Office of Inspector General

September 23, 2004
Report No. 04-039

FDIC's Capital Investment Management Review Process for Information Technology Investments

EVALUATION REPORT

FDIC
Federal Deposit Insurance Corporation
801 17th St. NW Washington D.C. 20434

Office of Audits
Office of Inspector General

DATE: September 23, 2004

MEMORANDUM TO: Steven O. App
Deputy to the Chairman and
Chief Financial Officer

Michael E. Bartell
Chief Information Officer and
Director, Division of Information Resources Management

[Electronically produced version; original signed by Stephen M. Beard for Russell A. Rau],

FROM: Russell A. Rau
Assistant Inspector General for Audits

SUBJECT: *FDIC's Capital Investment Management Review Process for Information Technology Investments*
(Report No. 04-039)

The subject final report is provided for your use and comment. Please refer to the Executive Summary section for the overall results. Our evaluation of your response is incorporated into the body of the report, and your response is included, in its entirety, as an appendix to the report. Management's proposed actions for addressing nine recommendations are responsive, and those recommendations are resolved but will remain undispositioned and open for reporting purposes until we have determined that agreed-to corrective actions have been completed and are effective. Management did not concur with recommendations 4 and 6.

For recommendation 4, we remain convinced that management should clarify, in the updated *FDIC Capital Investment Policy* on June 30, 2005, the requirements for the independent validation of quarterly project assessments. Doing so would serve to strengthen existing policy and project monitoring. Accordingly, this recommendation will remain unresolved, undispositioned, and open. We request that management reconsider its position and provide additional written comments within 15 days. For recommendation 6, we agree that further action is not required. This recommendation is considered resolved, dispositioned, and closed for reporting purposes.

If you have any questions concerning the report, please contact Stephen M. Beard, Deputy Assistant Inspector General for Audits, at (202) 416-4217, or Marshall Gentry, Director, Corporate Evaluations, Office of Audits, at (202) 416-2919. We appreciate the courtesies extended to the audit staff.

cc: James H. Angel, Jr., OERM

Table of Contents

Executive Summary

WHY WE DID THIS EVALUATION

Recognizing that a strong investment management program is critical to the attainment of the Corporation's business goals, the Federal Deposit Insurance Corporation (FDIC) created the Capital Investment Review Committee (CIRC) in September 2002. The goal of establishing the CIRC was to create a more structured and disciplined process for managing capital investments than had previously existed at the FDIC. The intent of this evaluation was to assess the FDIC's progress in accomplishing this goal.

EVALUATION OBJECTIVE AND APPROACH

Specifically, the objective of this evaluation was to determine whether the FDIC's CIRC is implementing an efficient and effective review process that supports budgeting for the FDIC's information technology (IT) capital investments and ensures the regular monitoring and proper management of these investments once they are funded. The FDIC defines capital investments as initiatives that have a total capital outlay in excess of $3 million and may generally yield a return on investment (ROI) or increase functionality for the Corporation. Additionally, a project meeting one of the following criteria may be included in the CIRC portfolio:

- has significant multiple-division impact,
- is mandated by legislation or executive order,
- was identified by the Chairman as critical,
- requires a consistent infrastructure investment,
- is a corporate strategic or mandatory-use system, and
- significantly differs from or affects the corporate infrastructure, architecture, or standards guidelines.

We used the U.S. Government Accountability Office (GAO)[1] IT Investment Management (ITIM) Maturity Framework as the basis for evaluating the steps taken by the FDIC from September 2002 through June 2004 to establish its capital planning and investment management (CPIM) process.[2] GAO's ITIM model identifies and organizes processes critical for successful IT investment into a framework of five increasing stages of maturity. Specifically, we reviewed the FDIC's progress in establishing an investment management structure for capital investments relative to the following stages in GAO's ITIM model:

- **Stage 2 - Building the Investment Foundation**, which involves developing the capability to control projects and establishing basic capabilities for selecting new IT projects.

[1] The name of the General Accounting Office changed to the Government Accountability Office, effective July 7, 2004.
[2] *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, Version 1.1 (Report No. GAO-04-394G, dated March 2004).

- **Stage 3 - Developing a Complete Investment Portfolio**, which involves a continual assessment of proposed and ongoing projects as part of a complete investment portfolio – an integrated and competing set of investment options.

We recognize that the FDIC may be implementing key practices associated with higher maturity stages. Indeed, GAO's framework discusses the fact that an organization may be concurrently implementing key practices that are associated with several maturity stages.

We evaluated the FDIC IT CPIM process in place as of June 30, 2004. Our evaluation did not include assessing the FDIC's investment management process for non-CIRC projects other than to gain a basic understanding of the process. Furthermore, we also obtained a basic understanding of the FDIC's enterprise architecture (EA) program as part of our work.[3]

Appendix I describes our objective, scope, and methodology in detail.

WHAT WE FOUND

Measuring the overall effectiveness of the CIRC was difficult because of its relatively short history. Nevertheless, the establishment of the CIRC in September 2002 and the Capital Investment Budget in December 2002 were significant steps toward creating a more disciplined and effective planning and management process than previously existed. Since 2002, the FDIC's efforts have encompassed a broad range of activities, including ongoing work to develop:

- an IT governance structure, including the establishment of the Chief Information Officer (CIO) Council in February 2004;
- a systematic, quarterly management oversight process for capital investment projects;
- corporate tools and guidance for project managers; and
- a portfolio perspective of IT capital investments.[4]

These activities align with the processes associated with the second and third stages of maturity in GAO's five-tiered model. Specifically, the FDIC's program has evolved from an ad hoc, unstructured, and unpredictable investment process associated with the lowest level of maturity in GAO's ITIM model. However, work remains to achieve a mature, repeatable process. Table 1 identifies some of the key accomplishments and actions needed for continued progress.

[3] An EA is an institutional systems blueprint that defines, in 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 environments.
[4] A portfolio perspective enables an organization to consider investments in a comprehensive manner, so that investments address not only the strategic goals, objectives, and mission of the organization, but also the impact that projects have on one another.

Table 1: OIG Assessment of the FDIC's Efforts Through June 30, 2004

Critical Process	Key Program Accomplishments	Key Actions Needed to Sustain Progress
Instituting the Investment Board	• Establishment of the IT-governance structure, including CIRC, CIO Council, and other supporting committees. • Continued senior-level executive commitment to the process.	• Institutionalizing the role of the IT-related committees, in particular, the role of the CIO Council relative to the CIRC.
Meeting the Business Needs	• Issued the *FDIC Capital Investment Policy*, which requires executive sponsors to link IT investments to business needs. • Developed a standard business case template. • Issued the *IT Strategic Plan*.	• Institutionalizing the use of the *IT Strategic Plan* as a tool for ensuring that all IT investments align with corporate mission and goals.
Selecting an Investment	• Established project selection criteria in the CIRC charter. • Established the Financial Analysis Committee and EA committee review processes. • Issued *Re-baselining Capital Investment Policy*.	• Developing guidance for periodically evaluating and updating project selection criteria.
Providing Investment Oversight	• Established the *Quarterly IT Project Assessment Reports* for CIRC projects in the planning and development phases.	• Establishing additional procedures to strengthen investment oversight. • Documenting the CIO Council's process for overseeing capital investment projects in the steady state phase.[5]
Capturing Investment Information	• Launched CIRC and EA Websites and developing a CIO Council Website. • Developing a repository of key CIRC project data on FDIC's Digital Library. • Starting development of an EA repository.	• Developing guidance to document specific capital investment-related information, including information about steady state investments, that should be captured and maintained, where it should be stored, the organization responsible for updating the information, and how often it should be updated.

(Table 1 continued on next page.)

[5] Phases of the system development life cycle (SDLC) include a planning phase, requirements definition phase, design phase, development phase, test phase, implementation phase, and maintenance and operation phase (i.e., steady state phase).

Table 1: OIG Assessment of the FDIC's Efforts Through June 30, 2004 (cont'd)

Critical Process	Key Program Accomplishments	Key Actions Needed to Sustain Progress
Defining the Portfolio Criteria	• Establishment of the CIO Council. • Starting development of an EA repository and ongoing Application Rationalization Project.	• Establishing guidance for periodically evaluating and updating capital investment portfolio selection criteria.
Creating the Portfolio	• Established the CIRC portfolio for planning and development projects. • Established an investment budget.	• Institutionalizing the role of the CIO Council and using the *IT Strategic Plan* and EA to ensure IT investment decisions are consistent with enterprise-wide priorities.
Evaluating the Portfolio	• Developed the quarterly *Capital Investment Report* for the Board of Directors.	• Establishing additional procedures to strengthen evaluation of the portfolio.
Conducting Post-Implementation Reviews (PIRs)	• Planning ongoing for PIRs. • Held a series of meetings to discuss process improvement.	• Completing scheduled PIRs and defining the responsibilities of the CIRC-related committees in the PIR process.

Source: OIG Analysis of FDIC's CPIM process activities.

In evaluating the FDIC's progress, it is important to consider several points:

- GAO's ITIM model does not provide guidance related to the time it should take to establish the critical processes in each maturity stage, and we have reported previously that the establishment of the CPIM process is a multi-year effort.[6]
- The FDIC's CPIM management activities are being undertaken in the midst of a major transformation resulting from the Corporation's recent Information Technology Program Assessment (ITPA), which was aimed at improving Division of Information Resources Management's (DIRM) overall performance.[7] Improving investment management, project management, and implementing a new SDLC methodology are key components of DIRM's multi-year transformation efforts.
- To date, the capital investments monitored by the CIRC have included only projects in the planning or development phases. Thus, PIRs have not yet been conducted on CIRC projects.
- The FDIC's EA program is still evolving, and the ability of the CPIM process to achieve a more mature status is dependent on the FDIC's progress in the EA program area, particularly in regard to critical processes in Stage 3 of GAO's model.

---

[6] *Independent Evaluation of FDIC's Information Security Program – 2003* (OIG Evaluation Report No. 03-040, dated September 17, 2003).

[7] In 2003, DIRM contracted with Deloitte Consulting to conduct a comprehensive review of DIRM's operations. The recommendations from this review are being implemented and include a new organizational structure, along with a variety of fundamental changes in the processes for managing IT. DIRM's transformation Phase I organization structure was implemented on June 13, 2004.

RECOMMENDED COURSE OF ACTION TO MEET FUTURE CHALLENGES

The FDIC has many efforts underway or planned that should result in continued maturation of the CPIM process. Our recommendations addressed strengthening CPIM-related guidance, including guidance related to the FDIC's investment management governance structure. In addition, we are recommending that the FDIC ensure that long-term CPIM program goals are integrated into corporate or DIRM plans to ensure continued focus on IT investment process improvements. Doing so will allow the FDIC to continue to systematically prioritize, sequence, and evaluate improvement efforts. We believe this is particularly important given the broad range of program activity ongoing.

Background

Legislative Overview

Congress has passed several laws that lay the groundwork for agencies to establish an investment approach for managing IT projects.[8] One of the key pieces of legislation is the Clinger-Cohen Act of 1996 (CCA). The CCA requires the establishment of IT investment and capital planning processes and performance management. In addition, the Office of Management and Budget (OMB) has issued executive guidance in this area.

Central Tenets of IT Investment Management

- Development, implementation, and maintenance of an **EA**. An EA is the explicit description and documentation of the current and desired relationships among business and management processes and IT.
- Implementation of a **capital planning and investment control process,** which is a structured means by which the EA is implemented. This is a systematic approach to managing risks and returns of IT investments. Under this process, new and ongoing projects originate from business and mission needs of the Corporation as well as from the sequencing plan for transition from the current to the target architecture.
- To be successful, an IT investment management process should have elements of three essential phases.
  - **Select Phase –** ***how do you know that you have selected the best projects?***
  - **Control Phase –** ***how are you assuring that projects deliver benefits?***
  - **Evaluate Phase –** ***are the systems delivering what you expected?***

Source: GAO and OMB Circular No. A-130, Transmittal Memorandum, No. 4, *Management of Federal Information Resources*, dated November 28, 2000.

The FDIC is not legally bound by all the laws and executive guidance for managing IT investments. However, in recognizing that such laws and guidance constitute best practices, the FDIC's policy position is that the laws and guidance should be adopted either in whole or in part.

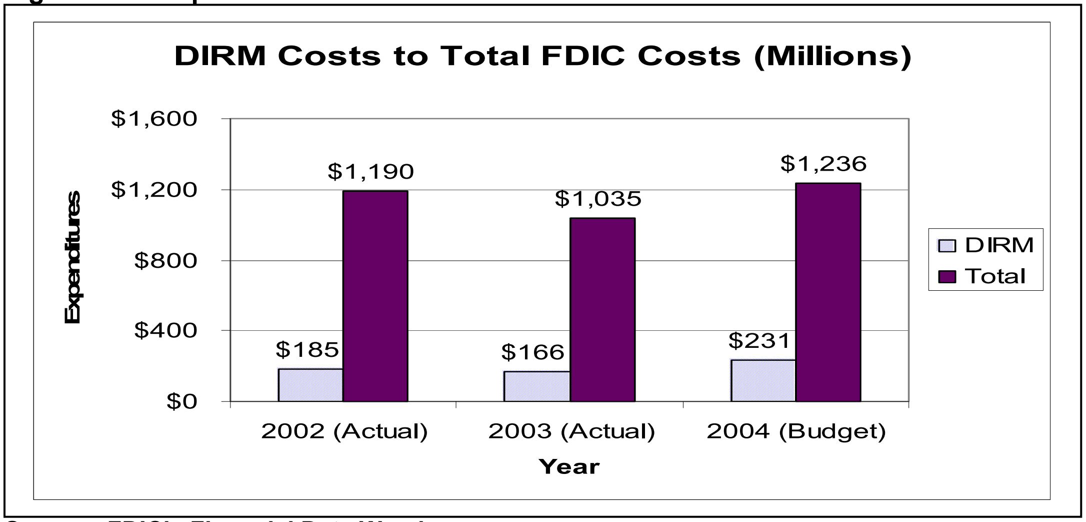
The FDIC's Capital Planning and Investment Management Process

The FDIC invests significant resources in IT each year and recognizes that it needs to ensure that IT dollars are spent in the right places and obtain the best value. A strong investment management program is critical to attainment of the Corporation's business

[8] The following are some of the key laws that put in place various requirements related to IT Investment Management – the Clinger-Cohen Act of 1996 (Pub. L. No. 104-106); the Paperwork Reduction Act of 1995 (Pub. L. No. 96-511); the Federal Acquisition Streamlining Act of 1994 (FASA) (Pub. L. No. 103-355); the Government Performance and Results Act of 1993 (Pub. L. No. 103-62); the Chief Financial Officers Act (CFOA) of 1990 (Pub. L. No. 101-576); and the E-Government Act of 2002 (Pub. L. No. 107-347). Of these statutes, the CCA and FASA are not applicable to the FDIC. Portions of the CFOA apply to the FDIC, but other portions of the CFOA do not, including those related to agency chief financial officers and their roles regarding management systems and inventories. However, these provisions may represent prudent practices for the FDIC.

objectives. Figure 1 illustrates DIRM's budget, which contains the majority of IT-related costs, relative to the FDIC's budget.

Figure 1: Comparison of DIRM Costs to Total FDIC Costs

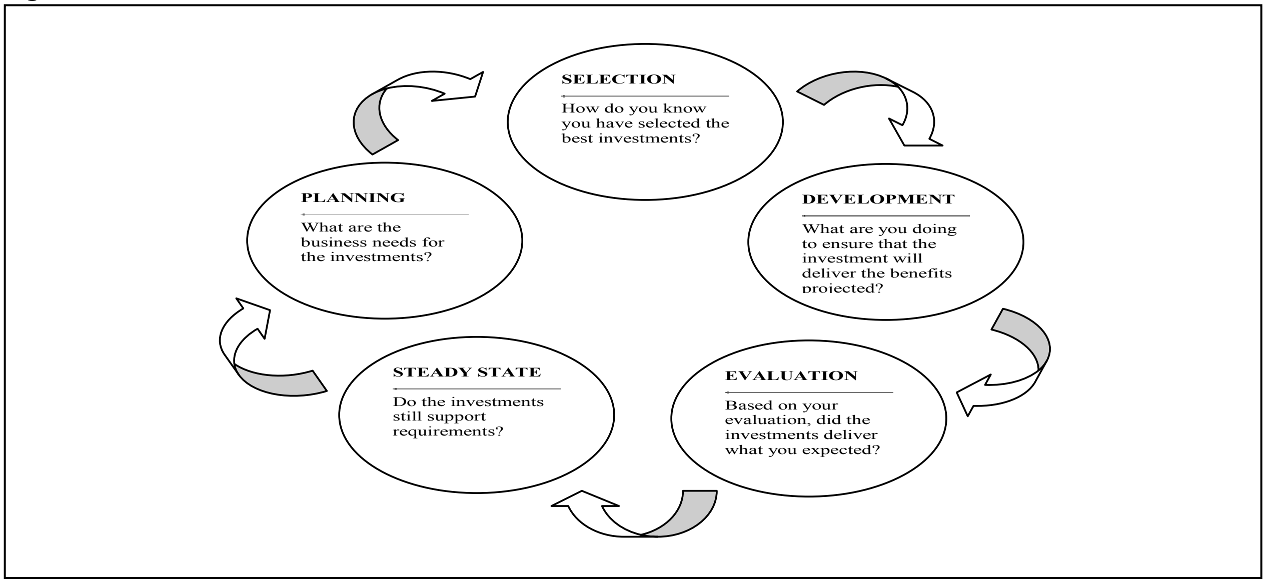


Source: FDIC's Financial Data Warehouse.

To that end, during 2002, the FDIC began to develop an EA in order to establish a corporate-wide roadmap for achieving its mission within an efficient IT environment. The FDIC recognizes that the establishment of the EA will provide a sound foundation to support its CPIM process. When the CIRC was created, the FDIC abolished the IT governance structure that had been established in 1996 which included an IT Council and IT Technical Committee.

The CIRC's role is to determine whether a proposed investment is appropriate for the FDIC's Board of Directors (Board) consideration, oversee approved investments throughout their life cycle, and provide quarterly capital investment reports to the Board. The CPIM is the FDIC's systematic approach to managing the risks and returns of capital investments for a given mission. As Figure 2 depicts, the FDIC's CPIM process expands upon the fundamental select, control, and evaluate phases.

Figure 2: The FDIC's CPIM Process



Source: The FDIC CIRC Website.

Beginning with the 2003 budget, the FDIC began budgeting and tracking capital investment expenses as a separate component of the budget to enhance management's ability to focus on such projects. The investment budget includes planned spending on projects that involve substantial costs (i.e., in excess of $3 million) and are expected to yield significant long-term benefits to the Corporation. Project funds established within the investment budget are to be available for the life of the project rather than for the fiscal year. Final responsibility for approving the initial creation or modification of a project's capital investment budget rests with the FDIC's Board of Directors.

GAO's IT Investment Management Maturity Framework

In 1997, GAO developed guidance, based primarily on the CCA, that provides a method for evaluating and assessing how well a federal agency is selecting and managing its IT resources and identifies specific areas where improvements can be made.[9] The guide expanded upon the select/control/evaluate process model. GAO reports that evaluations of the investment management processes in the private sector and at several federal agencies indicate that IT investment management is a step-by-step process that occurs over time.

In March 2004, GAO issued Version 1.1 of its ITIM maturity framework.[10] This framework enhances GAO's 1997 guidance by identifying critical processes for successful IT investment and organizing these processes into an assessment framework with five stages of maturity. Table 2 provides a brief description of the five maturity stages.

---

[9] *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-Making*, Version 1 (GAO Report No. GAO/AIMD 10.1.13, dated February 1997).
[10] *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* Version 1.1 (GAO Report No. GAO-04-394, dated March 2004). GAO issued an exposure draft of this report in 2000 (GAO Report No. GAO/AIMD-10.1.23 Version I, dated May 2000).

Table 2: The Five Stages of Maturity Within the ITIM Framework

Maturity		Description
Enterprise and strategic focus ↑↑↑↑↑↑↑↑↑↑↑↑ Project-centric	**Stage 5:** **Leveraging IT for strategic outcomes.**	The organization has mastered the selection, control, and evaluation processes and now seeks to shape its strategic outcomes by benchmarking its IT investment processes relative to other "best-in-class" organizations.
	Stage 4: **Improving the investment process.**	The organization is focused on evaluation techniques to improve its IT investment processes and portfolio(s) while maintaining mature selection and control techniques.
	Stage 3: **Developing a complete investment portfolio.**	The organization has developed a well-defined IT investment portfolio, using an investment process that has sound selection criteria and maintains mature, evolving, and integrated selection, control, and evaluation processes.
	Stage 2: **Building the investment foundation.**	Basic selection capabilities are being driven by the development of project selection criteria, including benefit and risk criteria, and an awareness of organizational priorities when identifying projects for funding. Executive oversight is applied on a project-by-project basis.
	Stage 1: **Creating investment awareness.**	Ad hoc, unstructured, and unpredictable investment processes characterize this stage. There is generally little relationship between the success or failure of one project and the success or failure of another project.

Source: GAO.

GAO reports that these maturity stages are cumulative; that is, in order to attain a stage of maturity, an agency must have institutionalized all of the requirements for that stage in addition to those for all of the lower stages. An organization may be concurrently implementing key practices associated with several maturity stages. In fact, key practices associated with upper-stage critical processes are frequently initiated while the organization, as a whole, is at a lower stage of maturity.

Evaluation Results

Building the Investment Foundation for Capital Investments

According to GAO's ITIM model, Stage 2 builds the foundation for current and future IT investment success by establishing basic selection and control processes. Table 3 provides a high-level overview of the critical processes in Stage 2.

Table 3: Stage 2 Maturity – Critical Processes

ITIM Critical Processes
Instituting the Investment Board *Process for creating and defining the membership, guiding policies, operations, roles, responsibilities, and authorities for one or more IT investment boards within an organization.*
Meeting the Business Needs *Process for developing a business case that identifies the key executive sponsor and business customers and the business needs that the IT project will support.*
Selecting an Investment *A defined process that an organization can use to select new IT project proposals and reselect ongoing projects.*
Providing Investment Oversight *Pivotal process whereby the organization monitors projects against cost and schedule expectations as well as anticipated benefits and risk exposure and takes corrective action when expectations are not being met.*
Capturing Investment Information *Process by which specific details about a particular investment are captured and maintained to provide asset-tracking data to executive decision makers.*

Source: GAO.

A detailed analysis of the Corporation's efforts to date and remaining challenges follows.

Corporate Efforts to Date

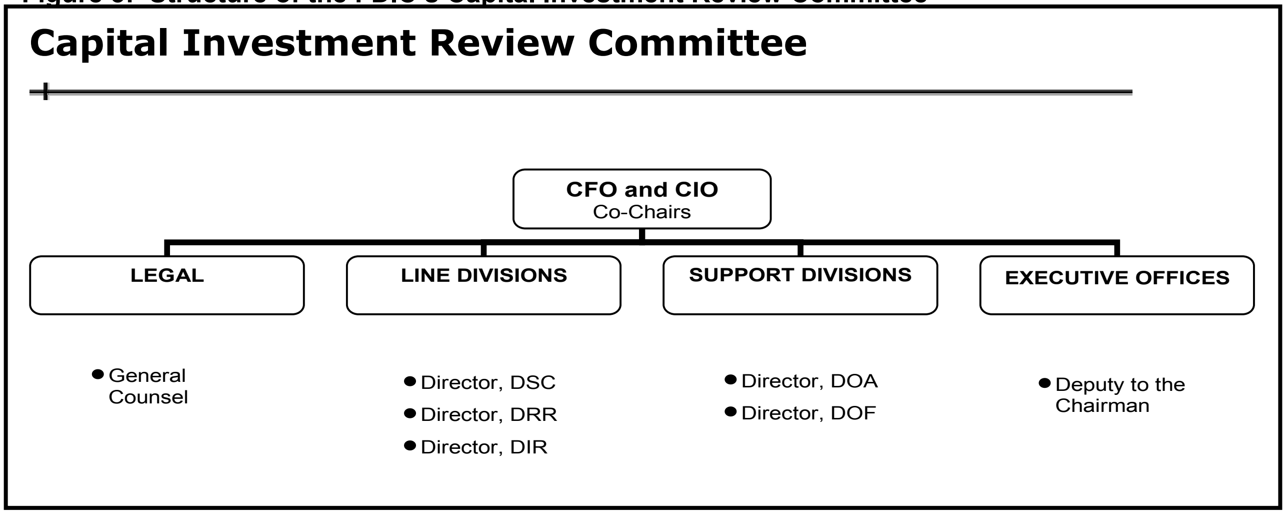
Instituting the Investment Board. In 2002, the FDIC replaced its IT governance structure by instituting the CIRC and supporting CPIM IT governance structure.[11] In February 2004, the FDIC also created a new CIO Council based on the results of the Corporation's recent ITPA. After the CIO Council was established, the FDIC undertook a review of the CIRC's supporting IT governance structure. The role of the CIRC and key support committees, the Financial Analysis Committee (FAC) and Enterprise Architecture Committee (EAC), did not change significantly. As of June 30, 2004, the FDIC had ratified charters for each of the committees under the new governance structure. However, the CIO and Chief Financial Officer (CFO), as CIRC Co-Chairs, need to continue efforts to ensure that the role of each committee, in particular the role of the CIO Council, becomes an institutionalized part of the CPIM process.

According to GAO's ITIM model, the purpose of this critical process is to define and establish an appropriate IT investment management structure and the processes for selecting, controlling, and evaluating IT investments. According to GAO, instituting the IT investment board is a key component in the IT investment management process. Specifically, this critical process defines the membership, guiding policies, operations, roles, responsibilities, and authorities for each designated board and, if appropriate, each board's support staff.

The FDIC CIRC acts as the governing body for all IT capital investment projects (i.e., those over $3 million) and is responsible for developing the CPIM process. For other IT projects, the sponsoring division director governs the project, and the newly established CIO Council will be responsible for oversight of those projects. As Figure 3 illustrates, the CIRC includes the Deputy to the Chairman, the CFO, CIO, and members from the highest levels of FDIC management from each of the FDIC's line divisions – the Division of Supervision and Consumer Protection (DSC), Division of Resolutions and Receiverships (DRR), Division of Insurance and Research (DIR), key corporate support divisions – Division of Administration (DOA) and Division of Finance (DOF), and the Legal Division. The composition of the CIRC represents a significant organizational commitment to the CPIM process. The CIRC meeting minutes indicated that the CIRC met 17 times between September 2002 and June 2004, the meetings were well attended by members, and discussions covered broad CPIM process issues as well as specific project performance.

[11] When the CIRC was created in September 2002, the FDIC disbanded its existing IT Council.

Figure 3: Structure of the FDIC's Capital Investment Review Committee



Source: CIRC Charter.

To support the CIRC, the FDIC established two key committees – the FAC and EAC. The FAC provides analysis and guidance to the CIRC with regard to financial plans and proposals. The EAC reviews all IT investment business cases to evaluate alignment with the EA blueprint. Both committees prepare memoranda to the CIO and CFO that document the results of the committees' respective reviews.

As of June 30, 2004, the FAC has issued seven review memoranda to the CIRC. Committee members told us that the FAC analysis of one case is covered in a series of FAC meetings. The EAC has also issued seven review memoranda to the CIRC. Some cases have not yet been subject to the FAC or EAC review process. In other cases, the project approval predated the establishment of the CIRC.

Both committees include representatives from FDIC divisions and offices, and participation is considered an ancillary duty for the members. DIRM Enterprise Technology is responsible for the EA program and provides support for the EAC such as recording and distributing minutes from EAC meetings. FAC members meet as needed, but the designated committee chairman stated that recording official minutes of the meetings has not been a priority and would require additional resources. Recording the minutes of the FAC deliberation process would be beneficial to establish a corporate repository of policy matter discussions as well as discussions on specific cases. FDIC officials should consider assigning additional resources to do this.

In February 2004, a CIO Council was created to be one of the primary governance mechanisms for IT management. The CIO Council is made up of senior IT-focused executives from each of the FDIC's line divisions. The Council is responsible for advising the CIO in developing an enterprise perspective on corporate systems and assisting in the development of an overall IT strategic plan and reviewing IT initiatives, projects, priorities, and resources. According to the *IT Strategic Plan,* the CIO Council is responsible for setting the strategic direction for IT, and in concert with the CIRC, is responsible for reviewing and recommending IT investments to be made by the Corporation. The *FDIC Capital Investment Policy* issued in June 2004 does not define the CIO Council's responsibilities. The policy should be updated to help ensure that the CIO Council's role relative to the CIRC is clear.

When the CIO Council was established, the Council initiated a review of the FDIC's IT–related committee structure, resulting in revisions to the existing EAC and FAC charters and the creation of the Technical Review Group (TRG). The charters for all the committees were ratified as of June 30, 2004. Table 4 provides an overview of the purpose and responsibility of each committee.

Table 4: Overview of IT-Related Capital Investment Committees

Committee	Purpose/Responsibility
CIRC	Provides systematic management review processes to support budgeting for FDIC's capital investments and ensures ongoing monitoring of the investments once funded.
CIO Council	Provides a leadership forum and governance structure for discussing issues across organizational boundaries of mutual interest.
EAC	Provides the leadership necessary to ensure that the appropriate data, applications, and technical infrastructure components are defined, documented, and implemented to support the strategic business objectives of the corporation.
FAC	Provides analysis and guidance to the FDIC CIRC with regard to financial plans, proposals, and ongoing operations for projects to be considered by the CIRC.
Corporate Data Sharing Steering Committee (CDSSC)	Provides the executive sponsorship and leadership necessary to facilitate positive changes in the FDIC's culture to ensure that both structured data (databases) and unstructured data (electronic documents) are viewed and managed as corporate assets that are not owned by any single division or office.
TRG	Provides the FDIC with an enterprise approach to evaluating IT solutions so that the scope of technology includes the needs and requirements of the entire Corporation and provides sound technical recommendations to the CIO.

Source: Committee Charters.

In addition to these changes, DIRM is establishing an Enterprise Program Management Office (PMO) to provide improved guidance for oversight of IT initiatives, including application development efforts, throughout the FDIC. The goals of the PMO are to ensure increased focus on operational innovation, effectiveness, and process improvement and to establish project management standards, processes, and guidelines.

Meeting the Business Needs. The CPIM process is considered to be an integral part of the Corporation's strategic and capital planning process. The *FDIC Capital Investment Policy* requires that each IT capital investment have an executive sponsor who is responsible for establishing a link between the recommended investment and the FDIC's strategic goals and objectives. This link is documented in the business case that is subject to review by the CIRC and supporting committees. Additionally, the *IT Strategic Plan* is intended to provide another tool for ensuring the IT investments align with the FDIC's business needs.

The purpose of this critical process, i.e., *Meeting the Business Needs*, is to ensure that IT projects and systems support the organization's business needs and meet users' needs. This critical process establishes a mechanism for verifying that the business case drives continued support for each IT system and for ensuring that an essential link exists between the organization's business objectives and its IT strategy. The process also helps to ensure that a defined partnership exists between the sponsoring unit and the IT solution. IT projects and systems should be tightly aligned with the business needs of the organization, providing support for highly visible core business processes.

Consistent with the *FDIC Capital Investment Policy*, executive sponsors have been identified for each of the capital investment projects. In addition, the sponsoring division or office is required to establish an Executive Steering Committee (ESC) for each project. The ESCs are responsible for reviewing and approving project requirements and plans and for providing guidance to the project manager as needed. The ESC should consist of senior managers from the project's stakeholder divisions or offices that possess specific knowledge critical to the success of the project. The size and composition of the ESC should be consistent with the project's overall scope and complexity.

Further, CPIM procedures require the project team to develop a project proposal (i.e., business case) that documents the business needs of the project. Among other things, the business case must demonstrate financial soundness and alignment with the EA. As discussed later in the report, during 2003, the CIRC, through the FAC, created a standardized business case template. The SDLC process is also designed to help ensure that an IT investment project meets users' needs. Specifically, the *FDIC SDLC Manual* advises that participation by system users and all levels of FDIC management across all involved functional areas is essential to the implementation of effective information systems.[12] The manual indicates the DIRM project manager, the divisional program manager, and the user community should work together to define the system requirements.

Additionally, the FDIC's *2001-2006 Strategic Plan* and *2004 Annual Performance Plan* provide a framework to guide FDIC IT operations. Finally, the CIO Council issued the *IT Strategic Plan* in August 2004. The CIO stated that the *IT Strategic Plan* lays out a strategy to improve FDIC operations by better using technology, in concert with people, processes, and information. This plan should strengthen the CPIM process by providing a tool for ensuring investments align with business needs and strategies.

Selecting an Investment. The FDIC established selection criteria for capital investments when the CIRC was created, as part of the CIRC charter. The CIRC is to use these criteria to review project business cases and quarterly performance data and to evaluate how projects align with the criteria. In 2004, the CIRC also issued its *Re-baselining Capital Investment Projects* policy, which outlines the justification for re-baselining projects that are not meeting performance requirements in the development phase.

The purpose of this critical process is to ensure that a well-defined and disciplined process is used to select new IT proposals and re-select ongoing investments. Defining and implementing a selection process is a basic step toward implementing the mature IT critical processes for proposal and project selection in Stage 3. According to GAO, an agency's EA should be reflected in the selection criteria. Investments not consistent with the current EA should be either assimilated into the EA or provided a waiver. Re-

[12] *FDIC SDLC Manual* Version 3.0, dated July 1997. The FDIC is implementing a new SDLC methodology. The FDIC will be implementing the Rational Unified Process ® (RUP) methodology. 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.

selection of ongoing projects is an important part of this critical process. If a project is not meeting the goals and objectives established in the original selection, the investment board must make a decision on whether to continue to fund it. Additionally, GAO states that an organization should create a process for ensuring that the criteria change as the organizational objectives change.

The CIRC charter defines nine broad criteria to use to select proposed projects. This information is published and has been posted on the CIRC Website since April 2003. However, the FDIC has not established a procedure to periodically review and update the selection criteria. The criteria are fundamentally aligned with IT investment principles included in OMB guidance. Additionally, the CIRC charter states that the CIRC will consider IT projects only if they have received prior approval from the EAC. To document its review, the EAC prepares a memorandum to the CIRC, stating whether the proposal recommends solutions that are in alignment with the FDIC's EA. FDIC Circular 1303.1, *FDIC Enterprise Architecture Program,* states that consistency with the EA shall be one of the decision criteria for funding IT investments.

CIRC Selection Criteria

Investments proposed for funding should:

- Align with the FDIC's strategic vision, mission, and business requirements.
- Be undertaken by the FDIC because no alternative private sector or governmental product, service, and/or source can efficiently support the function.
- Consider off-the-shelf software for all new IT applications.
- Support work processes that have been re-engineered to reduce costs, improve effectiveness, and/or make maximum use of commercial, off-the-shelf technology.
- Demonstrate a projected ROI that is clearly equal to, or better than, alternative uses of available resources.
- Reduce the risk by establishing clear measures and accountability for project progress and by securing substantial involvement and buy-in throughout the project.
- Employ an acquisition strategy that appropriately allocates risk between government and contractor, effectively uses competition, ties contract payments to accomplishments, and takes maximum advantage of commercial technology.
- Ensure that improvements to existing information systems and the development of planned information systems do not unnecessarily duplicate IT capabilities within the FDIC, from other financial regulatory agencies, or from the private sector.
- Integrate information and physical security, ensuring that controls are adequate to mitigate risks to the Corporation.

Source: CIRC Charter.

As noted previously, the CPIM procedures require the project team to prepare a business case for each project. The FDIC's standard business case template is generally consistent with OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, *Exhibit 300*, which is the government equivalent of a business case.[13] The FDIC's business case includes consideration of full life cycle costs, consideration of project alternatives, and security. More specifically, the business case includes the following elements:

[13] *Exhibit 300* is used as part of the federal government's appropriation process, which the FDIC is generally not required to follow. *Exhibit 300* establishes policy for planning, budgeting, acquiring, and managing federal capital assets.

- Financial formulas that calculate ROI and operational benefits.
- Representation of financial data in a common set of tables and charts.
- Standardized cost factors (e.g., salary, outside services, discount to calculate net present value).

As a result of these standardizations, the FDIC expects to achieve the following benefits:

- Review committees can concentrate on the merits of the business case.
- Individual business cases can be compared with one another.
- Business case development teams can produce financial results immediately.

In January 2004, the FDIC adopted a policy entitled, *Re-baselining Capital Investment Projects*. Re-baselining a capital investment project is the process in which the project's original budget, schedule, requirements, functionality, or business case/ROI is materially modified due to some previously unforeseen event(s). The project manager is responsible for developing a business case outlining the need to re-baseline the project. All baseline modifications, including changes to investment expectations and commitments, must be presented to and approved by the CIRC.[14] This process allows for the CIRC and FDIC Board to evaluate or "re-select" ongoing development projects. Since January 2004, the CIRC and FDIC Board have approved re-baselining cases for two projects – DSC's Virtual Supervisory Information on the Net (ViSION) and DOF's New Financial Environment (NFE).

Once the CIRC project reaches the steady state phase, the CIO Council will be responsible for reviewing the ongoing alignment and value of the steady state investment. Officials told us that the CIO Council is reviewing investments as part of the application rationalization project and the FDIC's annual budget process. The application rationalization project is discussed later in the report. According to GAO, periodic evaluation of IT investments permits the investment board to determine the ongoing value of each investment to the organization and its end users. These periodic evaluations are critical to determining whether to continue to fund an IT system.

The *FDIC Capital Investment Policy* issued in June 2004 states that the CIRC is tasked with the establishment of procedures relating to the Corporation's CPIM process. Accordingly, the CIRC needs to establish procedures to periodically review the existing selection criteria.

Providing Investment Oversight. The FDIC has addressed key aspects of this process by establishing an oversight structure and implementing a project assessment process. Specifically, the CIRC's *FDIC Capital Investment Policy* defines the fundamental management structure for project oversight and establishes a quarterly project assessment reporting process for projects in the development and planning phases. However, establishing additional procedures should strengthen the process.

The purpose of this critical process is to ensure that an organization provides effective oversight for its IT projects throughout all phases of their life cycle. GAO reports that each project development team should be responsible for meeting project milestones

[14] If the new projected total investment cost of the project exceeds the existing Board-approved investment budget, the final authority for approving the re-baselining rests with the Board.

within the expected cost parameters that have been established by the project's business case and cost-benefit analysis. However, the investment board should employ early warning systems that enable it to take corrective actions at the first sign of cost, schedule, and performance problems. The investment board must also ensure that projects maintain alignment with the FDIC's EA.

CPIM procedures require a *Project Plan* for all projects to document project scope, tasks, schedule, allocated resources, and interrelations with other projects. The *FDIC Capital Investment Policy* requires that the project ESC review and approve project requirements and plans and provide guidance to the project manager as needed. The *FDIC Capital Investment Policy* also requires project managers to prepare a *Quarterly IT Project Assessment Report* (quarterly report) that compares actual project progress to the project plan.[15] Specifically, capital investment projects are rated in relation to their finances, attainment of critical milestones, and performance. The quarterly reporting process should be integrated with the implementation the new SDLC RUP ® methodology. DIRM's Investment Management Branch (IMB) has developed templates and instructions to improve consistency and quality in the preparation of the quarterly reports for the CIRC.

The *FDIC Capital Investment Policy* also states that the project's executive sponsor and the ESC are responsible for assigning an overall assessment rating based on an evaluation of the project's individual component assessments. DIRM IMB has developed guidance to assist project managers and ESC members in assigning ratings in the quarterly reports to various aspects of project performance as well as to each project as a whole.

The FDIC's Quarterly Project Assessment Report Rating Factors

Finance	The project's performance with respect to its financial plan as originally submitted in its approved business case.
Milestones	The project's overall performance with respect to its original project plan.
Performance	The project's overall scope and management. Addresses questions about the project's functionality, adequacy of resources (financial and human), and risk management.
Overall	The current state of the project as a whole. It should *not* be interpreted as representing an average of the three previous factors (that is, finance, milestones, and performance). Rather, it represents a candid, realistic assessment of the project's overall status in light of all currently known facts and circumstances currently or likely to be impacting the project's ultimate success.

Source: The FDIC's *Capital Investment Project Assessment Rating System* guidance.

The guidance provides a "stoplight" system (red/yellow/green) for rating project performance and identifies thresholds for follow-up on variances. The color-coded system indicates whether actual data fall within an acceptable range in comparison to

[15] Detailed IT project budget and actual cost information is obtained from the Project Number Information Application (PNIA). PNIA was established to summarize FDIC project-related cost information from the FDIC Financial Data Warehouse.

expected cost, schedule, and scope (functionality) information. Project managers must specify planned actions to address identified problems for projects rated "yellow" or "red."

The FDIC Assessment Rating Definitions

G	The project is performing and is expected to continue to perform according to plan and to deliver all of the expected functionality.
Y	The project's overall performance varies slightly (up to 10 percent) from the project plan and is likely to be slightly over budget or slightly behind schedule, and the functionality to be delivered may not conform in certain respects to the original plan.
R	The project's overall performance varies significantly from the project plan. Cost overruns, schedule slippages, and material variances from desired functionality in the system ultimately delivered are all present or are quite likely to varying degrees and, taken as a whole, show a project that is at serious risk in the absence of corrective action.

Source: *Capital Investment Project Assessment Rating System* guidance.

DIRM's IMB reviews the adequacy and consistency of project information provided in the quarterly reports, but the CIRC is ultimately responsible for approving the quarterly assessment of project performance and for taking corrective actions as necessary. The CIRC has the authority to recommend to the FDIC Board that a project be canceled, funds be limited, or other corrective actions be taken when cost overruns, major schedule delays, or performance shortfalls occur. The CIRC may also recommend redirecting funds to other high-priority initiatives. The CIRC itself is not authorized to cancel projects or redirect funds.

Project teams have submitted quarterly reports since the first quarter of 2003. As the process has evolved, the reports have progressed from being a point-in-time snapshot of the projects to a more forward-looking analysis of project risks. When significant variances were identified, the CIRC required corrective actions to improve project performance, including re-baselining the project plan to address schedule slippage and increased costs.

However, the process could be further improved by establishing additional procedures.

- CPIM procedures should specify requirements for validation of project assessments by independent qualified personnel.

- Also, CPIM procedures should be established for reviewing the quarterly performance criteria at regular intervals to ensure that the criteria reflect current performance expectations and the organization's current strategic objectives.

- CIRC procedures should be established for documenting and tracking performance problems and verifying completion of necessary corrective actions. For example, the CIRC could maintain a corrective action tracking matrix that summarizes CIRC decisions on corrective actions, parties responsible for corrective actions, and associated time frames for completing such actions.

The CIRC quarterly review process is for projects in the planning and development phase. Officials stated that the CIRC will monitor capital investments until the PIR is complete then the CIO Council will assume oversight responsibility. According to GAO, capital investments should be monitored throughout their life cycles to ensure that investments continue to meet users' needs. The FDIC needs to develop specific guidance to document the CIO Council's process for overseeing IT capital investments in the steady state phase.

Additionally, the FDIC should continue efforts to establish an earned value management (EVM) system that controls government and contractor cost as a part of the FDIC's project management procedures. EVM provides early insight into performance trends and variances from initial plans, allowing decision makers enough time to take corrective action.[16] DIRM is researching the FDIC's options for establishing such a system.

Capturing Investment Information. The FDIC generates and maintains project information in various documents and systems. However, the FDIC efforts to develop a comprehensive repository of investment-related project information are ongoing. Key investment-related information for projects in the steady state phase has not been identified. In addition, the FDIC has not fully established policies and procedures for capturing and maintaining information on IT investments, including key information that should be updated and maintained on a regular basis. Therefore, the FDIC cannot adequately ensure that an inventory of such information can be relied upon as an effective tool to assist in investment decision making.

According to GAO, to make good IT investment decisions, an organization must identify its IT assets, be able to acquire pertinent information about each investment, and store that information in a retrievable format, to be used in future investment decisions. A guiding principle for developing the information source is that it should be accessible where it is of the most value to those making decisions about investments. GAO has also stated that this critical process may be satisfied by the information contained in the current EA, augmented by additional information (e.g., financial information, risks, benefits) that the investment board may require to ensure that informed decisions are being made. An organization's "as-is" architecture, along with its sequencing plan, can provide a resource for developing a list of existing investments.

An asset inventory is also a requirement of the Federal Information Security Management Act (FISMA).[17] FISMA requires the inventory to identify the interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency. The FISMA requirement stems from OMB's

---

[16] As reported in OIG report *Enhancements to the FDIC System Development Life Cycle Methodology*, (OIG Report No 04-019, dated April 30, 2004), EVM measures the actual work being performed (milestones completed) against a detailed plan in order to accurately predict the final costs and schedule results for a given project. The tool requires that a plan for project performance measurement be created. The earned value, or work performed, is then measured against the actual costs of accomplishing the work, providing a measure of the project's true cost performance. The method provides project managers with a type of "early warning" system, allowing them to take corrective action should project spending outpace the physical work being accomplished.

[17] See Section 305(c) of FISMA (title III of the E-Government Act, Pub. L. No. 107-347), which amends 44 U.S.C. § 3506. The FDIC is legally bound by this provision.

expectation that each agency have such an inventory in accordance with its work on developing its EA. FISMA also requires that the inventory be updated at least annually.

Furthermore, the National Institute of Standards and Technology (NIST) has noted that a key aspect of GAO's Stage 2 maturity is the creation of an asset inventory to ensure the agency can identify cost, benefit, schedule, and risk milestones and investment ownership information and review investment performance accordingly.[18] NIST advises agencies to build a single asset inventory that meets the requirements of both the GAO ITIM framework and FISMA. Agencies will then have a single repository where they can manage IT security reporting concerns for FISMA and effectively manage their investments to continue maturing along the ITIM framework path.

CIRC procedures require the project sponsor, in collaboration with the DIRM program manager, to establish and maintain project-related information, including, but not limited to, project security costs, the schedule, technical baselines, risk mitigation activity, and status information. The *FDIC SDLC Manual* requires that project managers develop a project work plan that compares results being achieved to the projected costs, benefits, and risks, so that actual or potential managerial, organizational, or technical problems can be identified. The project work plan can be used to recognize when the project is in difficulty and to discuss the difficulties with the client as soon as possible.

Project-level investment information is provided to the CIRC primarily through the quarterly reports. Additionally, a list of the current CIRC-level projects and policies is maintained on the CIRC Website on the FDIC Intranet. The list provides general financial and contact information about each project. The quarterly assessment reports (CIO Report, CIRC Financial Report), and CIRC Website serve as a point-in-time repository of selected information on CIRC projects. The FDIC also collects and stores IT-project related information in other locations, including the FDIC Digital Library (FDL), the EA Website, and the IT Corporate Data Repository (CDR). All three are accessible through the FDIC network.

- The FDL includes project information, such as business cases, quarterly project assessment reports, and FAC and EAC review memoranda. The FDIC's EA blueprint, containing the FDIC's EA principles and high-level information on the FDIC's current and target EAs is also available in the FDL. However, project-related information for several capital investment projects had not yet been placed in the FDL as of the time of this evaluation.

- The EA Website, launched in November 2003, contains general information on the FDIC's EA but does not contain detailed current application architecture information for each FDIC division.

- The IT CDR, maintained by DIRM Delivery Management (DM), includes an inventory of those applications managed by DM and those client-developed and maintained applications of which DM is aware. The CDR identifies applications in development, in production, or inactive. DM does a quarterly review of the CDR and certifies to the accuracy of its data to the DIRM Deputy Director.

[18] *Integrating IT Security into the Capital Planning and Investment Control Process* (NIST draft special publication 800-65, dated June 2004). This publication provides guidance to agencies but is not legally binding on the FDIC.

DIRM has several efforts underway that should help to establish a comprehensive repository of IT project-related information.

- The new PMO has also begun work to develop an inventory of project-related data that can be used for project standardization, analysis, and control.

- As a result of the DIRM transformation project, an inventory of several hundred FDIC applications was recently completed, and an analysis of that inventory is in process. This effort is known as the Application Rationalization Project. The objective of the inventory is to help IT management identify possible reductions in costs related to maintenance and support staffing requirements, licensing needs, planning for infrastructure enhancements, and platform upgrades.

- DIRM recently implemented an Enterprise Asset Management (EAM) system that will be used to manage all IT assets and will be integrated with the FDIC's financial and help desk systems.

- The FDIC has begun efforts to develop an EA repository by creating a meta-model of repository data and by evaluating various repository tools. In addition, the FDIC is seeking contractor assistance to use the tool, once selected, to populate and maintain the repository with up-to-date information on FDIC systems. A key advantage in using a repository tool (with data that is continually updated) is continuous management visibility of current performance results of each investment.

The lack of a comprehensive repository increases the risk that the CIRC and CIO Council will not have at its disposal reliable information for supporting project and portfolio investment decisions and oversight. As the FDIC continues work to identify and inventory information about its IT projects and systems, the CIRC, in concert with the CIO Council, should establish guidance to document the specific capital investment-related information, including information about steady state investments, that should be captured and maintained, where it should be stored, the organization responsible for updating the information, and how often it should be updated.

Challenges for Building the Investment Foundation for Capital Investments

The FDIC has made progress in building its investment foundation for capital investments. However, additional work is needed to sustain progress and establish a repeatable, effective, and efficient process. Table 5 identifies the FDIC's efforts underway that should institutionalize some of these processes and the steps for which additional action is needed to further strengthen the program.

Table 5: Steps for Progressing in Stage 2

Building an Investment Foundation

To sustain progress and strengthen the process.

Efforts underway that should **institutionalize** the CPIM process:

- **Instituting the Investment Board –** Fostering a strong understanding of the interrelationships among recently restructured IT-related committees.
- **Meeting the Business Needs** – Using the *IT Strategic Plan* as a tool to help ensure IT investments align with corporate missions and goals.
- **Providing Investment Oversight** – Implementing planned initiatives related to strengthening project management skills and ensuring such skills include EVM.
- **Capturing Investment Information** – Completing a comprehensive inventory of IT project information and establishing the EA repository to provide IT project information that is readily available to assist the CIRC and CIO Council in making more informed investment decisions.

Actions needed to **strengthen** the existing governance structure and CPIM process:

- **Instituting the Investment Board** – (1) Update the *FDIC Capital Investment Policy* to outline the CIO Council's responsibilities in the CPIM process and (2) keep formal records of FAC meetings and deliberations.
- **Selecting an Investment** – Establish procedures to periodically review and update (as needed) the existing project selection criteria.
- **Providing Investment Oversight** – Develop procedures for (1) specifying requirements for validating quarterly project assessments by independent qualified personnel, (2) reviewing and updating quarterly project performance assessment criteria at regular intervals, (3) documenting and tracking project performance problems and verifying the completion of necessary corrective actions, and (4) specifying the CIO Council process for overseeing IT capital investments in the steady state phase.
- **Capturing Investment Information** – Develop guidance to document specific capital investment-related information, including information about steady state investments, that should be captured and maintained, where it should be stored, the organization responsible for updating the information, and how often it should be updated.

Source: OIG analysis of program activities.

Developing a Complete Investment Portfolio for Capital Investments

To operate successfully at Stage 3, the organization must have in place the structure and repeatability of the project-centric management processes in Stage 2. Many of the Stage 3 processes build upon Stage 2 critical processes. The development of portfolio criteria communicates organizational priorities to the IT project management community and ensures that each investment submitted for funding supports the organization's mission, strategies, goals, and project-specific outcomes. Table 6 provides a high-level overview of the critical processes in Stage 3.

Table 6: Stage 3 Maturity – Critical Processes

ITIM Critical Processes
Defining the Portfolio Criteria *Process of developing quantitative or qualitative factors such as cost, benefit, schedule, and risk in order to select projects for inclusion in the investment portfolio(s).*
Creating the Portfolio *Process of comparing worthwhile investments and then combining the investments selected into a funded portfolio.*
Evaluating the Portfolio *Process that builds upon the Providing Investment Oversight critical process from Stage 2 by adding the element of portfolio performance to the organization's control process activities.*
Conducting PIRs *Process for reviewing IT projects in order to learn from past investments and initiatives by comparing actual results to estimates. PIRs also serve as vehicles for evaluating the entire CPIM process.*

Source: GAO.

A detailed analysis of the corporation's efforts to date and remaining challenges follows.

Corporate Efforts to Date

Defining the Portfolio Criteria. The CIRC's portfolio criteria are generally defined in the CIRC charter. As previously discussed, the FAC and EAC assist the CIRC in evaluating whether projects should be recommended for funding and, therefore, included in the portfolio. However, the CPIM-related guidance does not specifically define the process for updating portfolio criteria. As it gains experience over time, the CIRC may be able to prescribe more specific portfolio selection criteria. Additionally, as discussed in the next section, development of the *IT Strategic Plan* and maturation of the EA program should enable the CIRC and CIO Council to evaluate and better define the FDIC's portfolio selection criteria over time.

The purpose of this critical process is to ensure that the organization develops and maintains IT portfolio selection criteria that support the FDIC's mission, organizational strategies, and business priorities. Developing an IT investment portfolio involves defining appropriate IT investment cost, benefit, schedule, and risk criteria to ensure that the organization's strategic goals, objectives, and mission will be satisfied by the selected investments. According to GAO, if an EA exists, it should be used as the foundation for developing and updating the portfolio selection criteria. Portfolio selection criteria build on the criteria that are used to select individual projects and focus on alignment with the organization's mission, organizational strategy, and line-of-business priorities. When IT projects are not considered in the context of a portfolio, criteria based on narrow, lower-level requirements may dominate enterprise-wide selection criteria.

As of March 31, 2004, the CIRC portfolio accounts for approximately 85 percent of the development-type projects at the FDIC.[19] When the CIRC was created, the overall benchmark for the CIRC review was capital initiatives that represented 80 percent of total funding for IT and other capital investments. The non-CIRC projects are managed and monitored at the division and office level. For example, DSC used a consultant to complete an independent review of its IT operational and administrative applications supporting its core business functions.

CPIM guidance states that proposed CIRC projects shall be evaluated for inclusion in the portfolio based on their contributions to the achievement of corporate goals and objectives and their ROI. For example, as discussed earlier, the FAC review is designed to ensure that all CIRC-proposed project business cases are adequately supported and that financial analyses are consistently performed. Additionally, the FAC's cost-benefit analysis guidance includes a broad description of its general investment decision criteria. That is, investments are initiated or continued when the projected future benefits to society or the FDIC exceed the projected future costs. Moreover, the guidance states that a positive ROI is only one factor in the cost-benefit analysis. Intangible costs and benefits must also be considered along with applicable overriding legislative or policy mandates. The CIRC has not established a particular ROI threshold that investments must meet to be included in the portfolio and, at this time, the CIRC may not have enough data to establish meaningful standards. Furthermore, the CIRC has not established a procedure to ensure that the portfolio selection criteria are periodically updated.

Additionally, the EAC works with the CIRC and CIO Council to ensure that all IT investments align with the FDIC's EA. If a project does not align with the EA, alternative solutions must be provided or an explicit waiver must be obtained from the CIRC. In addition to presenting CIRC projects at EAC meetings, divisions and offices have also presented other IT project proposals to ensure that those projects are aligned with the FDIC's EA principles. The Technical Review Group and Corporate Data Sharing Steering Committee coordinate with the EAC. The TRG is responsible for reviewing and evaluating technical solutions in a manner that will provide the FDIC with an enterprise approach to evaluating IT solutions so that the scope of the technology includes the needs and requirements of the entire Corporation. The CDSSC sets the strategic direction for corporate data planning, management, and use within the FDIC.

---

[19] Development-type projects include projects coded as development (D), enhancements (E), technical initiatives (I), and planning (P).

Creating the Portfolio. As of March 31, 2004, the CIRC portfolio included 11 IT projects. The FDIC's investment budget captures most of the projects in the CIRC portfolio.[20] However, the CIRC is also monitoring two projects that are not part of the investment budget. As discussed in the next section, the CIRC prepares a quarterly report for the Board of Directors that demonstrates the CIRC's ongoing assessment of the portfolio. As the CIO Council, use of the *IT Strategic Plan*, and EA repository tools become institutionalized components of the CPIM process, the CIRC should be better able to ensure that IT investment decisions are consistent with enterprise-wide priorities and that the FDIC is spending its IT dollars in the right place and getting the best value.

The purpose of creating the portfolio is to ensure that IT investments are analyzed according to the organization's portfolio selection criteria and to ensure that an optimal IT investment portfolio with manageable risks and returns is selected and funded. The development of the portfolio is an ongoing process that includes decision making, prioritization, review, realignment, and reprioritization of projects that are competing for resources and funding. The IT investment board should collectively analyze and compare all investments and proposals to select those that best fit with the strategic business direction, needs, and priorities of the entire organization. According to GAO, each organization has practical limits on funding, the risks the organization is willing to take, and the length of time during which the organization is willing to incur costs for a given investment before benefits are realized. To address these practical limits, the process of creating a portfolio primarily uses categorization to aid in investment comparability and cost, benefit, schedule, and review oversight. For example, the portfolio categories could be established by:

- aligning IT spending with the strategic goals of the organization – identifying specific types of projects, groups, or service lines;
- defining spending levels for the portfolio categories, for example, "XX" percent to technology development, "XX" percent to new services, "XX" percent to infrastructure projects, "XX" percent to technology enhancements and improvements; and
- prioritizing IT projects within the portfolio categories.

According to FDIC officials, the establishment of the Investment Budget allows the CIRC to focus on significant IT initiatives in a systematic manner. Table 7 provides a snapshot of CIRC-related projects included in the FDIC's Investment Budget and illustrates that the CIRC portfolio includes investments from different FDIC line divisions and DOA, Legal, and DOF.

[20] The FDIC's Investment Budget also includes budgeted expenses of $110.8 million associated with the Virginia Square Phase II construction project. A second office building is being built to expand the FDIC's offices in Arlington, Virginia. The costs associated with this project are not monitored by the CIRC because the governance structure for Virginia Square construction was already in place before the formation of the CIRC.

Table 7: CIRC IT Projects in the FDIC's Investment Budget

Project Name	Total IT Investment Budget (in thousands)	Percent of IT Investment Budget	Project Sponsor
Asset Servicing Technology Enhancement Project	$31,843	23%	DRR
Corporate Human Resources Information System – Time and Attendance	2,779	2%	DOA
FDIC*connect*	2,040	1%	Corporate
Federal Financial Institutions Examination Council Call Modernization – CDR	17,815	13%	DIR
IT Infrastructure Modernization	22,659	16%	DIRM
Laptop Replacement	10,429	8%	Corporate
Legal Information Management System	3,643	3%	Legal Division
NFE	34,711	25%	DOF
ViSION – Phase IV	12,725	9%	DSC
Total IT Capital Investment Portfolio*	**$138,644**	**100%**	

Source: CIRC Financial Report 1st Quarter 2004 and CIRC Management Reports – CIO Report.

* In addition to monitoring the IT projects included in the Investment Budget, the CIRC is monitoring one project in the planning phase – Claims Process Reengineering and one project in the development phase – EAM system. The EAM project is less than the $3 million capital investment threshold but is considered to have an enterprise-wide impact.

The *IT Strategic Plan* documents the alignment of IT investments that are supporting the Corporation's program areas and provides a tool to ensure that no strategic requirements are overlooked. However, as discussed in the prior section of the report, the CIRC has not established specific portfolio selection criteria that would provide a foundation for assessing the FDIC optimal portfolio mix. Nonetheless, the FDIC has begun, through the CIO Council's ongoing work, to evaluate the extent to which IT investments are aligned with the FDIC's strategic goals. In addition, the CIRC has begun to evaluate the organization's capacity to concurrently handle a number of major development projects. For example, in the April 13, 2004 CIRC meeting, members of the CIRC discussed that in the future, the FDIC may not want to initiate several major development projects at one time. The *1st Quarter 2004 Capital Investment Report* stated that the CIRC does not expect to recommend the creation of any additional investment projects during the remainder of 2004. Rather, the CIRC intends to focus on the successful execution of the existing portfolio's business plans.

Evaluating the Portfolio. The CIRC is responsible for providing a quarterly assessment of the FDIC's current capital investment portfolio to the Board of Directors. The quarterly reports contain updates for individual projects as well as metrics for measuring the performance of the portfolio as a whole, including risk trends. However, additional steps can be taken to strengthen this process. Moreover, the role of the CIO Council in evaluating the portfolio of capital investments in the steady state needs to be better documented.

The purpose of this critical process is to review the performance of the organization's investment portfolio at agreed-upon intervals and to adjust the allocation of resources among investments as necessary. GAO reports that the investment board's role is not to micromanage each investment but to ensure appropriate executive-level involvement and participation in monitoring each investment's progress toward achieving performance expectations. This critical process focuses on how the investment board monitors and controls the investment portfolio to ensure that the overall portfolio provides the maximum benefits at a desired cost and at an acceptable level of risk. GAO also notes that criteria for assessing portfolio performance must be reviewed at regular intervals to reflect current performance expectations. Criteria that were developed to assess the original investment portfolio may no longer reflect the organization's strategic objectives.

The *FDIC Capital Investment Policy* requires the CIRC to provide a quarterly assessment of the FDIC's current capital investment portfolio to the FDIC Board of Directors. Specifically, after the individual *Quarterly IT Project Assessment Reports* are reviewed and approved by the CIRC, DIRM's Investment Management Branch, on behalf of the CIRC, compiles the individual project reports and an overall summary assessment into a single *Capital Investment Report* for the Board. The report summarizes the overall risk assessment for each of the projects as well as business line investment allocation information, financial risk trends, and other financial data. As of June 30, 2004, the CIRC had prepared five quarterly *Capital Investment Reports* for the Board.

CIRC Overall Evaluation Criteria

On Track: Project within costs, on schedule, no notable performance problems.

Minor Variance: Minor variance (up to 10 percent) in costs, milestones/schedule, and/or performance.

Significant Variance: Significant variances in costs, milestones/schedules, and/or performance.

Source: ***Capital Investment Report*.**

Based on its assessment of the portfolio activities during 2003, the CIRC concurred with recommendations to place four projects on hold in order to focus resources on other current projects. For example, during the fourth quarter 2003, project personnel determined that the planned December 2003 implementation date of the Corporate Document Management and Imaging project could not be met and that the cost and length of time needed to fix the problems could not be reasonably estimated. DSC and DIRM management decided, and the CIRC concurred, to place the Corporate Document Management and Imaging project on hold in order to direct their full attention to the completion of the ViSION project, which required re-baselining. The Corporate Learning System, Corporate Call Applications, and the Receivership Liability System Version 9 projects were also placed on hold in 2003.

However, the CIRC policies and procedures do not document specific criteria that the CIRC uses to assess portfolio performance nor document how performance problems are monitored or tracked. Moreover, the CIRC has not formally defined its role in evaluating projects once they enter the steady state phase. For steady state or operational status investments, OMB Circular No. A-11, *Exhibit 300*, states that each agency must review its portfolio of capital assets every year to determine whether the investment continues to meet the agency's mission needs and to prioritize the portfolio. Assets in the steady state phase must demonstrate how close annual operating and maintenance costs are to the original life-cycle cost estimates, and whether the level or quality of performance/capability meets organizational performance goals and continues to meet agency and user needs.

As discussed earlier, officials stated that the CIO Council will be responsible for steady state investments. Specifically, the CIO Council was established to further strengthen the management of IT investments. To that end, the Council is responsible for advising the CIO on all aspects of adoption and use of IT at the FDIC. Among other duties, the CIO Council will be responsible for reviewing and recommending IT investments to be made by the Corporation; conducting a quarterly review of the IT project portfolio, including assessing project health and progress and making recommendations for any corrective action; and supporting the CIRC in its oversight of IT investments from a corporate perspective. The *FDIC Capital Investment Policy* and procedures should be updated to describe the CIO Council's role in overseeing the portfolio of capital investments in the steady state phase and the CIRC's role, if any, in evaluating investments in that phase of the life cycle.

Conducting Post-implementation Reviews. The *FDIC Capital Investment Policy* states that PIRs will be performed on all capital investments. The purpose of the PIR is to measure the project team's performance in achieving the project's defined objectives and performance in executing the project plan on schedule and within budget. None of the CIRC projects have yet been subjected to a PIR because none of the CIRC projects have reached this stage, but the CIRC has sponsored meetings with project managers to discuss process improvement. The FDIC plans to conduct the PIRs using its *Post-Implementation Review Methodology;* however, not all of the current procedures have been documented. In addition, the charters for the FAC and EAC state that these committees will have a role in PIR process but their roles have not yet been explicitly defined.

According to GAO's ITIM framework, the purpose of a PIR is to evaluate an investment after it has completed development (i.e., after its transition from the implementation phase to the operations and maintenance phase) in order to validate actual investment results. This review is conducted (1) to examine differences between estimated and actual investment costs and benefits and possible ramifications for unplanned future funding needs and (2) to extract "lessons learned" about the investment selection and control processes that can be used as the basis for management improvements.

The FDIC's PIR program is designed to review system development projects to determine whether the projects meet stated business goals, are completed in a timely manner, are cost-effective, and meet end-user requirements and expectations. PIR procedures require that the PIR compare the investment cost and benefit assumptions with actual cost and benefit data to date. This requirement is reflected in the *FDIC PIR Handbook*, which indicates that the PIR report should include discussion or analysis of cost and schedule variance, tangible and intangible benefits achieved, continued need for the system, and improvements to project implementation practices.

Several projects are expected to be implemented by the end of calendar year 2004. In fact, one CIRC project moved from the development phase to the implementation phase at the end of June 2004. DIRM officials presented a summary of the processes and procedures used during the PIR for the Assessment Information Management System II project (a non-CIRC project) to the CIRC during the January 16, 2004 CIRC meeting. The purpose of the discussion was to provide information to CIRC members and project managers on what to expect during future reviews.

Additionally, the *FDIC Capital Investment Policy* identifies the personnel responsible for completing a PIR. Specifically, for IT-related projects, the project's sponsoring division or office is responsible for forming an independent review group to perform the PIR. The review group should, therefore, not include any members from the project team for the project under review. The policy also indicates that the PIR should begin 6 to 12 months after project completion. Management's goal is to complete PIRs within 180 days of their start date.

The FDIC has developed a *PIR Methodology* document to enable the FDIC to confirm the quality of system development projects and improve management over IT investments. In addition, the FDIC has developed a *PIR Handbook* to identify PIR roles and responsibilities, specific steps to follow in completing a PIR, and templates and worksheets to facilitate the data gathering and reporting tasks. The *PIR Handbook* requires the following quantitative and qualitative data to be obtained and evaluated as part of the PIR:

- management interviews,
- user surveys,
- focus group meeting results,
- approved requirements and design documents, and
- planned and actual system development costs, schedule, savings, maintenance costs, performance, and deliverables.

The CIRC is responsible for reviewing all PIRs, communicating relevant findings, and adopting best practices into the CPIM process. The *PIR Methodology* and *PIR Handbook* require that needed corrective actions, lessons learned and identified best practices be documented in the PIR report. Follow-up on corrective actions is the responsibility of the project team. The Office of Enterprise Risk Management's (OERM) Internal Risks Information System (IRIS) was used to document and track lessons learned in the Assessment Information Management System PIR.[21] However, PIR procedures do not address the use of the OERM IRIS tracking system. To strengthen the existing process, the FDIC needs to update the PIR procedures to identify the current process for documenting and tracking corrective actions identified during the PIR process.

In addition, the CPIM procedures state that the FAC and EAC are to review the results of the PIRs and determine whether the processes and standards need to be modified based on the findings. Further, the FAC charter indicates that one of the functions of the FAC is to produce periodic or needed PIRs in order to compare actual to projected benefits. However, no procedures have been developed to define the FAC or EAC responsibilities in the PIR process, and discussions with FAC and EAC members indicated that they had not established what their PIR-related role should be. It would be

[21] IRIS is the official FDIC tracking system for all GAO and OIG audits, reviews, and surveys. IRIS is used to track audit findings/conditions, recommendations, corrective actions, and milestones.

beneficial for the FAC and EAC to formally review the results of the PIR as a means of improving the quality of business case information and architectural analysis of proposed projects. To strengthen this process, the FDIC should develop guidance detailing FAC and EAC responsibilities for reviewing PIR results.

Although PIRs have not yet been completed, at the CIRC's direction, DIRM's IMB has held a series of meetings with project managers to share lessons learned and best practices identified through the CIRC process. DIRM's IMB along with OERM and the Corporate University[22] hosted a project management best practices conference on May 11, 2004. The theme for the conference was "*The Art of Project Management.*" The goals of the conference were to reinforce the FDIC's commitment to maintain a strong project management program and provide the FDIC's senior staff, project managers, and senior project team members with new and innovative approaches to managing projects Staff from all divisions and offices attended the conference and provided positive feedback.

Challenges for Developing a Complete Investment Portfolio for Capital Investments

The FDIC is beginning to address each of the critical processes in this stage, but further progress depends on sustaining Stage 2 processes and additional maturation of the FDIC's EA program. Table 8 identifies the FDIC's efforts underway that should institutionalize some of these processes and the steps for which additional action is needed to further strengthen the program.

Table 8: Steps for Progressing in Stage 3

Developing a Complete Investment Portfolio for Capital Investments

To sustain progress and strengthen the process.

Efforts underway that should **institutionalize** the CPIM process:

- **Creating the Portfolio** – Instituting the role of the CIO Council, developing the IT strategic plan, and ongoing development of EA program.
- **Conducting PIRs** – Completing scheduled PIRs and integrating lessons learned.

Actions needed to **strengthen** existing CPIM-related and PIR process:

- **Defining the Portfolio Criteria** – Establish a systematic process for evaluating and making necessary modifications to the IT portfolio selection criteria that may include specific cost, benefit, schedule, and performance criteria.
- **Evaluating the Portfolio** – Establish procedures to document (1) specific criteria used by the CIRC to assess portfolio performance, (2) responsibilities for tracking portfolio performance problems and corrective actions, and (3) the manner in which the CIO Council will oversee the portfolio of capital investments in the steady state phase.
- **Conducting PIRs** – (1) Develop guidance detailing FAC and EAC responsibilities for reviewing PIR results and (2) update PIR procedures to reflect current practices, including use of the IRIS to record and track corrective actions identified during the PIR process.

Source: OIG analysis of program activities.

[22] The Corporate University is the training and employee development arm of the FDIC.

Conclusion and OIG Recommendations

Measuring the overall effectiveness of the CIRC was difficult because of its relatively short history. In broad terms, GAO reports that, to be successful, an agency's IT investment processes should include the following elements:

- Key organizational decision makers are committed to the process and are involved throughout each project's life cycle.
- The investment management process is repeatable, efficient, and conducted uniformly and completely across the organization.
- Decisions are made consistently throughout the organization.
- Accountability and learning from previous projects is reinforced.
- The emphasis is on optimizing the portfolio mix in order to manage risk and maximize the rate of return.
- The process incorporates all IT investments but recognizes and allows for differences between various project types (e.g., mission-critical, administrative, infrastructure) and phases (e.g., new, under development, operational).

The FDIC has undertaken a broad range of activities to address the elements GAO considers necessary to implement a successful IT investment process. Effectively managing capital investment projects has been included in the *Corporate Performance Objectives* since 2002 and is a goal in the *IT Strategic Plan*. The *Corporate Performance Objectives* has been the FDIC's primary vehicle for prioritizing, sequencing, and evaluating CPIM improvement efforts.

To help ensure that the FDIC's CPIM process continues to mature, we recommend that the CFO and CIO, the CIRC Co-Chairs, take the following actions:

Strengthen the IT investment management governance structure.

(1) Update the *FDIC Capital Investment Policy* to outline the CIO Council's responsibilities in the CPIM process.
(2) Keep formal records of the FAC meetings and deliberations.

Strengthen CPIM-related procedures.

Establish CPIM procedures that, at a minimum, include guidance for:

(3) Periodically reviewing and updating (as needed) the existing CIRC project and portfolio selection criteria. This may include evaluating the need for more specific cost, benefit, schedule, and performance selection criteria.
(4) Specifying requirements for validating quarterly project assessments by independent qualified personnel.
(5) Periodically reviewing and updating quarterly project and portfolio assessment criteria.
(6) Documenting and tracking project performance problems and verifying the completion of necessary corrective actions.
(7) Documenting the CIO Council's oversight process for capital investments in the steady state phase.

(8) Documenting specific capital investment-related information, including information about steady state investments, that should be captured and maintained, where it should be stored, the organization responsible for updating the information, and how often it should be updated.
(9) Documenting the FAC and EAC responsibilities for reviewing PIR results.

In addition, PIR procedures should be

(10) Updated to reflect current practices, including the use of IRIS to record and track corrective actions identified during the PIR process.

Create a CPIM plan.

(11) Ensure that long-term CPIM program goals are integrated into corporate or DIRM planning documents to ensure continued focus on IT investment process improvements.

Corporation Comments and OIG Evaluation

The Deputy to the Chairman and CFO and the CIO and Director, DIRM, provided a written response dated September 17, 2004 to a draft of this report. The FDIC's response is presented, in its entirety, in Appendix III. Appendix IV presents a summary of the FDIC's responses to our recommendations.

The FDIC agreed with recommendations 1, 2, 7, 8, 9, and 11. The FDIC's proposed actions are sufficient to resolve these recommendations. However, they will remain undispositioned and open for reporting purposes until we have determined that the agreed-to corrective actions have been completed and are effective.

The FDIC partially concurred with recommendations 3, 5, and 10. The FDIC agreed with the intent of recommendation 3, but stated that the *FDIC Capital Investment Policy,* approved June 30, 2004, provides for periodically reviewing CIRC project and portfolio selection criteria. Specifically, the policy states that the CIRC is responsible for reviewing the policy annually and revising it as needed. Management explained that this statement is intended to mean that all aspects of the FDIC's capital investment planning program will be reviewed. Nevertheless, management stated that it would integrate the selection criteria into the policy to ensure that it is reviewed annually.

For recommendation 5, the FDIC responded that reviewing and updating quarterly project and portfolio assessment criteria is a routine part of the FDIC's CPIM process and stated that it will be part of the annual policy review. Additionally, management recognized that reviewing the guidance and application of the assessment criteria should be done on a regular basis and stated that the PMO will review the application of the assessment criteria and recommend changes to the CIRC as needed.

For recommendation 10, management agreed that existing PIR procedures require updating, but did not consider that IRIS represented the best tool for tracking PIR findings and recommendations. However, management stated that the PMO that will be established will take the lead in the development of policies and procedures relating to the PIR process, including the selection of any tool(s) for tracking PIR findings. In the interim, lessons learned from PIRs will be discussed at CIRC meetings and will be disseminated to corporate project managers through periodic best practices meetings – two of which were held in 2004.

The FDIC's proposed actions for recommendations 3, 5, and 10 are sufficient to resolve the recommendations. However, they will remain undispositioned and open for reporting purposes until we have determined that the agreed-to corrective actions have been completed and are effective.

The FDIC did not concur with recommendations 4 and 6. For recommendation 4, the FDIC responded that current procedures provide for an adequate independent validation of quarterly project assessments at multiple levels. Specifically, the *FDIC Capital Investment Policy* requires the project managers to submit a quarterly assessment report to the CIRC and Board of Directors, outlining the project's current status. Management stated that to ensure adequate independence of project assessments, the policy states that responsibility for assessing the performance of a project (i.e., reviewing the quarterly report) rests with its executive sponsor and executive steering committee, not the project manager. Furthermore, the policy establishes the CIRC as the final authority for approving all project assessments. Management also stated that the CIRC also issued the Capital Investment Project Assessment System guidance to executive sponsors and executive steering committees in assessing their respective projects. Accordingly, management believes that the existing structure provides requirements for validating quarterly project assessments by independent qualified personnel.

The intent of this recommendation was to ensure that existing control requirements for the review of quarterly assessment reports are clearly documented. We recognize that the executive steering committee plays an important role in reviewing the quarterly assessment ratings. However, according to the *FDIC Capital Investment Policy,* the executive steering committee is part of the project management structure, and some executive steering committee charters indicate that project managers serve as steering committee chairmen. In our view, additional controls are needed to ensure independence in the review process. These additional controls appear to exist based on our discussion with program officials but are not documented. We would expect that controls related to the independent review would parallel those in the new SDLC process.

Specifically, as discussed in the report, DIRM's IMB and the CFO also have roles in reviewing the adequacy and consistency of quarterly assessment reports, but the roles of the IMB and CFO are not described in the *FDIC Capital Investment Policy*. Additionally, through discussions with program officials, we understand that OERM staff also participate on executive steering committees. OERM's role could be defined to include reviewing project assessments for accuracy and consistency. Therefore, management should reconsider its position and provide additional information on requirements for validating quarterly project assessments by independent qualified personnel when it updates the *FDIC Capital Investment Policy* in June 30, 2005. Doing so would serve to strengthen existing policy. Accordingly, this recommendation will remain unresolved, undispositioned, and open, pending receipt of additional management comments, which we requested be provided within 15 days.

For recommendation 6, management stated that the quarterly assessment report will be the primary vehicle for reporting project information to the CIRC. Any project receiving a rating of "yellow" or "red" for any assessment factor is required to develop a plan for returning the project to "green" and to document the plan in the quarterly report. Due to the limited number of projects that make up the capital investment portfolio at any given time, management stated that the current procedures are sufficient. We plan to subsequently review the performance assessment process for the broader portfolio of FDIC IT investments. We reviewed the 2004 second quarterly assessment reports and found that plans for returning the projects to "green" are included. Accordingly, we agree that further action is not required. This recommendation is considered resolved, dispositioned, and closed for reporting purposes.

Objective, Scope, and Methodology

The objective of this evaluation was to determine whether the FDIC's CIRC is implementing an efficient and effective review process that supports budgeting for the FDIC's IT capital investments and ensures the regular monitoring and proper management of these investments once they are funded. To accomplish our objective, we used the GAO's ITIM Framework as a basis for evaluating the steps taken by the FDIC in the last 22 months (September 2002 through June 2004) to develop an IT investment management process for CIRC projects. GAO's ITIM model identifies processes that are critical for successful IT investment and organizes them into a framework of increasing maturity stages. We focused on reviewing the FDIC's progress in two stages of GAO's maturity model:

- **Stage 2 - Building the Investment Foundation**, which involves developing the capability to control projects and establishing basic capabilities for selecting new IT projects.
- **Stage 3 - Developing a Complete Investment Portfolio**, which involves a continual assessment of proposed and ongoing projects as part of a complete investment portfolio: an integrated and competing set of investment options.

We evaluated IT CPIM activities and processes in place as of June 30, 2004. We recognize that the FDIC may be implementing key practices associated with higher maturity stages. Indeed, GAO's framework discusses the fact that an organization may be concurrently implementing key practices that are associated with several maturity stages. Nonetheless, FDIC program officials agreed that the scope of our review aligned with their focus and efforts to date.

To obtain information about the FDIC's program activities and gain an understanding of internal controls related to our objective, we did the following:

- Interviewed the CIO and CFO, officials in DIRM's IMB, and FAC and EAC members.
- Reviewed relevant policies and procedures, including draft policies and other information available from the FDIC's Intranet, including the DIRM's Transformation Website, the CIRC Website, the EA Website, and the FDL.
- Observed a demonstration of the FDIC's business case template.
- Reviewed IT investment management governance charters, including those of project-level executive steering committees.
- Reviewed CIRC and EAC meeting minutes and attended one CIRC meeting and two EAC meetings.

We did not review the effectiveness of project-level oversight other than to gain a general understanding of the project-level governance structure – i.e., understanding the roles and responsibilities of the project manager, executive sponsor, and executive steering committee. Our evaluation did not include assessing the FDIC's investment management process for non-CIRC projects other than to gain a basic understanding of the process. Furthermore, obtaining a basic understanding of the FDIC's EA program was also a part of our work.

We also reviewed applicable laws and regulations and used them as criteria, where appropriate, to evaluate the FDIC's IT investment management process.

The limited nature of the evaluation objective did not require reviewing related performance measures under the Government Performance and Results Act[23] or determining the reliability of computer-processed data obtained from the FDIC's computerized systems. Not performing assessments of these areas did not affect the results of our evaluation.

We conducted our evaluation from January to June 2004 in accordance with generally accepted government auditing standards.

[23] Pub. L. No. 103-62, codified principally at titles 5 and 31, United States Code.

Acronyms

CCA	Clinger-Cohen Act of 1996
CDR	Corporate Data Repository
CDSSC	Corporate Data Sharing Steering Committee
CFO	Chief Financial Officer
CFOA	Chief Financial Officers Act of 1990
CIO	Chief Information Officer
CIRC	Capital Investment Review Committee
CPIM	Capital Planning and Investment Management
DIR	Division of Insurance and Research
DIRM	Division of Information Resources Management
DM	Delivery Management
DOA	Division of Administration
DOF	Division of Finance
DRR	Division of Resolutions and Receiverships
DSC	Division of Supervision and Consumer Protection
EA	Enterprise Architecture
EAC	Enterprise Architecture Committee
EAM	Enterprise Asset Management
ESC	Executive Steering Committee
FAC	Financial Analysis Committee
FASA	Federal Acquisition Streamlining Act of 1994
FDIC	Federal Deposit Insurance Corporation
FDL	FDIC Digital Library
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
IMB	Investment Management Branch
IRIS	Internal Risks Information System
IT	Information Technology
ITIM	Information Technology Investment Management
ITPA	Information Technology Program Assessment
NFE	New Financial Environment
NIST	National Institute of Standards and Technology
OERM	Office of Enterprise Risk Management
OMB	Office of Management and Budget
PIR	Post-implementation Review
PMO	Program Management Office
PNIA	Project Number Information Application
ROI	Return on Investment
RUP	Rational Unified Process ®
SDLC	System Development Life Cycle
TRG	Technical Review Group
ViSION	Virtual Supervisory Information on the Net

CORPORATION COMMENTS

FDIC
Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500 Co-Chairmen Capital Investment Review Committee

September 17, 2004

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

FROM: Steven O. App [Electronically produced version; original signed by Steven O. App]
Deputy to the Chairman and
Chief Financial Officer

Michael E. Bartell [Electronically produced version; original signed by Michael E. Bartell]
Chief Information Officer and
Director, Division of Information Resources Management

SUBJECT: Draft Report Entitled *FDIC's Capital Investment Management Review Process for Information Technology Investments* (Assignment No. 2004-015)

Thank you for the opportunity to comment on the above-referenced report. As you are aware, the FDIC has been actively developing and implementing a formalized capital planning and investment management (CPIM) process utilizing the GAO's Information Technology Investment Management (ITIM) framework and industry best practices. We are pleased at the considerable progress that has been made and intend to continue to institute practices to bring the FDIC's program to an even higher level of maturity.

It is important to note that implementation of the CPIM process has been occurring during a period of significant organizational change in the FDIC, in particular the ongoing DIRM transformation effort. An important component of this initiative is the establishment of a Program Management Office (PMO), which will be an additional resource to support and guide the CPIM activities. These organizational changes will impact the CPIM process as well as the ability to address the specific recommendations in the above referenced report.

Specifically, given that the future DIRM organizational structure is currently being re-defined, combined with the fact that no new capital investment projects are planned for the remainder of 2004, management has determined that it would be an inefficient use of resources to further document many of today's CPIM procedures. Rather management will focus resources on the successful implementation of the upcoming organizational changes. Upon completion of Phase II of the DIRM Transformation Plan – at which time it is believed that most of the necessary organizations will be in place – procedures will be refined and appropriately documented. Taking into account the timing of Phase II of the Transformation Plan and the degree of change anticipated, DIRM believes agreed upon corrective actions will be completed by June 30, 2006 unless otherwise specified below.

Recommendations:

Strengthen the IT investment management governance structure.

1. *Update the FDIC Capital Investment Policy to outline the CIO Council's responsibilities in the CPIM process.*

Concur. The *FDIC Capital Investment Policy*, approved June 30, 2004, will be reviewed and, as needed, updated at least annually. The policy will be modified by June 30, 2005, to incorporate the role of the CIO Council.

2. *Keep more formal records of the Financial Analysis Committee (FAC) meetings and deliberations.*

Concur. While the Committee's formal business decisions are documented in a memorandum to the CIRC, management recognizes the need for maintaining formal meeting minutes. Beginning immediately, minutes of all future FAC meetings will be produced outlining relevant discussion points and decisions. While no date has been set for the next FAC meeting, it is expected to occur prior to December 31, 2004.

Strengthen CPIM-related procedures.

Establish CPIM procedures that, at a minimum, should include guidance for –

3. *Periodically reviewing and updating (as needed) the existing CIRC project and portfolio selection criteria. This may include evaluating the need for more specific cost, benefit, schedule, and performance criteria.*

Partially concur. The Corporation agrees with the intent of the recommendation but believes that the *FDIC Capital Investment Policy* approved June 30, 2004 provides for periodically reviewing CIRC project and portfolio selection criteria. Specifically, the policy states that the CIRC is responsible for reviewing the policy annually and revising it as needed. This statement is intended to mean that all aspects of the FDIC's capital investment planning program are to be reviewed.

Nevertheless, selection criteria will be moved from the CIRC Charter to the *FDIC Capital Investment Policy* and reviewed annually as part of the policy review. This action will be completed by June 20, 2005.

2

4. *Specifying requirements for validating quarterly project assessments by independent qualified personnel.*

Do not concur. The CIRC believes that current procedures provide for adequate independent validation of quarterly project assessments at multiple levels. Specifically, the *FDIC Capital Investment Policy* requires project managers to submit a quarterly assessment report to the CIRC and Board of Directors outlining the project's current status. To ensure adequate independence of project assessments, the policy states that responsibility for assessing a project rests with its Executive Sponsor and Executive Steering Committee, not the project manager. Furthermore, the policy establishes the CIRC as the final authority for approving all project assessments. This current process – as documented in the *FDIC Capital Investment Policy* – provides multiple levels of independent review of all project assessments. Furthermore, its effectiveness is demonstrated by the downgrading by the CIRC of several proposed project assessments submitted over the course of the last year.

The CIRC also issued the *Capital Investment Project Assessment System* which provides guidance to Executive Sponsors and Executive Steering Committees in assessing their respective projects. This guidance was issued to provide consistency among the assessments of all the projects in the portfolio. As a result, management believes that its existing, documented procedures are sufficient to ensure consistent and independent assessments of all capital investment projects.

5. *Periodically reviewing and updating quarterly project and portfolio assessment criteria.*

Partially concur. Reviewing and updating quarterly project and portfolio assessment criteria is a routine part of the FDIC's CPIM process. Over the last year, the CIRC's quarterly Capital Investment Report to the Board of Directors has evolved steadily to incorporate a more portfolio oriented summary of the capital investment projects. These reviews and enhancements occur every quarter as part of the report preparation process.

Furthermore, the project assessment criteria are periodically reviewed and modified to reflect knowledge gained by additional experience with the CPIM process. During the first quarter of 2004, formal guidance outlining the assessment criteria was drafted and distributed to project managers for use in preparing their respective first quarter 2004 project assessment reports. This guidance will continue to be reviewed periodically (at least annually) as more experience is gained. The first annual review will occur by June 30, 2005.

Nevertheless, it is recognized that reviewing the guidance and application of the assessment criteria should be done on a regular basis. The to-be-established PMO will review the application of the assessment criteria and recommend changes to the CIRC as needed.

6. *Documenting and tracking project performance problems and verifying the completion of necessary corrective actions.*

Do Not Concur. All project managers are required to document project performance problems in their quarterly project assessment reports. In addition, any project receiving a rating of "Yellow" or "Red" for any assessment factor is required to develop a plan for returning the project to "Green" and to document this plan in the quarterly report. While the quarterly assessment report is the CIRC's primary tool for tracking project performance, all projects encountering significant problems are also required to promptly discuss these issues at the CIRC meetings. If warranted, a special CIRC meeting will be called. These discussions are documented in the CIRC meeting minutes. CIRC members are able to monitor the progress of corrective actions by reviewing future quarterly reports and through follow-up discussions with project management at future CIRC meetings.

In developing the CPIM process, the CIRC was cognizant of the need to provide effective management oversight of capital investment projects while avoiding micro-managing them. In order to minimize the amount of reporting required of project managers, it was decided that the quarterly assessment report will be the primary vehicle for reporting project information to the CIRC. Given the limited number of projects that make up the capital investment portfolio at any given time, it is believed that the current procedures are sufficient.

Below the CIRC level, the *FDIC Capital Investment Policy* also requires each capital investment project to establish an Executive Steering Committee. The Executive Steering Committee is charged with monitoring the progress of the project, approving any modifications to the existing plan, and following up on any changes to ensure that the project is completed as intended. These responsibilities are also delineated in the Executive Steering Committee's charter. This multi-level monitoring system allows significant project issues to rise to the level of the CIRC while making the Executive Steering Committee primarily responsible for monitoring any specific corrective actions.

7. *Document the CIO Council's oversight process for capital investments in the steady state phase.*

Concur. During the next revision of the *FDIC Capital Investment Policy*, provisions will be incorporated to specify the CIO Council's responsibilities regarding oversight in the steady state phase. This action will be completed by June 30, 2005.

8. *Documenting specific capital investment-related information, including information about steady state investments that should be captured and maintained, where it should be stored, the organization responsible for updating the information, and how often it should be updated.*

Concur. Responsibility for oversight of investment projects in the steady state phase will rest with the CIO Council and each project's respective division or office sponsor. The Council is currently performing a review of the entire portfolio of IT projects in use by the FDIC in order to identify overlapping systems and potential cost savings. In addition, a new enterprise asset tool will be installed to assist with tracking capital investments in the steady state phase. Specific tracking information will be developed and documented.

9. *Documenting the FAC and EAC responsibilities for reviewing PIR results.*

Concur. During the next revision to the *FDIC Capital Investment Policy*, specific responsibilities of the FAC and EAC in relation to the PIR will be incorporated. Current policy requires the next revision to be completed by June 30, 2005.

10. *Update PIR procedures to reflect current practices, including use of IRIS to record and track corrective actions identified during the PIR process.*

Partially concur. Management agrees that existing PIR procedures require updating to reflect new realities instituted by the CPIM process, the establishment of the PMO, and the introduction of the Rational Unified Process (RUP) software development process. However, at this time, management does not believe that IRIS represents the best tool for tracking PIR findings and recommendations. So while management agrees with the intent of the recommendation, disagreement is centered on the tracking tool specified.

Within the CPIM framework, the PIR is used to identify and document best practices and project management shortcomings that can be applied to other IT development efforts to improve future project results. These lessons learned are best presented to management, including the CIRC, where they can be reviewed and, as appropriate, acted upon. Where appropriate, these recommendations will be reflected in modifications to existing CPIM policies and procedures. Project management recommendations will continue to be disseminated to corporate project managers through periodic best practices meetings – two of which have been held year-to-date.

As some PIRs may not result in corrective actions, management believes it is premature to designate IRIS as the optimal method of capturing, disseminating, and tracking PIR results. To date, no CIRC project has undergone the PIR process. As a result, a final selection of any tracking system(s) has yet to be made. The *FDIC Capital Investment Policy* requires all capital investment projects to undergo a PIR within six-to-twelve months of completion. The Laptop Replacement Project, which concluded on June 30, 2004, will be the first capital investment project to undergo a PIR. By policy, this review is not required to be completed until June 30, 2005.

Current plans call for the PMO to take the lead in development of policies and procedures relating to the PIR process. Included in this responsibility is the selection of any tool(s) for tracking PIR findings. Management believes additional experience and analysis is required before any tool(s) can be selected.

Create a CPIM plan.

11. Ensure long term CPIM program goals are integrated into Corporate or DIRM planning documents to ensure continued focus on IT investment process improvements.

Concur. Corporate and DIRM objectives will continue to be used to ensure that the CPIM process continues to remain a primary focus of the Corporation. An IT Strategic Plan has been finalized and 2005 Corporate Performance Objectives will again include an objective that FDIC effectively manages capital investment projects. These planning documents will be used to ensure that the CPIM process continues to remain a primary focus of the Corporation. These actions are expected to be completed by December 31, 2004.

MANAGEMENT'S RESPONSE TO RECOMMENDATIONS

This table presents the management response on the recommendations in our report and the status of the recommendations as of the date of report issuance.

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	The FDIC will modify the *FDIC Capital Investment Policy* to incorporate the role of the CIO Council.	June 30, 2005	N/A	Yes	No	Open
2	Minutes of all future FAC meetings will be produced, outlining relevant discussion points and decisions.	December 31, 2004	N/A	Yes	No	Open
3	Selection criteria will be integrated to the *FDIC Capital Investment Policy* and reviewed as part of the annual policy review.	June 20, 2005	N/A	Yes	No	Open
4	Management did not concur with the corrective action. Management believes existing procedures are sufficient to ensure independent validation of quarterly project assessments at multiple levels.	N/A	N/A	No	No	Open
5	Project assessment criteria will be reviewed as part of the annual review of the *FDIC Capital Investment Policy.* Additionally, the to-be-established PMO will review the application of the assessment criteria and recommend changes to the CIRC as needed.	June 30, 2005	N/A	Yes	No	Open
6	Management did not concur with the corrective action. The existing quarterly review assessment report is the CIRC's primary tool for tracking project performance. In addition, the executive steering committees are charged with monitoring the progress of the project. This multi-level monitoring system allows significant project issues to rise to the CIRC while making the Executive Steering Committee primarily responsible for monitoring any specific corrective action.	N/A	N/A	Yes	Yes	Closed

7	During the next revision to the *FDIC Capital Investment Policy*, provisions will be incorporated to specify the CIO Council's responsibilities regarding oversight in the steady state phase.	June 30, 2005	N/A	Yes	No	Open
8	The CIO Council is performing a review of the entire portfolio of IT projects in use by the FDIC to identify overlapping systems and potential cost savings. In addition, a new enterprise tool will be installed to assist in tracking investments in the steady state phase. Specific tracking information will be developed and documented.	June 30, 2006	N/A	Yes	No	Open
9	Specific responsibilities of the FAC and EAC in relation to the PIR will be incorporated in the next revision to the *FDIC Capital Investment Policy.*	June 30, 2005	N/A	Yes	No	Open
10	The PIR will be updated to reflect new realities instituted with the CPIM process, the establishment of the PMO, and the introduction of the Rational Unified Process ® software development process. However, management stated that additional experience and analysis is required before any tracking tool(s) can be selected.	June 30, 2006	N/A	Yes	No	Open
11	The *IT Strategic Plan* has been finalized, and the 2005 *Corporate Performance Objectives* will again include an objective that FDIC effectively manages capital investment projects.	December 31, 2004	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.