignment throughout the SDLC for all information technology projects. Current guidance also does not address how the evaluation for EA alignment will be used to support funding decisions when system development is based on an iterative development model. Each of these issues is discussed in more detail below.

The federal Chief Information Officer's (CIO) Council²⁸ acknowledges that an EA is essential for evolving information systems and developing new systems that optimize their mission value. OMB Circular A-130 instructs federal agencies to base investments in information technology on the agency EA. Additionally, the GAO has noted that developing, maintaining, and using architectures, or blueprints, is a best practice in engineering individual systems and entire enterprises. GAO has also acknowledged that it is important to ensure that systems are built and modified within the context of the EA that the system supports.

Alignment with FDIC's EA: The DIRM SPS has prepared draft checklists that could be used when reviewing SDLC documents, such as business cases, for evidence of EA alignment. However, these checklists have been issued in draft form only and do not provide detailed guidance for evaluating a project for alignment with the FDIC's EA. For example, the planning phase EA checklist No. 1 addresses whether the project adequately identifies data sharing and exchange opportunities, which could indicate EA alignment. The checklist, however, does not explain how to identify and document such opportunities. Also, the SPS has prepared draft guidance on how and when to report EA alignment information to oversight committees, for both large and small projects, but the guidance does not reflect how the procedures would change for iterative development processes. The evaluation of EA alignment may be required more frequently with an iterative development process because the complete system architecture may not be known in the early stages of the project but is developed and refined over time as each iteration is completed.

The GAO found that attempting to define system-level architectures (e.g., requirements and design specifications) and to use them to build systems without an EA or alignment with an EA often results in systems that are duplicative, poorly integrated, unnecessarily costly to maintain, and limited in terms of optimizing mission performance.

Investment Funding Based on EA Alignment: The FDIC's EA policy²⁹ requires that consistency with the EA shall be one of the decision criteria for funding IT investments. Small and large projects should be reviewed for alignment with the EA before funding is authorized. The FDIC's Capital Planning and Investment Management (CPIM)³⁰ process and the EA Blueprint provide general guidelines for when and how to perform these funding reviews. These guidelines, however, do not yet address funding issues that may arise from the use of iterative development processes. The FDIC guidance does not describe how and when EA alignment will be reviewed and the related funding established for each iteration. Consequently, the FDIC

²⁸ The CIO Council serves as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of federal agency information resources.

²⁹ FDIC Directive 1303.1, *FDIC Enterprise Architecture Program*, dated November 7, 2003.

³⁰ The CPIM process identifies the steps and activities necessary to ensure that the FDIC's capital investments are well thought out and cost-effective and support the mission and business goals of the Corporation.

would not be assured that IT investments developed using an iterative approach are adequately evaluated for EA alignment prior to funding.

Additionally, the existing SDLC methodology indicates that a project may need a cost-benefit analysis (CBA) but does not provide guidance for its preparation or the criteria for updating the CBA. The CPIM requires a CBA as part of the business case to seek funding for the system development effort and that project sponsors submit an updated CBA when the procurement process or other factors result in substantially different cost estimates. However, the CPIM process provides only limited guidance on identifying and evaluating the factors that might require an update to the CBA.

OMB Circular A-130 requires federal agencies to prepare and update a CBA³¹ for each information system throughout its life cycle. OMB explains that cost-benefit analyses provide vital management information on the most efficient allocation of human, financial, and information resources to support agency missions. When preparing CBAs to support IT investments, agencies should seek to quantify the improvements in agency performance results through the measurement of program outputs. This analysis should not merely serve as budget justification material, but should be part of the ongoing management oversight process to ensure prudent allocation of scarce resources.

Reasons for updating a CBA may include:

- Significant changes in projected costs and benefits,
- Significant changes in information technology capabilities,
- Major changes in requirements (including legislative or regulatory changes), or
- Empirical data based on performance measurement gained through prototype results or pilot experience.

OMB Circular A-130 does not require a new CBA at each stage of the information system life cycle, but notes it is useful to refresh these analyses with up-to-date information to ensure the continued viability of an information system prior to and during implementation.

Security Management

NIST Special Publication 800-64 *Security Considerations in the Information System Development Life Cycle*, dated October 2003, notes that including information security early in the SDLC will usually result in less expensive and more effective security than adding it to an operational system. To be most effective, information security must be integrated into the SDLC from system inception. The *Systems Development Life Cycle Manual Version 3.0*, dated July 17, 1997, recognizes the need to consider security activities throughout the SDLC and references guidance on the security requirements for each project, including security certification and accreditation (C&A).³² DIRM has issued Internal Policy Memorandum 03-011, *Policy on Incorporating Information Security into the System Development Life Cycle*, dated December 19, 2003, to provide interim guidance for FDIC's C&A Program by requiring that the information security tasks, deliverables, and approval requirements be addressed in each of the eight phases of the current SDLC methodology. The DIRM policy memorandum notes that a more robust

³¹ Referred to in OMB Circular A-130 as a benefit-cost analysis (BCA).

³² C&A refers to the official management decision to authorize operation of an information system that has undergone a comprehensive evaluation of the management, operational, and technical security controls in an information system.

formalized C&A Program will follow. In addition, the interim guidance does not reference draft C&A guidelines proposed by NIST.³³ Until more detailed guidance is provided as part of the FDIC C&A program, there may be inconsistent applications of C&A practices that affect, among other things, testing requirements.

ONGOING INITIATIVES

The FDIC has recognized the importance of replacing its SDLC methodology. One of the 2004 Corporate Performance Objectives is to select and implement a new SDLC methodology. In that regard, DIRM selected a new risk-based SDLC methodology on February 20, 2004 and is in the process of hiring a contractor to tailor that methodology to the FDIC environment and ensure that it is scalable for various projects. Specifically, the draft Statement of Work (SOW) requires the contractor to tailor the SDLC methodology to address FDIC-specific requirements, including development and maintenance of projects of varying size, complexity, and risk as well as COTS products. The SOW also requires the contractor to assess which FDIC policies and procedures may need to be modified and/or defined such as integration with the Program Management Office, quality assurance (performance assessment) function, EA, and C&A. The contractor, however, is not tasked with preparing any of the policy and procedure changes or additions that may be needed.

Additionally, DIRM has either issued or is developing guidance for project management, performance assessment, and EA. However, much of the guidance is at the conceptual stage and is not supported by detailed information for the project managers to use in developing information systems. Further, DIRM has developed an interim policy on C&A, but has not yet finalized procedures for implementing the policy.

CONCLUSION AND RECOMMENDATIONS

Our audit has identified best practices that should be associated with the SDLC methodology and related control framework that will be adopted by the Corporation. Because the FDIC has selected a risk-based SDLC methodology and developed a SOW to implement the new methodology, we are not making any recommendations related to the selection of a risk-based SDLC methodology. However, as DIRM implements the new methodology, DIRM should promptly implement the necessary control framework. Doing so would provide the Corporation with greater assurance that projects meet cost, schedule, and quality goals; the development process continually improves; all system development projects are consistent with the FDIC EA, and effective security controls exist in all completed systems.

³³ See NIST draft Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Technology Systems*, dated June 2003. This publication will supersede Federal Information Processing Standards Publication 102, *Guidelines for Computer Security Certification and Accreditation*, dated September 1983, and will establish a standard process, general tasks, and specific subtasks to certify and accredit federal IT systems.

Recommendations

We recommend that the CIO and Director, DIRM, establish and issue appropriate detailed implementing guidance to:

- (1) Integrate the key project management activities identified in the PMBOK[®] guide with the development process. These key activities include preparing the project plan, preparing the management plans in the nine knowledge areas, and adopting an EVMS.
- (2) Incorporate the results of performance assessment practices such as performing quality assurance testing and PIRs into the development process.
- (3) Align systems development with the FDIC's EA, establish how funding will be reviewed and provided in an iterative development environment, and update cost-benefit analyses during the life cycle of the system.
- (4) Incorporate NIST guidance for C&A of security requirements.

CORPORATION COMMENTS AND OIG EVALUATION

On April 27, 2004, the DIRM Director provided a written response to the draft report. The response is presented in its entirety in Appendix VI of this report. DIRM generally concurred with the report's findings and agreed to continue ongoing actions regarding the report's recommendations. These recommendations are considered resolved but will remain undispositioned and open until we have determined that agreed-to corrective action has been implemented and is effective. The responses to the recommendations are summarized below.

- DIRM will establish an Enterprise Program Management Office (PMO), which will standardize project management processes across all information technology projects. This will include improved procedures for project initiation, project planning, project execution and control, and project closeout.
- The DIRM PMO will periodically review the results from performance assessment activities (such as quality assurance testing and post-implementation reviews) to ensure that best practices and lessons learned are incorporated into future project/development processes.
- The Corporation's EA program will assist in supporting decision-making bodies in determining which new system projects will be undertaken and their alignment with new or existing architectures. The PMO will be one of many additional control points to ensure that the Corporation's EA is understood and applied to projects.
- FDIC guidelines for applying new C&A standards are in place, and briefings are underway to discuss the new processes and evaluate impact on project plans.

With respect to the response addressing C&A standards, more needs to be done before the guidelines are fully established and in place. Specifically, DIRM has issued an initial policy to provide a framework for FDIC's federally-mandated C&A program and has drafted a policy

specifically focused on C&A. In addition, DIRM issued *Guidelines on Implementing Certification and Accreditation for FDIC Systems*, on February 17, 2004. These guidelines outline C&A activities, but do not provide detailed implementing guidance on how C&A is to be conducted. Without such detailed guidance, FDIC cannot be assured that C&A activities, including testing, will be conducted effectively and consistently.

The CIO also provided comments on DIRM's Transformation program, including initiatives on adoption of improved practices in systems engineering, project management, capital investment planning, enterprise architecture, and security planning. One of the goals of the Transformation program is to assist DIRM in restructuring its operations in order to provide the most cost-efficient, customer-oriented service possible to all FDIC divisions and offices. The Transformation Office's mission is to manage the organizational and program changes, resulting from a 2003 independent IT Program Assessment, that are approved for implementation by FDIC and DIRM senior management.

Transformation activities began this year and will continue over a period of several years. The CIO stated that DIRM is addressing the issues discussed in this report in a highly-integrated and in-depth manner through the Transformation program and that significant progress and results in these areas are expected by the end of 2005.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The overall objective of our audit was to determine whether the FDIC's SDLC methodology ensures the delivery of quality systems that satisfy corporate requirements in a timely and cost-effective manner. As part of our audit, we examined: (1) The adequacy and cost-effectiveness of management controls in the FDIC's SDLC methodology and (2) federal agency and industry best practices for managing information system development projects. To achieve this objective, we conducted on-line research, interviews, and analysis of government and industry best practices in SDLC methodology. Appendix III contains a complete listing of the agency and industry entities that provided information on SDLC. We performed our work from November 2003 through February 2004 in accordance with generally accepted government auditing standards.

Scope

DIRM engaged a consultant to conduct an Information Technology Program Assessment (ITPA) of the FDIC's IT program management in 2003. The consultant recommended enhancing and updating the SDLC methodology as one of three activities that could be addressed in a 3- to 6-month timeframe. The consultant's report stated that the objective of the SDLC review should be to refine the SDLC methodology by incorporating the best elements of more recent approaches to system development. The following key activities should be included in completing the methodology selection:

- review the current SDLC methodology,
- gather information on current thinking and best practices in SDLC,
- collect external benchmarks that can be used to identify strengths and areas for improvement, and
- gather and prioritize requirements for enhancing methodology.

We focused our efforts on addressing these key activities.

In addition to reviewing the SDLC methodology, we reviewed the SDLC IT control framework. This control framework includes project management, performance assessment, the enterprise architecture, and security management.

Current SDLC Process

To gain an understanding of FDIC's current SDLC practices, we reviewed:

- *FDIC System Development Life Cycle Manual version 3.0*, dated July 1997.
- FDIC Circular 1320.3, *Systems Development Life Cycle Version 3.0*, dated July 17, 1997.
- FDIC Circular 1320.4, *FDIC Software Configuration Management Policy*, dated July 8, 2003.

- FDIC Circular 1360.18, *FDIC Software Quality Assurance Policy*, dated August 6, 2003.
- FDIC Circular 1303.1, *FDIC Enterprise Architecture Program*, dated November 7, 2003.
- DIRM Policy No. 03-011, *Policy on Incorporating Information Security into the System Development Life Cycle*, dated December 19, 2003.

Areas Identified for Improvement

To obtain an understanding of areas for improvement in the FDIC SDLC methodology and perceived best practices, we interviewed DIRM assistant directors responsible for application development. We conducted interviews of two project managers assigned to DIRM-identified project successes for best practices. We also interviewed other DIRM employees and the ITPA consultant and analyzed the FDIC's *Systems Development Life Cycle Manual Version 3.0* and prior OIG reports to identify potential areas for improvement in the FDIC's current SDLC process. Specifically, we reviewed three recently issued OIG reports:

- *The New Financial Environment Project Control Framework* (Report No. 03-016), dated March 5, 2003;
- *New Financial Environment Scope Management Controls* (Report No. 03-045), dated September 29, 2003; and,
- *XBAT Contracting and Project Management* (Report No. 04-014) dated March 26, 2004.

These reports concluded that improvements are needed in the SDLC practices to help ensure that FDIC system development efforts are more effectively controlled for scope, cost, and quality.

Selected Federal Agencies With Best Practices

To select agencies with SDLC best practices, we contacted the General Accounting Office (GAO) whose work in government oversight provided an overview of agency activities for system development. The GAO identified SDLC best practices adopted by the Federal Aviation Administration (FAA) and the Department of the Treasury's Financial Management Services. We also included the Federal Reserve Board, Department of Labor, and Department of Justice in our analysis of SDLC best practices based on preliminary research conducted by DIRM or identified through research with other agencies.

Selected Industry Entities With Best Practices

We conducted research to select industry entities with SDLC best practices. Our research showed and GAO confirmed that Carnegie Mellon's Software Engineering Institute is a leading authority on SDLC. Also, to identify process improvements we obtained SDLC best practices work conducted by International Business Machines and Deloitte Consulting as part of two contracts with DIRM. We also selected Software Productivity Research to provide insight on

software development performance measurement. Finally, Forrester Group and PricewaterhouseCoopers presented best practices on project management to some FDIC managers; we reviewed those practices for applicability to SDLC best practices.

Methodology

For each of the entities above, we obtained documentation related to SDLC or project management, conducted interviews to clarify our understanding of the documents presented, and reviewed the theories, practices, processes, and controls. We interviewed the FDIC personnel currently responsible for maintaining the SDLC to identify the scope of efforts completed to date for SDLC improvement. To obtain relevant information on best practices, we conducted extensive on-line research of SDLC theories and methodologies put forward by academicians and practitioners.

We evaluated the FDIC's SDLC process using industry and Federal agency best practices that addressed the potential improvement areas identified through our interviews and reviews of reports and the *FDIC System Development Life Cycle Manual version 3.0*. We used the Project Management Institute's *A Guide to the Project Management Body of Knowledge (PMBOK®)*, 2000 Edition as our primary resource for evaluating FDIC's SDLC project management activities. PMBOK® describes generally accepted project management knowledge and practices applicable to most projects by organizing the processes into nine knowledge areas (i.e., integration, scope, time, cost, quality, human resources, communication, risk, and procurement management). The nine knowledge areas provide the practices needed to manage a successful SDLC. In addition, we evaluated the SDLC for coverage of security controls cited in National Institute of Standards and Technology (NIST) Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* and post-implementation review requirements contained in Office of Management and Budget (OMB) Circular A-130, Transmittal 4.

To enhance our understanding of the enterprise architecture framework as it relates to the SDLC, we reviewed three GAO reports:

- *Information Technology - Enterprise Architecture Use Across the Federal Government Can Be Improved*, GAO-02-6, dated February 2002.
- *Information Technology – OMB Leadership Critical to Making Needed Enterprise Architecture and E-government Progress*, GAO-02-389T, dated March 21, 2002.
- *Air Traffic Control – FAA's Modernization Efforts – Past, Present, and Future*, GAO-04-227T, dated October 30, 2003.

Lastly, we contacted the FDIC's Corporate University and the manager of DIRM's new Program Management Office to determine the actions being taken to promote and develop good project management skills for SDLC project managers.

Management Controls

We limited our assessment of DIRM's system of internal controls to gaining an understanding of the division's procedures for developing systems. Specifically, we evaluated (1) the adequacy of processes to maintain and update procedures and controls; (2) FDIC's objectives for its SDLC processes; (3) project management controls for ensuring delivery of quality, risk-managed systems within time and budget constraints; and (4) the FDIC control framework for evaluating system development efforts. We did not test internal controls; however, the fact that we did not perform those tests did not affect our ability to achieve the stated audit objectives or the audit results.

Government Performance Results Act³⁴

The FDIC 2004 Corporate Performance Objectives include the selection and implementation of a new SDLC methodology. To meet this objective, DIRM has undertaken a review of the current SDLC and federal agency and industry best practices related to systems development with a goal of selecting and implementing a new SDLC methodology by November 1, 2004.

Reliance on Computer Generated Data

We relied on computer-generated data from DIRM's Project Number Information Application to compute the estimated budgeted system development costs for 2003 and 2004. Also, we used computer-generated data from the FDIC Financial Data Warehouse to identify the total FDIC budget for 2003. We did not perform specific tests to determine the reliability of computer-processed data, because the results of our audit were not based on such data.

Summary of Prior Audit Coverage

The OIG issued Report No. 97-012, *Audit of FDIC's System Development Life Cycle Methodology*, dated January 30, 1997. This report provided nine recommendations for improving the FDIC SDLC methodology. The report indicated that management provided responses for all nine recommendations that met the requisites of a management decision. We did not perform any detailed procedures to specifically follow up on the corrective actions related to the nine recommendations.

³⁴ The Government Performance and Results Act of 1993 (Pub. L. No. 103-62, codified at Title 5 and 31, U.S.C.) was enacted to improve the management, effectiveness, and accountability of federal programs. The Results Act requires most federal agencies, including the FDIC, to develop a strategic plan that broadly defines the agency's mission and vision, an annual performance plan that translates the vision and goals of the strategic plan into measurable objectives, and an annual performance report that compares actual results against planned goals.

Compliance With Laws and Regulations

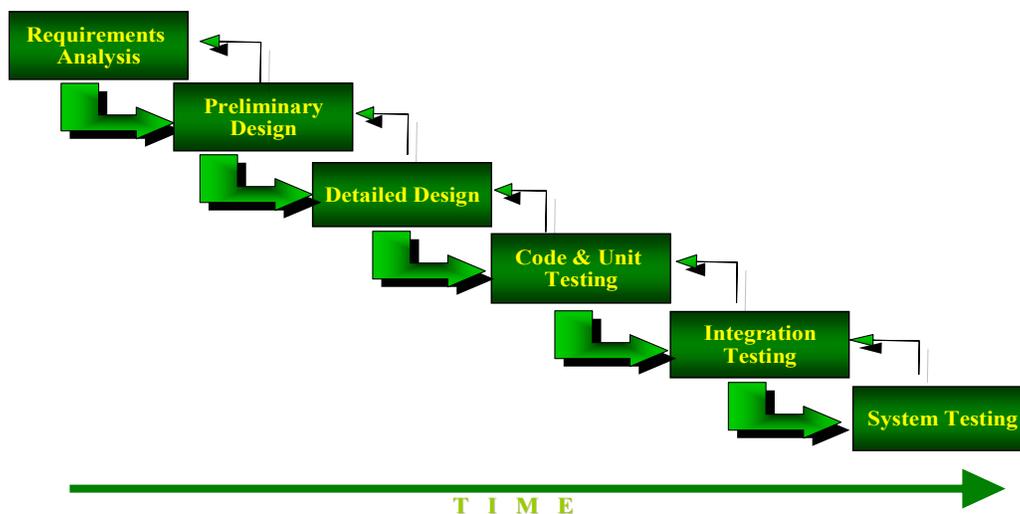
We did not identify any laws or regulations specifically requiring an SDLC methodology. We also did not develop specific audit procedures to detect illegal acts because we did not consider illegal acts to be significant to the audit objective. However, throughout our audit, we were sensitive to the potential of illegal acts, including fraud, waste, abuse, and mismanagement.

WATERFALL AND ITERATIVE SYSTEM DEVELOPMENT MODELS

Waterfall Model

The traditional model for system development -- the linear sequential or “waterfall” model -- provides for clearly defined process phases. Each phase of development will proceed in order, with limited, if any, overlap or iterative steps. Generally, each phase must be completed and approved before the next phase can commence. Figure 2 provides an example of the waterfall approach.

Figure 2: Waterfall Model of System Development



Source: University of Calgary Software Engineering Research Network.

The waterfall model has been found to work well for projects for which requirements are well understood and fixed early on, such as projects involving changes to existing systems. The disadvantage of a waterfall model is that it does not allow for much revision. Once an application is in the testing stage, it is difficult to go back and change what was not known or well thought out in the concept stage.

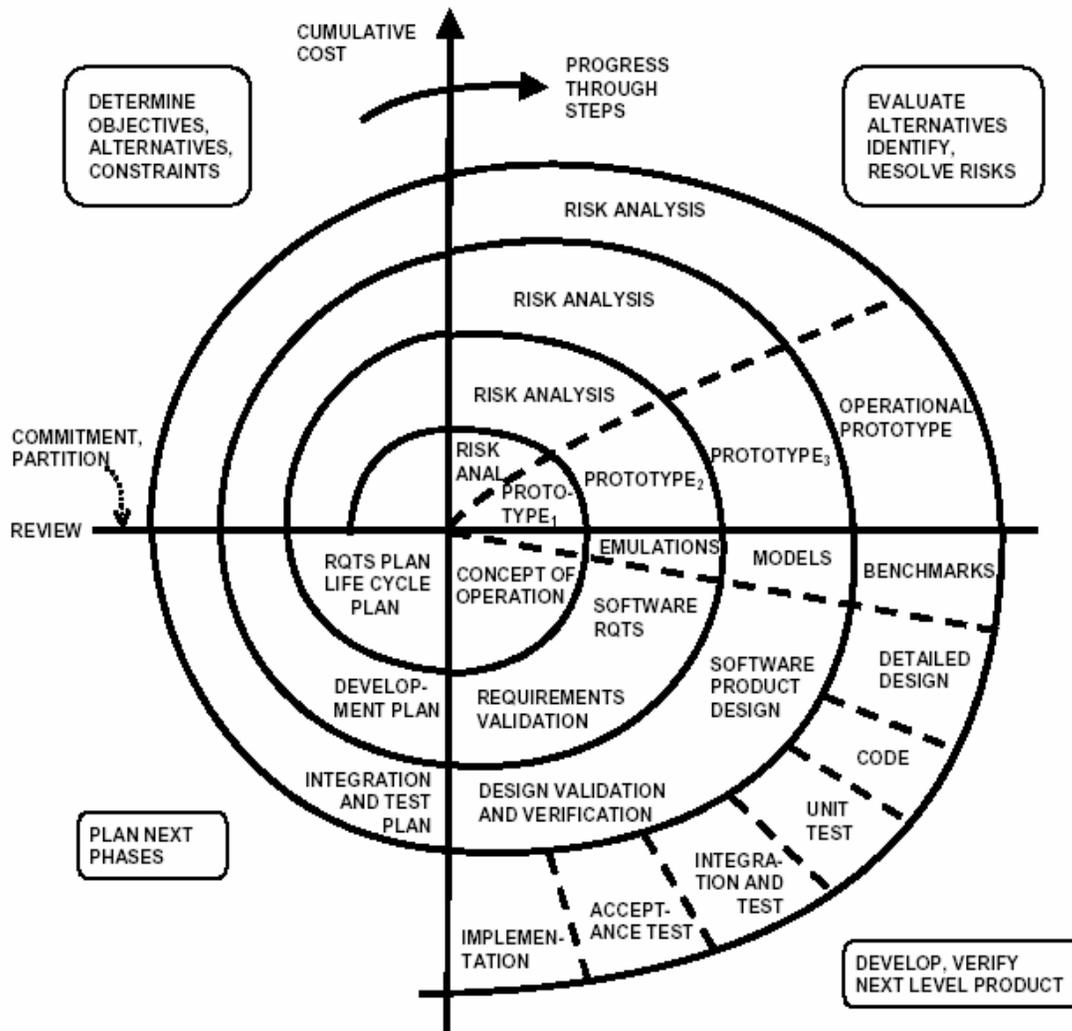
Iterative Development Models

Iterative development is an approach to building software in which the overall project life cycle is composed of several sequential iterations. Each iteration is a self-contained mini-project composed of activities such as requirements analysis, design, programming, and test. The final iteration release is the planned product released to the client.

The advantage of using iterative development is that the end user is continually involved throughout the development process, making it possible to make changes easily and identify and solve problems at each stage of development. These models work best when not all project requirements are known in detail ahead of time. However, problems may be encountered in integrating the many iterative releases.

Figure 3 below represents one phase of a project developed using the spiral iterative model. As noted in the figure, the spiral model provides a *cyclic* approach for incrementally increasing a system's degree of definition and implementation while decreasing its degree of risk.

Figure 3: Spiral Software Development Life Cycle



Source: Understanding the Spiral Model as a Tool for Evolutionary Acquisition by Barry Boehm and Wilfred J. Hansen, January 2001

The GAO has recognized the FAA's³⁵ spiral development approach. The GAO noted that although the use of this approach can increase costs initially, money can be saved in the long run by avoiding costly mistakes after system development. The GAO concluded that this approach has helped the FAA improve its management of systems acquisitions and avoid costly late-stage changes by providing for mid-course corrections.

Considerations for the Acquisition of COTS Software

The SEI has noted that the use of COTS products as elements of larger systems is becoming increasingly commonplace. Shrinking budgets, accelerating rates of COTS enhancement, and expanding system requirements are all driving this process. Also, GAO best practice guidance³⁶ notes that the advantages of using COTS software include (1) a less costly development in comparison to developing in-house applications, (2) software upgrades that are affordable and regularly available, and (3) a design that includes best practices.

However, the use of COTS software also includes risks that require an iterative approach to system development. Through its COTS-Based Systems (CBS) Initiative, the SEI changes the focus of software engineering from one of traditional system specification and construction to one requiring consideration of and balance between:

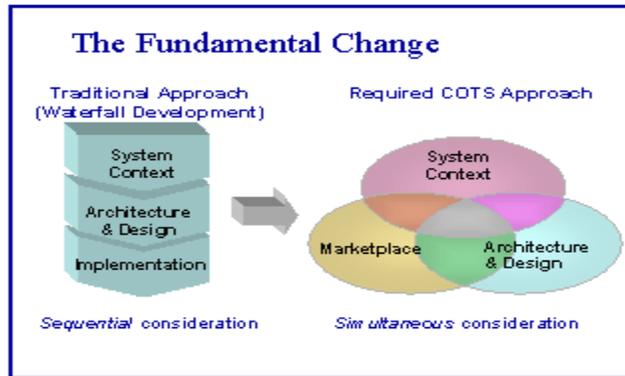
- *system context* (stakeholder and business process requirements and project management aspects such as cost, schedule, and risk considerations);
- *marketplace* (available and emerging COTS technology and products and relevant standards); and
- *architecture and design* (the essential elements of the system and the relationships between them).

Figure 4 provides a summary of the CBS approach.

³⁵ GAO testimony, *Air Traffic Control, FAA's Modernization Efforts – Past, Present and Future*, GAO 04-227T, dated October 30, 2003.

³⁶ GAO Executive Guide, *Creating Value Through World-class Financial Management*, GAO/AIMD-00-134, dated April 2000.

Figure 4: COTS-Based Systems Approach



Source: The SEI COTS-Based Systems Initiative.

The SEI noted that numerous projects have unsuccessfully tried to integrate COTS software using the more traditional approach of defining the requirements, formulating an architecture to meet those requirements, and then trying to fit components into that architecture. The SEI, therefore, recommends the use of a risk-based spiral, or iterative, system development approach to building, fielding, and supporting COTS-based systems.

**FEDERAL AGENCIES AND INDUSTRY ENTITIES THAT PROVIDED
INFORMATION ON SDLC METHODOLOGY AND BEST PRACTICES**

Federal Agencies

Department of Justice

Department of Labor

Department of the Treasury's Financial Management Services

Federal Reserve Board

Federal Aviation Administration

General Accounting Office

Industry

Carnegie Mellon's Software Engineering Institute

Deloitte & Touche/ Deloitte Consulting

Forrester Group

International Business Machines

PricewaterhouseCoopers

Queen's University of Computing

Rational Software Management

Software Productivity Research, LLC

University of Calgary

PROJECT MANAGEMENT GUIDANCE

The Project Management Institute (PMI) has conducted extensive research and analysis in the field of project management and published a standards guide in 2000 entitled *A Guide to the Project Management Body of Knowledge* (PMBOK® Guide). The PMBOK® Guide documents proven practices, tools, and techniques that have become generally accepted in the field of project management, including information systems development and implementation. The PMBOK® Guide is an approved standard of the American National Standards Institute and the Institute of Electrical and Electronics Engineers. The PMBOK® Guide identifies nine distinct knowledge areas associated with successful project management. The nine areas are integration, scope, time, cost, quality, human resources, communication, risk, and procurement management.

- **Integration Management:** The processes that ensure various elements of a project are properly coordinated. Integration management consists of project plan development and execution and integrated change control.
- **Scope Management:** The processes that ensure a project includes all of the work required, and only the work required, to complete the project successfully. Scope management consists of initiation and scope planning, definition, verification, and change control.
- **Time Management:** The processes that ensure timely completion of a project. Time management consists of activity definition, sequencing, and duration estimating as well as schedule development and schedule control.
- **Cost Management:** The processes that ensure a project is completed within the approved budget. Cost management consists of resource planning and cost estimating, cost budgeting, and cost control.
- **Quality Management:** The processes that ensure a project will satisfy the needs for which it was undertaken. Quality management consists of quality planning, assurance, and control.
- **Human Resource Management:** The processes that make the most effective use of the people involved with a project. Human resource management consists of organizational planning, staff acquisition, and team development.
- **Communications Management:** The processes that ensure timely and appropriate generation, collection, dissemination, storage, and ultimate disposition of project information. Communications management consists of communications planning, information distribution, performance reporting, and administrative closure.
- **Risk Management:** The processes concerned with identifying, analyzing, and responding to project risk. Risk management consists of risk management planning, risk identification, qualitative and quantitative risk analysis, risk response planning, and risk monitoring and control.
- **Procurement Management:** The processes related to acquiring goods and services from outside the organization. Procurement management consists of procurement and solicitation planning, solicitation, source selection, contract administration, and contract closeout.

USEFUL BUSINESS MEASURES OF SYSTEM DEVELOPMENT PERFORMANCE

In the report, *Measuring Performance and Demonstrating Results of Information Technology Investments*, AIMD-98-89, dated March 1998, GAO identified these useful information technology internal business measures of system development performance:

Applications development and maintenance:

- Number of function points³⁷ delivered per labor hour
- Number of defects per 100 function points at user acceptance
- Number of critical defects per 100 function points in production
- Percentage of decrease in application software failures and problems
- Mean time to resolve critical defects
- Cycle time for development

Project performance:

- Percentage of projects on time and on budget
- Percentage of projects meeting functionality requirements
- Percentage of projects using standard methodology for systems analysis and design

Infrastructure availability:

- Percentage of computer availability
- Percentage of communications availability
- Percentage of applications availability
- On-line system availability

Enterprise architecture standards compliance:

- Number of variations from standards detected by review and audit per year
- Percentage of increase in systems using architecture
- Percentage of staff trained in relevant standards

³⁷ Function point analysis was first published by International Business Machines in 1979. It is a metric for the purpose of an economic and productivity analysis that uses weighted counts of five parameters: inputs, outputs, inquiries, logical files, and interfaces.

CORPORATION COMMENTS



Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500

Division of Information Resources Management

April 27, 2004

MEMORANDUM TO: Stephen M. Beard
Deputy Assistant Inspector General for Audits
Office of Inspector General

FROM: Michael E. Bartell *MB*
Chief Information Officer and
Director, Division of Information Resources Management

SUBJECT: Draft Report Entitled *Enhancements to the FDIC System
Development Life Cycle Methodology*
(Assignment No. 2004-01)

Thank you for your follow-up to the Division of Information Resources Management's (DIRM) request for assistance in assessing practical updates and enhancements to the FDIC's system development life cycle (SDLC). Your report contains four recommendations and acknowledges that DIRM has begun the process to define a series of improved software development practices and methodologies. The report requests DIRM's concurrence, partial concurrence, or non-concurrence for each recommendation.

As a member of the Transformation Advisory Group and observer for the CIO Council, the Office of Inspector General (OIG) is fully aware of DIRM's effort to implement many of the recommendations provided in the Information Technology Program Assessment that was completed in December 2003 with the assistance of Deloitte Consulting Group. These strategic and programmatic improvements are being coordinated and implemented within a comprehensive Transformation program. The initiatives include adoption of improved practices in systems engineering, project management, capital investment planning, enterprise architecture (EA), and security planning. Your report touched on elements within all of these disciplines, as did your final recommendations. While DIRM has no significant disagreement with the report's content and recommendations, we are currently addressing the issues in a highly-integrated and in-depth manner through our Transformation program. Transformation activities began this year, and will continue over a period of several years. However, significant progress and visible results are to be expected by the end of 2005 in all of the areas highlighted in your report, and we request that the OIG use that date as the expected completion date for our planned actions. The Transformation plan includes key milestones for the many dimensions of the effort. It is through the Transformation plan that we will report our actions to the Office of Enterprise Risk Management addressing your recommendations. Doing so will minimize DIRM's tracking of the actions in multiple reports that are prepared for various purposes.

CORPORATION COMMENTS

Over the past six months, DIRM requested assistance from several parties, including the OIG, and conducted its own research on issues related to managing systems engineering efforts. DIRM has been examining the types of systems development efforts the FDIC is most likely to require in the future, the current systems engineering methodologies that will best support those types of projects, and conditions under which the methodologies should be adapted due to system complexity or risk. We believe this approach is consistent with your suggestion to implement a risk-based SDLC strategy. DIRM is engaging contractual support to develop plans to establish the details of an improved software development methodology along with plans to ensure careful integration with FDIC's overall systems architecture and management control environment.

Recommendation 1 – Integrating project management activities with the SDLC process.

Your recommendations call for adoption and integration of the standards published by the Project Management Institute (PMI). As you are aware, the Transformation program includes the establishment of an Enterprise Program Management Office (PMO) which will standardize project management processes across all information technology projects. This will include improved procedures for project initiation, project planning, project execution and control, and project closeout. In addition, the newly established CIO Council will play a key role in establishing and enforcing sound project management principles and practices. DIRM draws a distinction between an updated SDLC and a project management methodology such as that established by PMI. While the processes and goals of each are closely intertwined, they do represent separate technical disciplines. It is our intent to implement processes that are well-coordinated and fully supportive of one another.

Recommendation 2 – Incorporating results of performance assessment practices into the development process.

Once established, the PMO, as part of its responsibilities for establishing DIRM-wide project policies and standards, will periodically review the results from DIRM's performance assessment activities (such as quality assurance testing and post implementation reviews) for identified best practices and lessons learned to ensure that they are incorporated into future project/development processes.

Recommendation 3 – Aligning systems development with the EA.

I know that you are also aware of the FDIC's efforts to build and support a strong EA program. This work will be further supported by a number of Transformation initiatives that provide the necessary expertise and resources to define, document and implement comprehensive and cohesive enterprise architecture. The Corporation's EA program will assist in supporting decision-making bodies such as the CIO Council, the Capital Investment Review Committee and other executive bodies in determining what new systems projects to undertake and how they will align with new or existing architectures. The PMO will be one of many additional control points to ensure that the Corporation's EA is understood and applied to projects.

CORPORATION COMMENTS

Recommendation 4 – Incorporate NIST guidance for certification and accreditation of security requirements.

Finally, the report recommends that DIRM incorporate NIST guidance for certification and accreditation of security requirements for systems. FDIC guidelines for applying these new standards are in place and briefings with business managers and project teams are underway to discuss the new processes and evaluate impact on project plans. NIST's Federal guidelines are still evolving; therefore our internal procedural documents will also have to evolve to address changes or enhancements. Several major systems initiatives have applied the new requirements and are in the process of being certified and accredited according to specifications.

In conclusion, DIRM generally agrees with all of the recommendations and had incorporated these issues into our Transformation efforts. Therefore, we will not be tracking these recommendations as a response to this audit report, but rather continue to address and monitor these issues as a part of the overall Transformation effort.

cc: Michael MacDermott, OERM
Vijay Deshpande, DIRM
Jerry Russomano, DIRM
Steve Anderson, DIRM
Martha Adams, DIRM
Ned Goldberg, DIRM
Gail Verley, DIRM
Rack Campbell, DIRM

MANAGEMENT RESPONSES TO RECOMMENDATIONS

This table presents the management responses that have been made on recommendations in our report and the status of recommendations as of the date of report issuance. The information in this table is based on management’s written response to our report.

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved: ^a Yes or No	Dispositioned: ^b Yes or No	Open or Closed ^c
1	DIRM will establish an Enterprise Program Management Office (PMO), which will standardize project management processes across all information technology projects. This will include improved procedures for project initiation, project planning, project execution and control, and project closeout.	December 31, 2005	N/A	Yes	No	Open
2	The DIRM PMO will periodically review the results from performance assessment activities (such as quality assurance testing and post-implementation reviews) to ensure that best practices and lessons learned are incorporated into future project/development processes.	December 31, 2005	N/A	Yes	No	Open
3	The Corporation’s EA program will assist in supporting decision-making bodies in determining which new system projects will be undertaken and their alignment with new or existing architectures. The PMO will be one of many additional control points to ensure that the Corporation’s EA is understood and applied to projects.	December 31, 2005	N/A	Yes	No	Open
4	FDIC guidelines for applying NIST C&A new standards are in place, and briefings are underway to discuss the new processes and evaluate impact on project plans. Internal procedures will evolve to address future changes in the NIST guidelines.	December 31, 2005	N/A	Yes	No	Open

^a Resolved – (1) Management concurs with the recommendation and the planned corrective action is consistent with the recommendation. (2) Management does not concur with the recommendation but planned alternative action is acceptable to the OIG. (3) Management agrees to the OIG monetary benefits or a different amount, or no (\$0) amount. Monetary benefits are considered resolved as long as management provides an amount.

^b Dispositioned – The agreed-upon corrective action must be implemented, determined to be effective, and the actual amounts of monetary benefits achieved through implementation identified. The OIG is responsible for determining whether the documentation provided by management is adequate to disposition the recommendation.

^c Once the OIG dispositions the recommendation, it can then be closed.