Office of Inspector General

November 2007
Report No. EVAL-08-001

The FDIC's Internal Risk Management Program

Office of Evaluations

oig

Office of Evaluations

The FDIC's Internal Risk Management Program

Background and Purpose of Evaluation

Enterprise Risk Management (ERM) is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise. ERM is designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

ERM is a fundamental element of corporate governance practices in an organization. According to Protiviti®, Inc., a leading provider of independent internal audit and business and technology risk consulting services, "ERM is about establishing the oversight, control and discipline to drive continuous improvement of an entity's risk management in a changing operating environment."

In May 2004, the FDIC changed the name and focus of the Office of Internal Control Management to the Office of Enterprise Risk Management (OERM) and charged OERM with the responsibility of administering the FDIC's enterprise-wide risk management program.

Our objective was to assess: (1) the extent to which the FDIC has implemented an ERM program consistent with applicable government-wide guidance, and (2) OERM's implementation of FDIC Circular 4010.3, *FDIC Enterprise Risk Management Program*, dated September 25, 2006.

Results of Evaluation

The FDIC has a number of internally-focused committees and groups that help to keep the Board, Chairman, and senior executives informed of management operations and internal risks facing the Corporation and aid them in their decision-making. Taken collectively, these committees and groups as well as their respective reports and briefings provide a comprehensive means for managing internal risk and establishing transparency. More could be done, however, to (1) institutionalize how these entities interrelate and support ERM and (2) ensure the continuity of risk management efforts as changes in leadership and/or senior management occur.

We evaluated the FDIC's overall internal ERM efforts against key concepts and principles of COSO's ERM Framework. We also evaluated the FDIC's overall ERM efforts against the provisions of Office of Management and Budget Circular A-123, *Management's Responsibility for Internal Control*. The FDIC has implemented elements of several of the ERM Framework components through the establishment and actions of OERM and has established other internal risk management functions outside of OERM's purview. However, the FDIC's overall ERM program varies in some respects from what is recommended by COSO. Although organizations have latitude and flexibility in implementing ERM to meet specific needs, the FDIC may wish to further study the following aspects of its ERM program to maximize the effectiveness and efficiency of the various risk management activities currently in place throughout the Corporation.

- Defining and communicating the Corporation's risk appetite and ensuring that corporate objectives are aligned with that appetite;
- Implementing corporate-wide consistent processes for identifying, assessing, and responding to risks;
- Establishing effective channels for OERM to communicate risk information up, down, and across the Corporation; and
- Monitoring the implementation of the overall ERM program.

According to the FDIC Bylaws and implementing policy reflected in Circular 4010.3, *FDIC Enterprise Risk Management Program*, OERM is responsible for administering a comprehensive ERM program at the FDIC. OERM has issued policy providing high-level guidance for ERM program requirements and detailed guidance to OERM staff who serve as risk managers on large IT projects. FDIC senior officials advised us that they are pleased with OERM's contribution to risk management and key internal initiatives. However, we noted that OERM's activities and focus are inconsistent with the FDIC Bylaws and policy governing the Corporation's ERM program. In this regard, the FDIC could benefit from adding more structure to OERM's existing internal ERM policy and program, by:

- Defining the roles of the FDIC Board, Chairman, and Audit Committee in ERM and reconciling the stated role of OERM with actual practice;
- Issuing comprehensive procedures and guidance to establish consistent processes, tools, techniques, and models for identifying, assessing, mitigating, and reporting risks; and
- Providing corporate-wide training in ERM.

We evaluated the status of the FDIC's internal ERM program as administered by OERM against an ERM capability maturity model developed by Protiviti®, Inc., that provides criteria for ranking ERM programs on a continuum of five stages of

A principal source of criteria that we used in evaluating the Corporation's approach to internal risk management is the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management — Integrated Framework*. OERM's ERM policy (Circular 4010.3) states that the FDIC emphasizes guidance provided by COSO and references the ERM Framework.

Additionally, we researched relevant federal guidelines and practices related to ERM. We also consulted extensive work by Protiviti®, Inc., to gauge the maturity of OERM's risk management efforts and discern best practices in enterprise risk management.

Finally, we were mindful of the results of the recent study conducted by the U.S. Government Accountability Office (GAO) related to the Corporation's external risk management activities.

To view the full report, go to www.fdicig.gov/2008report.asp

Results of Evaluation (continued)

maturity from an *Initial State* to an *Optimizing State*. We concluded that the internal ERM program is in the *Initial State*, but possesses certain attributes of the *Repeatable State*, the second level of maturity. Characteristics of the *Repeatable State* include a basic policy structure, basic risk management processes, and basic control activities, all of which the FDIC possesses. However, the *Repeatable State* is also described as having explicitly defined and understood roles and commitments, people trained in the ERM process, independent spreadsheet models, and regular actionable reports—areas in which OERM's program has not progressed as far.

Finally, this report includes a matter for the FDIC's consideration regarding the relationship between the Corporation's internal and external risk management efforts. The FDIC's ERM Program is limited to internal FDIC operations, by design. However, this approach varies from the fundamental COSO tenet that ERM should be applied across the enterprise, at every level and unit, and should include taking an entity-level portfolio view of risk and consider interrelated risks from that perspective. In the interest of furthering effective corporate governance practices, we suggest that the FDIC examine the relationships between the Corporation's internal and external risk management activities to ensure they are complementary or integrated to the extent they efficiently and effectively mitigate any current or future risks to the successful accomplishment of the FDIC mission.

OIG Recommendations and Management Response

Much of the material in this report is informational—to provide an understanding of the various ERM activities currently in place throughout the Corporation. However, the report also contained seven recommendations and two suggestions intended to: (1) address the variances between certain current FDIC practices and approaches to ERM and those advocated by the COSO ERM Framework and applicable FDIC and government-wide guidance and (2) add clarity and structure to the ERM program.

After discussing the draft report findings, suggestions, and recommendations with the Chairman, management provided us a written response, dated October 18, 2007. FDIC management agreed in its response to our draft report to:

- Develop a more comprehensive blueprint to enhance coordination and to document the various committees and groups that contribute to ERM,
- Take efforts to more clearly define and communicate the Corporation's risk appetite and ensure that corporate objectives are aligned, and
- Clarify the roles of the Chairman, the Board, and the Audit Committee in relation to the ERM program.

These actions are responsive to one of our suggestions and two of our recommendations. Management disagreed with the remaining five recommendations and suggestion. In this instance, because the Chairman, who serves as the Corporation's audit follow-up official, has been involved in the response process, management's written comments constitute the FDIC's final determinations regarding the suggestions and recommendations in our draft report. Accordingly, we consider the recommendations closed and will not pursue them further. The Chairman committed to tracking those corrective actions agreed to by management. Accordingly, management's planned actions in response to (1) our suggestion regarding documenting how the various committees and groups interrelate in managing internal risk and (2) Recommendations 1 and 5 should be included in the Corporation's Internal Risks Information System, along with expected completion dates.

TABLE OF CONTENTS

Tables:

Figures:

ACRONYM LIST

ADR	Alternative Dispute Resolution
AICS	Administration & Internal Control Section, Division of Finance
APP	Annual Performance Plan
AU	Accountability Unit
BAPA	Budget and Accounting Procedures Act of 1950
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CFO Act	Chief Financial Officers Act of 1990
CIO	Chief Information Officer
CIRC	Capital Investment Review Committee
CM	Corporate Manager
COBIT©	Control Objectives for Information and Related Technology
COO	Chief Operating Officer
COSO	Committee of Sponsoring Organizations
CPO	Corporate Performance Objective
CU	Corporate University
DIR	Division of Insurance and Research
DIT	Division of Information Technology
DOA	Division of Administration
DOF	Division of Finance
DRR	Division of Resolutions and Receiverships
DSC	Division of Supervision and Consumer Protection
ERM	Enterprise Risk Management
FDIC	Federal Deposit Insurance Corporation
FDIC Board	FDIC Board of Directors
FFIEC	Federal Financial Institutions Examination Council
FFMIA	Federal Financial Management Improvement Act
FISMA	Federal Information Security Management Act
FMFIA	Federal Managers' Financial Integrity Act of 1982
GAO	Government Accountability Office
GPRA	Government Performance and Results Act of 1993
ICL	Internal Control Liaison
ICRS	Internal Control and Review Section, Division of Supervision and Consumer Protection
IRG	Internal Review Group, Legal Division
IT	Information Technology

MSS	Management Support Section, Division of Administration
NFE	New Financial Environment
NRC	National Risk Committee
OCC	Office of the Comptroller of the Currency
ODEO	Office of Diversity and Economic Opportunity
OERM	Office of Enterprise Risk Management
OICM	Office of Internal Control Management
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPA	Office of Public Affairs

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

DATE: November 30, 2007

MEMORANDUM TO: Sheila C. Bair
Chairman, FDIC

[Signed]
FROM: Jon T. Rymer
Inspector General

SUBJECT: *The FDIC's Internal Risk Management Program*
(Report No. EVAL-08-001)

Enterprise Risk Management (ERM) is a process designed to help management effectively deal with risks to achieving an entity's objectives. ERM integrates risk management with existing management processes, identifies future events that can have both positive and negative effects, and evaluates effective strategies for managing the organization's exposure to those possible future events. It aligns strategy, people, processes, technology, and knowledge with a strategic emphasis and an enterprise-wide application.[1]

The FDIC has a number of committees and groups that contribute to the FDIC's overall ERM efforts. Further, the FDIC established the Office of Enterprise Risk Management (OERM) to be responsible for ensuring that the Corporation has a risk management program in place and operational for all divisions and offices. OERM specifically focuses on risks *internal* to the FDIC while *external* risk management is the primary responsibility of other divisions and offices throughout the Corporation.

EVALUATION OBJECTIVE

Our objective was to assess:

- the extent to which the FDIC has implemented an ERM program consistent with applicable government-wide guidance and

- OERM's implementation of FDIC Circular 4010.3, *FDIC Enterprise Risk Management Program*, dated September 25, 2006.

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

[1] Description of ERM is based on a publication entitled, *Enterprise Risk Management: Practical Implementation Ideas*, by Protiviti®, Inc., an independent risk consulting firm. Protiviti®, Inc., has issued a number of ERM-related publications and has been recognized by an independent research firm as a risk consulting services leader. The Managing Director for Protiviti®, Inc., was also a member of the Project Advisory Council to COSO during development of the ERM Framework.

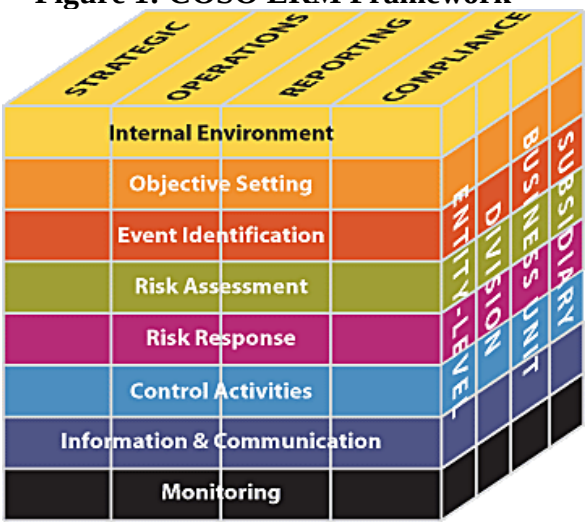
BACKGROUND

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines ERM as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

COSO's report, *Enterprise Risk Management – Integrated Framework*, (September 2004), defines essential components, suggests a common language, and provides direction and guidance for ERM. Notably, ERM requires an entity to take a "portfolio" view of risk that examines the entire organization, from the enterprise level, to a division or subsidiary, to the level of a single business unit's processes. As shown in Figure 1, ERM consists of eight interrelated components, which are integral to the way management runs the enterprise. The components are linked and serve as criteria for determining whether ERM is effective.

Internal control is encompassed within, and is an integral part of, ERM. ERM is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualization focusing more fully on risk.

Figure 1: COSO ERM Framework



Source: COSO ERM Integrated Framework, dated September 2004

History of Internal Control and ERM at the FDIC

In May 1996, the FDIC Board of Directors (FDIC Board) created the Office of Internal Control Management (OICM) to act as the corporate oversight manager for risk management and internal control. OICM's responsibilities included developing and implementing cost-effective programs to evaluate and strengthen internal controls, establishing guidelines and providing training related to internal controls, assisting program managers in identifying significant weaknesses and promoting timely and cost-effective corrective action, and establishing guidelines for a standard visitation program to effectively assess the condition of significant FDIC activities.

In March 2004, the FDIC Chief Financial Officer (CFO) proposed that OICM's office name be changed to OERM to better reflect industry risk management best practices and OICM's focus and initiatives at the time, particularly working with Information Technology (IT) security initiatives and serving as risk managers for several high-profile IT projects. In May 2004, the prior Chairman and the FDIC Board approved changes to the FDIC Bylaws to reflect the name change and revisions to the powers and duties of OICM.

According to the FDIC Bylaws, the Director, OERM, is responsible for administering the enterprise-wide risk management program that monitors and manages risk by maintaining partnerships with FDIC divisions and offices, providing training, and addressing internal control deficiencies. In addition to implementing a comprehensive ERM program, OERM is responsible for facilitating the annual assurance statement process, conducting program evaluations of the FDIC's major business lines, serving as a liaison to OIG and United States Government Accountability Office (GAO) auditors, providing staff support to the FDIC Audit Committee, and monitoring audit follow-up and resolution activities. OERM's ERM policy (Circular 4010.3) states that the FDIC emphasizes guidance provided by COSO and references the ERM Framework.

OERM's staffing consists of 13 employees, including a Director, an Assistant Director, 3 Senior Management Analysts (CG-15), 5 Senior Management Analysts (CG-14), 1 Management Analyst (CG-11), 1 Secretary, and 1 Student Intern. OERM's total budget for 2007 is about $2.2 million.

In addition, the FDIC has about 57 employees[2] assigned to divisional and office risk management/internal review units that perform internal control-related work for their respective division and office directors. These units may coordinate their efforts with OERM, but do not report to OERM. Appendix II provides detailed information about each of the division and office risk management/internal review units.

Legal and Regulatory Requirements

The Congress has long recognized the importance of strong internal control and enacted a number of related laws and requirements, including the following:

- Budget and Accounting Procedures Act of 1950 (BAPA), which required executive agencies, excluding government corporations, to establish and maintain systems of accounting and internal controls;
- Federal Managers' Financial Integrity Act of 1982 (FMFIA), which amended the Accounting and Auditing Act of 1950 (imbedded in BAPA) by requiring executive agencies to establish a continuous process for internal control assessment and improvement and to publicly report on the status of efforts by signing annual statements of assurance regarding their internal controls and accounting system;
- Chief Financial Officers Act of 1990 (CFO Act), which required government corporations to prepare statements on internal accounting and administrative control systems consistent with the corresponding requirements of the FMFIA;
- Government Performance and Results Act of 1993 (GPRA), which required agencies, including the FDIC, to set strategic and performance goals, and measure performance toward the goals; and
- Federal Financial Management Improvement Act of 1996 (FFMIA), which identified internal control as an integral part of improving financial management systems. This statute does not, however, apply to the FDIC.

[2] Some of these division and office employees have collateral duties beyond risk management.

The FMFIA required the Comptroller General to establish internal control standards and the Office of Management and Budget (OMB) to issue guidelines for agencies to follow in assessing internal control. The Comptroller General issued *Standards for Internal Control in the Federal Government* in 1983, identifying five standards for internal control. In 1999, the Comptroller General revised and reissued the internal control standards.

OMB issued Circular A-123, *Internal Control Systems*, in October 1981 in anticipation of FMFIA becoming law. In December 2004, OMB released a revised Circular A-123, *Management's Responsibility for Internal Control*, to provide updated internal control standards and new specific requirements for conducting management's assessment of the effectiveness of internal control over financial reporting. The revision also emphasizes the need for agencies to integrate and coordinate internal control assessments with other internal control-related activities and requires agencies to annually evaluate and report on the control and the financial management systems that protect the integrity of federal programs. Additional requirements for financial management systems are contained in OMB Circular A-127, *Financial Management Systems*, which expands upon the notion of agency accounting systems per FMFIA.

The FDIC considers Circular A-123 as setting forth "best practices" and has stated that, so long as the FDIC complies with the applicable FMFIA provisions on internal control, the Corporation will have complied with Circular A-123.

EVALUATION RESULTS

FDIC Committees and Groups that Contribute to Internal Risk Management

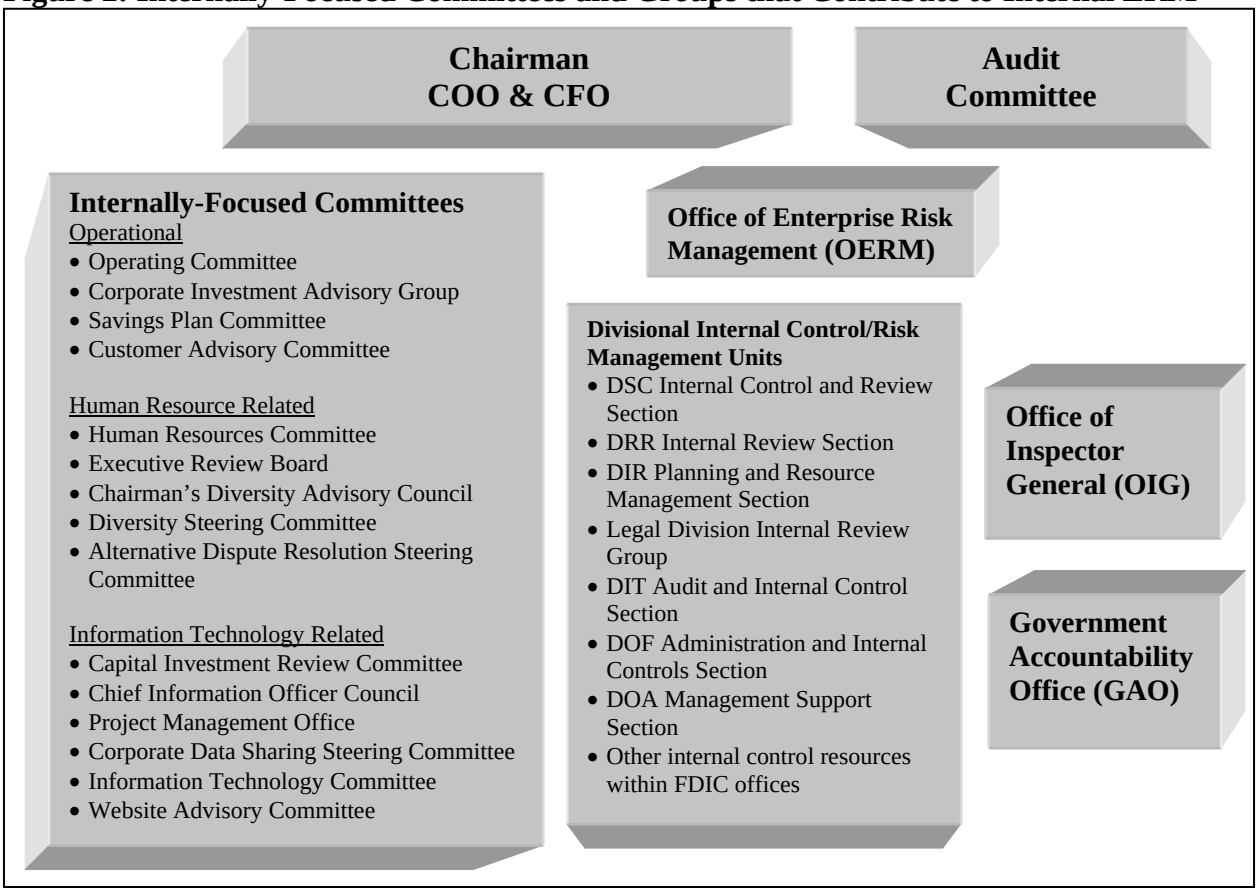
The FDIC has a number of internally-focused committees and groups that help to keep the FDIC Board, Chairman, Audit Committee, and senior-most executives informed of management operations and internal risks facing the Corporation and aid them in their decision-making. Taken collectively, these committees and groups and associated reports and briefings provide a comprehensive means for managing internal risk and establishing transparency.

We concluded that more could be done to institutionalize how these various entities interrelate and support ERM and to ensure the continuity of the Corporation's risk management efforts in the event of changes in leadership and/or senior management. As discussed below, many of these committees and groups are responsible for managing or monitoring specific internal corporate operations or functions such as major capital investments, system development efforts, or human capital initiatives that have the potential to present risks to the Corporation. While many of these committees have charters that specifically establish their purpose, membership, regular meetings, and reporting responsibilities, we did not see a clear articulation of how these committees and groups interact to support ERM in the Corporation. The FDIC's CFO indicated that such interactions do occur and are understood by FDIC managers, but acknowledged that such interactions could be better documented.

Figure 2 on the next page presents our understanding of the committees and groups involved in keeping the FDIC Board, Chairman, Audit Committee, and senior FDIC executives, such as the Chief Operating Officer (COO) and the CFO, aware of management operations and internal risks facing the Corporation and aiding them in their decision-making.[3] A brief discussion of each committee or group follows the figure. Figure 2 is not exhaustive and there may be other groups involved in internal risk management. In addition, Figure 2 does not include the committees and groups responsible for monitoring external risks facing the Corporation.

[3] We did not evaluate these committees or assess their activities in our review. Rather, through research, we obtained an understanding of the general purpose and membership of the various committees.

Figure 2: Internally-Focused Committees and Groups that Contribute to Internal ERM



Source: OIG analysis based on interviews and review of Corporation documents.

Operating Committee: Chaired by the COO, membership is comprised of the FDIC Chairman, Vice Chairman, Deputies to the Chairman and Vice Chairman, and directors of all divisions and offices. This Committee, which is scheduled to meet biweekly, serves as a briefing forum to ensure that Committee members are informed of issues concerning the Corporation.

Corporate Investment Advisory Group: Chaired by the CFO, membership includes Division of Finance (DOF), Division of Insurance and Research (DIR), and Division of Resolutions and Receiverships (DRR) directors, who review cash flow projections for each FDIC fund and provide advice to the CFO concerning (1) investment strategies in light of economic and market conditions, (2) appropriate levels of liquidity for each fund, and (3) purchase strategies for funds to be invested in Treasury securities. This Group meets quarterly.

Savings Plan Committee: This Committee is chaired by the CFO and includes the Director, DIR; Deputy General Counsel (Corporate Operations); Associate Director, Human Resources Branch, Division of Administration (DOA); and a representative from the National Treasury Employee's Union. The Committee considers issues related to the administration of the Corporation's 401(k) plan, including the performance of the plan's investment options.

Customer Advisory Committee: Co-chaired by the DOA and DOF Directors and includes a senior staff member from each division and office. This committee considers administrative matters of interest to FDIC management.

Human Resources Committee: Includes executives from FDIC Divisions and focuses on developing and evaluating human capital strategies with corporate-wide impact. The FDIC established this Committee to integrate strategic human capital planning into the Corporation's planning, budgeting, and investment processes. This Committee meets weekly.

Executive Review Board: Through this Board, the COO, CFO, and other members who might be appointed make recommendations to the FDIC Chairman on all matters affecting managers and executives, including compensation, benefits, incentives, and performance management.

Chairman's Diversity Advisory Council: Through this Council, individuals throughout the FDIC promote and support a diverse environment, facilitate employee communication with management regarding diversity concerns, and provide input to the Director, Office of Diversity and Economic Opportunity (ODEO), on recommendations for changes in policies and procedures that foster diversity objectives.

Diversity Steering Committee: Chaired by the Director, ODEO, membership consists of deputy directors for Division of Information Technology (DIT) and Division of Supervision and Consumer Protection (DSC) and the Deputy General Counsel, Legal Division. This Committee promotes and supports diversity initiatives.

Alternative Dispute Resolution Steering Committee: The Committee is comprised of representatives from every office and division designated to oversee corporate-wide alternative dispute resolution (ADR) policies, procedures, and programs and to assist in the design and implementation of new ADR processes. This Committee meets quarterly and also prepares for the FDIC Board an annual report on the uses of ADR throughout the Corporation.

Capital Investment Review Committee (CIRC): Co-chaired by the CFO and Chief Information Officer (CIO), membership consists of the Deputy to the Chairman, directors for DIR, DSC, DRR, DOF, and DOA, and the General Counsel. The committee meets quarterly and provides a systematic management review process to support budgeting for the Corporation's capital investments (defined as initiatives with a total capital outlay in excess of $3 million) and to ensure regular monitoring and proper management of these investments.

Chief Information Officer Council: Chaired by the CIO, members include executive representatives from DSC, DRR, DIR, DOF, DOA, Legal, DIT, and Corporate University (CU) as well as a representative of the COO. This Council, which normally meets monthly, advises the CIO on all aspects of adoption and use of information technology at the FDIC and supports the CIRC in its management and monitoring of the limited set of major IT investments.

Project Management Office: This office was established as a result of DIT's 2005 Transformation effort and resides within DIT's Business Administration Branch. The office

provides a number of critical functions to support the selection, management, oversight and analysis of a broad inventory of IT projects.

Corporate Data Sharing Steering Committee: Membership is comprised of representatives from all divisions, the COO's office, and the CFO's office. This Committee sets the strategic direction for corporate data planning, management, and use.

Information Technology Committee: Chaired by the Director, DIT, this Committee includes members from the CFO's Office and all divisions and reviews new IT initiatives and makes recommendations concerning the new initiatives to the CIO Council.

Website Advisory Committee: This Committee includes representatives from OPA, the Legal Division, DIR, DSC, DRR, DIT, and the COO's Office, and advises the Chief Web Officer on issues and corporate policies regarding the FDIC's Web page.

Audit Committee: This Committee is chaired by the Vice Chairman and includes the Director, Office of Thrift Supervision, and the Deputy to the FDIC Chairman. The FDIC's formal rules indicate that the Audit Committee is responsible for reviewing results of completed GAO and OIG audits and evaluations, requesting audit follow-up, if necessary, and submitting recommendations with respect to the audit reports to the Chairman's office and the FDIC Board.

OERM: Serves as liaison to the OIG and GAO staff working on audits of FDIC operations, provides staff support to the FDIC Audit Committee and select programs managed by other FDIC organizations, and coordinates preparation of the FDIC's Annual Performance and Accountability Report (Annual Report).

GAO and OIG issue audit and evaluation reports and present the results of their reviews of FDIC programs, operations, and functions to the Audit Committee. In addition to program operation and functional audits, the GAO annually audits the FDIC's financial statements. The OIG's business plan includes an annual evaluation of the FDIC's Information Security Program, as required by the Federal Information Security Management Act (FISMA).

Division and Office internal review units have their own internal risk management programs with activities such as regional and office reviews, annual risk assessments, internal control reviews, risk management reviews, and IT and business process reviews. Appendix II contains details on the resources and types of risk management activities for the divisions and offices.

Suggestion for Management

As discussed, the FDIC has a number of internally-focused committees and groups that collectively contribute to internal ERM and good corporate governance. More could be done, however, to institutionalize how these entities interact to manage internal risks facing the Corporation and for the purpose of preserving continuity in the event of senior management changes. Accordingly, we suggest that the Chairman's Office, in coordination with the COO and the CFO, articulate and document how the various committees and groups interrelate in managing internal risk.

Comparison of the FDIC's Overall Internal ERM Efforts to the COSO ERM Framework

The FDIC has incorporated elements of several of the eight interrelated components outlined in COSO's ERM Framework in the Corporation's overall internal risk management activities. Specifically, the FDIC's approach to risk management includes many of the principles encompassed in the Internal Environment, Objective Setting, and Control Activities components of COSO. However, we identified variances between the FDIC's existing ERM program and the COSO ERM Framework and concluded that opportunities exist for FDIC to make additional enhancements to its ERM program by incorporating key principles of the COSO ERM Framework.

COSO ERM Framework

Internal Environment:

Encompasses the tone of an organization, influencing the risk consciousness of its people, and is the basis for all other components of enterprise risk management providing discipline and structure.

According to COSO, the internal environment influences how strategies and objectives are established; business activities are structured; and risks are identified, assessed, and acted upon. This component influences the design and functioning of control activities, information and communication systems, and monitoring activities. Internal environment factors include:

- an entity's risk management philosophy;
- its risk appetite;
- oversight by the board of directors;
- the integrity, ethical values, and competence of the entity's people;
- how management assigns authority and responsibility; and
- how management organizes and develops its people.

Internal Environment Factors at the FDIC

The FDIC practices or possesses many of the internal environment factors in everyday operations of the Corporation. For example:

- The FDIC has published mission statements, a corporate vision statement, and core values.
- Members of the FDIC Board participate in monthly Board Meetings and are engaged in FDIC operations through management reports and periodic meetings with FDIC executives.
- The FDIC Board has established committees to manage certain functions, and the FDIC has established a number of operational committees to evaluate risks and manage projects.
- The FDIC Board has also delegated authority to committees and FDIC executives to carry out corporate functions.

- The FDIC holds its executives accountable for achieving corporate goals and objectives and has tied employee pay to performance.
- FDIC employees are required to follow government-wide standards of ethical conduct and supplemental standards pertaining to FDIC employees.
- The FDIC established the CU to coordinate and facilitate high-quality, cost-effective learning and development consistent with corporate objectives, and the FDIC requires employees to take annual awareness training related to information security and privacy.

Opportunities to Enhance the FDIC's Internal Environment

The FDIC may benefit from more explicitly addressing two factors in COSO's internal environment component, namely the FDIC's risk management philosophy and risk appetite. According to COSO, an entity's *risk management philosophy*:

- is the set of shared beliefs and attitudes characterizing how the entity considers risk in everything it does, from strategy development and implementation to its day-to-day activities;
- reflects the entity's values influencing its culture and operating style; and
- affects how enterprise risk management components are applied, including how risks are identified, the kinds of risks accepted, and how they are managed.

An entity's risk management philosophy is reflected in virtually everything management does in operating the entity and is captured in policy statements, oral and written communications, and decision making. COSO states that, when the risk management philosophy is well developed, understood, and embraced by an entity's personnel, the entity is positioned to effectively recognize and manage risk. Otherwise, there can be uneven applications of enterprise risk management across business units, functions, or departments.

Risk appetite is the amount of risk, on a broad level, that an entity is willing to accept in pursuit of value. It reflects the risk management philosophy and, in turn, influences culture and operating style. An entity's risk appetite is considered in strategy setting; guides resource allocation; and aligns organization, people, processes, and infrastructure. Entities can consider risk appetite (1) qualitatively, with categories of high, moderate, or low or (2) quantitatively, reflecting and balancing goals for growth, return, and risk. Protiviti®, Inc. reported that, in defining enterprise risk management, COSO set a standard for management to manage risk within the entity's risk appetite, as understood and agreed by the board of directors, and that management considers risk appetite when defining objectives, formulating strategy, allocating resources, setting risk tolerances,[4] and developing risk management capabilities.

In regard to risk appetite, the Director of OERM issued a November 2005 memorandum, *Update on ERM in the FDIC*, to division and office directors that discussed the link between "…risk appetite and reasonable assurance that the Corporation is in substantial compliance with any given requirement." The memorandum stated that:

[4] COSO defines risk tolerance, a term often used interchangeably with risk threshold or risk limit, as the acceptable level of variation relative to achievement of a specific objective, and often best measured in the same units as those used to measure the related objective.

> With respect to "risk appetite", I believe it is fair to characterize the Corporation as being primarily a risk-averse organization, relative to both our external and internal responsibilities. Clearly, this is a positive characteristic, given that we should be good stewards and strive to lead by example relative to both our peer group and the institutions we supervise. At the same time, however, managing to perfection or maintaining a zero-tolerance working environment on all controls is usually not a preferred course of action and could be counter-productive, particularly relative to employee morale and our overall cost-effectiveness.

We do note that elements of the FDIC's risk appetite are driven by law or regulation, such as the safety and soundness examination schedule, minimum institution capital levels, and limitations on investment options for the Deposit Insurance Fund. In other cases, the FDIC has imposed thresholds or limits, such as Maximum Efficiency, Risk-focused, Institution Targeted examination parameters or capital investment management oversight thresholds, which serve to establish risk appetite for discrete processes or functions.

Further, the FDIC Chairman has given speeches that describe the FDIC's risk appetite in regard to external matters in the banking industry such as subprime and predatory lending, mortgage foreclosures, and capital requirements. Also in reference to external risk responsibilities, the FDIC issued its second quarter 2007 *Letter to Stakeholders* in August 2007, in which the Corporation reported its continued focus on monitoring the mortgage market and any negative impacts on borrowers and insured institutions, bringing unbanked and underbanked populations into the financial mainstream, and working with other regulators to issue final rules regarding capital requirements for banks.

However, beyond the above-mentioned memorandum from the Director, OERM, we did not see evidence of a formally articulated risk philosophy or risk appetite for the Corporation. As discussed previously, COSO notes this articulation is important in ensuring that an entity is positioned to effectively recognize and manage risk, define objectives, and allocate resources.

COSO ERM Framework

Objective Setting:

Objectives must exist before management can identify potential events affecting their achievement. ERM ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

COSO states that objectives are set at the strategic level, establishing a basis for operational, reporting, and compliance objectives. Operational objectives, in particular, vary based on management's choices about structure, performance, and risk and reflect preferences, judgment, and management style. Effective ERM does not dictate which objectives management should choose, but does help to ensure that management has a process that aligns strategic objectives with the entity's mission and that ensures the chosen strategic and related objectives are consistent with the entity's risk appetite.

Objective Setting at the FDIC

Consistent with GPRA and related statutes, the FDIC defines its strategies and business objectives through the issuance of a strategic plan, an annual performance plan (APP), and a performance and accountability report (Annual Report). The FDIC also has implemented additional performance measurement processes in the form of Corporate Performance Objectives (CPOs) and balanced scorecards, as well as other performance metrics related to individual contracts and system development efforts. These measures cascade throughout the entity, divisional, and unit levels of the Corporation.

We recently issued an evaluation report[5] that concluded the FDIC has developed and implemented multiple performance measurement processes and approaches that serve various stakeholder needs and that FDIC managers use to varying levels to manage and monitor program performance. Collectively, we found that the FDIC uses performance measures to make management decisions to improve programs and results. We also found that the FDIC assigns responsibility for meeting specific performance objectives and completing corporate initiatives to individual agency managers.

Opportunities to Align Objectives with Risk Appetite

COSO notes that, as part of ERM, management not only selects objectives and considers how they support the entity's mission, but also ensures that they align with the entity's risk appetite. COSO also discusses establishing risk tolerances, which are acceptable levels of variation in the achievement of objectives. Entities use performance measures to ensure that actual results are within established risk tolerances. As discussed above, the FDIC has mechanisms in place for setting objectives and aligning them with its mission, and uses performance measurements to improve programs and results. However, with an established risk appetite, FDIC managers may be able to more readily establish objectives and measurements that are in keeping with the overall risk philosophy of the Board, Chairman, and other senior executives.

[5] *Evaluation of the FDIC's Use of Performance Measures* (EVAL-07-002), dated May 2007.

COSO ERM Framework

Event Identification:

Management identifies potential events that, if they occur, will affect the entity, and determines whether they represent opportunities or whether they might adversely affect the entity's ability to successfully implement strategy and achieve objectives.

According to COSO, an event is an incident or occurrence emanating from internal or external sources that affects implementation of strategy or achievement of objectives. Events with negative impact represent risks, which require management's assessment and response. Events with positive impact represent opportunities, which management channels back into the strategy and objective-setting processes. When identifying events, management considers a variety of internal and external factors that may give rise to risks and opportunities, in the context of the full scope of the organization. Examples of external factors are economic, natural environment, political, and social. Examples of internal factors include infrastructure, personnel, process, and technology.

Event Identification Factors at the FDIC

As discussed later, the FDIC identifies potential external events through the Corporation's external risk management activities performed principally through three divisions – DSC, DIR, and DRR – and the external risk committees identified later in Figure 4. In addition, the FDIC's 2007 Annual Performance Plan includes a discussion of external factors, such as the economy's performance at the national, regional, and local levels, which have an impact on the banking industry and the FDIC.

In regard to the FDIC's internal ERM program, Circular 4010.3 states that each FDIC manager should (1) identify key activities within his or her area of responsibility that contribute to the accomplishment of the division/office and/or corporate mission and (2) seek to determine what impediments (risks) might threaten the ability to achieve success. The policy notes that key activities could be tied to CPOs or initiatives defined in the program's balanced scorecard.

During the 2006 assurance statement process, OERM also requested divisions and offices to identify second-tier issues—areas of concern that did not rise to the level of a material weakness—in their assurance statements. The purpose of this exercise is to bring to light issues that previously may not have received attention because the focus of the assurance statement process was geared toward disclosing material weaknesses. Collectively, FDIC divisions and offices identified more than 60 issues. Examples of second-tier issues reported included topics such as Deposit Insurance Reform, the Contract Electronic File System, and curbing unfair and deceptive (lending) practices. OERM compiled the second-tier issues into a single list organized by division and office and provided the list to the Audit Committee in early 2007.

Opportunities to Enhance the FDIC's Event Identification

COSO notes that event identification needs to be robust, because it forms the basis for the risk assessment and risk response components. COSO also identifies examples of techniques and tools that may be used to facilitate event identification, such as:

- Event inventories: which are listings of potential events common to a specific industry or functional area,
- Facilitated workshops and interviews: usually of cross-functional teams regarding events that may affect achievement of entity or unit objectives,
- Process flow analysis: which involves mapping processes to identify potential events, and
- Loss event data tracking: which uses relevant data from past events to predict future occurrences.

COSO also discusses the importance of identifying interdependencies between events, categorizing potential events horizontally across an entity and vertically within operating units, and distinguishing events as either risks or opportunities. Doing so helps management develop an understanding of relationships between events, and provides information for assessing risks.

Although Circular 4010.3 provides high-level policy guidance for identifying key activities and associated risks, the Circular does not provide specific guidance for event identification, such as describing tools and techniques similar to those referenced by COSO above. Further, we confirmed that OERM has not issued specific guidance regarding the manner in which divisions and offices should identify events that could affect the achievement of strategic goals and objectives. We observed that divisions and offices conduct event identification processes to varying levels and degrees. For example:

- DIT is in the process of implementing the Control Objectives for Information and Related Technology (COBIT©) framework, an international IT controls and governance standard, which includes event identification efforts related to specific IT processes. DIT aligned its Accountability Units (AU)[6] with the 34 COBIT© IT business processes, one of which is to assess and manage IT risks. For this process, DIT prepared a management control plan for 2007 and identified and ranked IT risks.
- The FDIC's Legal Division meets annually with appropriate managers to identify new potential risks pertaining to individual AUs.
- DRR's risk management program is integrated with the division's annual planning cycle, and DRR uses its strategic plan to identify risk areas during the fourth quarter of each year to determine areas on which to focus internal review efforts for the upcoming year.
- DSC identifies risks annually based on and aligned with corporate initiatives.
- DOA identified eight functional areas for inclusion in its internal review program through consideration of emerging trends, consultation with OERM officials, known areas of high visibility and perceived risk, audit conditions, and DOA's judgment.

[6] An accountability unit is an organization's programs, functions or operations divided into meaningful units of appropriate size or nature to ensure an effective evaluation of internal accounting and administrative controls.

- DOF identified risks within the management control plans[7] developed for each of its accountability units.

COSO also stresses the importance of linking events and objectives, that is, identifying events that could prevent the achievement of objectives. In this regard, we interviewed officials from the Office of the Comptroller of the Currency (OCC) about the OCC's Enterprise Governance Program.[8] At the OCC, Enterprise Governance staff is responsible for facilitating the OCC strategic planning process. OCC executives hold an annual executive conference where executives identify strategic goals and objectives for the coming year. OCC executives also identify and assess risks associated with achieving strategic goals and objectives, and risk tolerances. Enterprise Governance staff document the results of the strategic planning and risk identification conference in a Strategic Risk Management Plan. An OCC Executive Committee monitors the plan during the year and meets quarterly to discuss plan status.

FDIC executives also hold an annual planning conference to develop CPOs and annual performance goals for the coming year, and we have observed that FDIC executives identify and discuss potential risks to achieving corporate objectives. However, this process is not as formal or well-documented as the OCC's approach or as closely coordinated with the ERM program.

[7] A management control plan represents a plan of scheduled internal control reviews based on the accountability unit's risk assessment.

[8] The Comptroller of the Currency established the Enterprise Governance unit, which reports to OCC's Chief of Staff and Public Affairs, to support the OCC's strategic planning, risk management, quality management, assurance testing, and business process improvement efforts.

COSO ERM Framework

Risk Assessment:

Identified risks are analyzed in order to form a basis for determining how they should be managed. Risks are associated with objectives that may be affected. Risks are assessed on both an inherent and a residual basis, with the assessment considering both risk likelihood and impact.

COSO notes that a risk assessment allows an entity to consider the extent to which potential events have an impact on the achievement of objectives. Management assesses events from two perspectives - likelihood and impact - and normally uses a combination of qualitative and quantitative methods. The positive and negative impacts of potential events should be examined, individually or by category, across the entity. Risks are assessed on both an inherent and a residual basis. Inherent risk is the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact. Residual risk is the risk that remains after management's response to the risk.

The COSO ERM Framework notes that the risk assessment component is a continuous and iterative interplay of actions that take place throughout the entity. While managers responsible for business unit, function, process, or other activities develop a composite assessment of risk for individual units, entity-level management should consider risk from a "portfolio" perspective.

Risk Assessment Factors at the FDIC

The FDIC's internal risk assessment activities are reflected in the following:

- Circular 4010.3 includes the concept of identifying and analyzing exposure to risks from both external and internal sources, and cites as policy that management should evaluate the risks identified for key activities in terms of both the likelihood of occurrence and the potential impact. The circular offers OERM's assistance to divisions and offices in regard to such evaluations.

- OERM's guidance for assurance statements highlights the concept of risk assessment being a continuous interplay of actions in an organization by stating that the primary basis for providing assurance on issues should be management's judgment based on knowledge gained from the daily operation of programs and systems and supplemented by results of internal reviews, audits, evaluations, and similar activities.

- OERM issued *OERM Risk Manager Guidelines* in 2005 for OERM staff who may be appointed to serve as risk managers on major IT projects. The guidelines include a discussion of risk assessment techniques, including assessing probability and impact.

- The FDIC's Legal Division, OERM, and CU developed enterprise risk management training which was presented to Legal Division management in July and October 2006. The training included a discussion of using qualitative techniques in risk assessments through which the impact of risk is portrayed as high, medium, or low, and the likelihood of occurrence is demonstrated as significant, moderate, or low.

Opportunities to Enhance the FDIC's Risk Assessments

FDIC Circular 4010.3 discusses the likelihood and impact of risk in the context of policy, but the circular does not indicate how risk assessments should be performed. OERM has not issued implementing procedures to specify how divisions and offices should be conducting risk assessments. Instead, Circular 4010.3 assigns responsibility for each division and office to establish its own risk assessment technique. Further, Circular 4010.3 focuses on division and office risk assessments for their respective organizations and does not address the principle of identifying and assessing risks that are common across the Corporation.

In this regard, we identified differences regarding how divisions and offices conducted risk assessment activities. Moreover, one division and one office representative expressed a desire for guidance from OERM regarding conducting risk assessments.

The COSO ERM Framework states that an entity need not use common assessment techniques across all business units and adds that the choice of techniques should reflect the need for precision and the culture of the business unit. However, COSO also states that although different methods may be used, they should provide sufficient consistency to facilitate the assessment of risks across the entity. Consistency would also facilitate developing an entity-wide risk portfolio. Finally, COSO notes that the time horizon used to assess risk should be consistent with the time horizon of the related strategy. Risk assessments may be:

- qualitative—such as risk rankings, risk maps, and risk questionnaires, or
- quantitative—such as probability-based techniques, stress testing, and scenario analyses.

As discussed earlier, OERM has requested divisions and offices to identify second-tier issues, which represents an improvement in the risk assessment process. However, OERM has not provided implementing guidance for prioritizing or assessing risk associated with second-tier issues, and we saw limited evidence that OERM or divisions and offices took steps to prioritize or perform risk assessments of second-tier issues. OERM's predecessor organization, the OICM, issued the *FDIC Internal Control and Risk Management Manual* in 1998, which included guidance for performing risk assessments and risk assessment questionnaires for management's use. As discussed in Appendix II, some FDIC organizations are still using some of the risk assessment techniques in the manual for their respective operations.

COSO ERM Framework

Risk Response:

Personnel identify and evaluate possible responses to risks, which include avoiding, accepting, reducing, and sharing risk. Management selects a set of actions to align risks with the entity's risk tolerances and risk appetite.

COSO provides that, having assessed relevant risks, management determines how it will respond. In considering its response, management assesses the effect on risk likelihood and impact, as well as costs and benefits, selecting a response that brings residual risk within desired risk tolerances. Management identifies any opportunities that might be available and takes an entity-wide view of risk, determining whether overall residual risk is within the entity's risk appetite.

Risk Response Factors at the FDIC

Circular 4010.3 provides possible risk mitigation strategies, including accepting a perceived low level of risk, developing additional controls, or instituting a process of independent testing to provide greater assurance that risks are mitigated to the extent necessary. In addition, in its guidance for the 2007 assurance statement process, OERM requested that divisions and offices provide a brief summary of any actions taken during 2007 to address second-tier issues identified during the 2006 assurance statement process.

We identified a good example where the FDIC identified and assessed risks, and developed mitigation strategies. The FDIC's Deposit Insurance Reform Executive Risk Management Committee prepared a proposed list of risks associated with deposit insurance reform activities, titled, *DI Reform – Risks Managed by DIRMT*. The listing included a title and description of identified risks, a numerical ranking of the magnitude of the risk, and control strategies for each risk to either mitigate the risk or develop contingency plans to address the risk. The listing effectively documented the risk response strategy and assigned a risk owner for each risk.

Opportunities to Enhance the FDIC's Risk Response

OERM could do more in this area by providing guidance to divisions and offices on how they should respond to identified risks (such as the second-tier issues) and to provide training related to the various types of risk responses (avoiding, reducing, sharing, accepting) and the concept of residual risk.[9]

We noted that OERM's guidance for assurance statements includes a statement that the non-material challenges reported for the year should be the primary (but not exclusive) basis for review initiatives planned by the respective division or office for the upcoming year. However, we did not see evidence that OERM evaluates the second-tier issues for commonality or aggregate effect across the Corporation. Taking such an enterprise-wide view may reveal that although business unit risks may be within the risk tolerances of the individual units, aggregate risks might exceed the risk appetite of the entity as a whole.

[9] COSO states that, in assessing risk, management considers both inherent and residual risk. Inherent risk is the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact. Residual risk is the risk that remains after management's response to the risk.

COSO ERM Framework

Control Activities:

Control Activities are the policies and procedures that help ensure that management's risk responses are carried out and objectives are achieved. Control activities may be categorized based on the nature of the entity's objectives to which they relate: strategic, operations, reporting, and compliance.

According to COSO, control activities occur throughout the organization at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, and segregation of duties.

Control Activities at the FDIC

The FDIC's risk management program identifies the internal control standard related to control activities stating that management shall develop and implement policies, procedures, techniques, and mechanisms ensuring that management directives are carried out. Some key control activities cited in Circular 4010.3 include:

- Top level review of actual performance.
- Management reviews at the program activity level.
- Management of human capital.
- Controls over information processing.
- Physical control over valuable assets.
- Establishment and review of performance measures and indicators.
- Segregation of duties.
- Proper execution of transactions and events.
- Accurate and timely recording of transactions and events.
- Access restrictions to and accountability for resources and records.
- Appropriate documentation of transactions and internal controls.

In addition, the FDIC has established scorecard initiatives in some divisions, and other control activities are reflected in corporate documents such as the FDIC Bylaws, DSC regional director memoranda, and various manuals and circulars.

OERM's guidance for preparing annual assurance statements requires divisions and offices to provide assurance on control activity-related areas of interest. For example, the 2006 assurance statement guidance requested that divisions and offices provide assurance on a number of items, including that:

- procedures were fully documented for all key activities,
- systems security was in substantial compliance with all relevant requirements,
- continuity of operations planning in all critical areas was sufficient to reduce risk to reasonable levels in the event of a disaster, and

- sufficient actions had been taken to minimize any negative impact associated with downsizing.

Opportunities to Align Control Activities with Risk Responses

The COSO ERM Framework notes that control activities are an important part of the process by which an entity strives to achieve its business objectives. While Circular 4010.3 identifies key control activities in the context of the GAO's *Standards for Internal Control in the Federal Government*, as is appropriate, the Circular does not address control activities in the context of ERM. In this regard, OERM could provide additional guidance or assistance to divisions and offices in:

- consistently linking corporate objectives to risk responses and to control activities;
- ensuring that control activities are designed to help ensure that strategic, operational, reporting, and compliance objectives are met; and
- evaluating control activities from a corporate-wide, or portfolio, perspective.

COSO ERM Framework

Information and Communication:

Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication occurs in a broader sense, flowing down, across, and up the entity.

COSO states that information is needed at all levels of an organization to identify, assess, and respond to risks, and to otherwise run the entity and achieve its objectives. Information systems must provide information to appropriate personnel so that they can carry out their operating, reporting, and compliance responsibilities. But communication also must take place in a broader sense, dealing with expectations, responsibilities of individuals and groups, and other important matters. Further, personnel must have a means of communicating significant information upstream. COSO also provides that every enterprise identifies and captures a wide range of information relating to external as well as internal events and activities, relevant to managing the entity. Technology plays a critical role in enabling the flow of information in an entity, including information directly relevant to enterprise risk management.

Protiviti®, Inc. notes that reporting is integral to the information and communication ERM component because it drives transparency about risk and risk management throughout the organization to enable risk assessment, execution of risk responses and control activities, and monitoring of performance.

Information and Communication Factors at the FDIC

The FDIC communicates information through a number of periodic reports for senior corporate managers pertaining to internal FDIC matters, such as:

- Quarterly CIRC reports on the status of capital investment projects (such as IT system development efforts);
- Semiannual Contract Assessment Reports that provide cost, milestone, and performance information on contracts valued at $5 million or greater;
- Quarterly Emergency Preparedness Reports;
- Quarterly CFO reports to the Board highlighting financial activities and results; and
- Quarterly Performance Summary on the status of CPOs and Annual Performance Goal exception reporting.

The Chairman's office has taken steps to make sure that the Chairman and the FDIC Board Members receive appropriate management reports in a format and level of detail that enhances understanding. The Chairman's office is developing a secure electronic repository to house FDIC Board and Chairman-level reports to improve management report delivery and availability. With regard to providing information to employees, the FDIC communicates information to staff in various ways, including:

- Posting on the FDIC's internal Web site performance information such as the CPOs, summary of year-to-date cumulative results on the accomplishment of the CPO goals, and APPs.
- DSC's balanced scorecard is available to all DSC staff and provides detailed information about strategic objectives and performance targets to provide a comprehensive view of business operations at the national, regional, and territory level.
- DOF's balanced scorecard is available to FDIC employees and presents performance measurement information about DOF operations, strategies, and initiatives.
- DOA and DOF encouraged their staff to participate in the 2008 corporate-wide planning and budget process by submitting potential new projects, performance objectives, and initiatives for 2008.

Annual Assurance Statement Process: As discussed earlier, OERM issues annual assurance statement guidance to divisions and offices that includes instructions for providing assurance on internal control objectives (for purposes of external reporting) and disclosing non-material challenges (second-tier issues) requiring management's attention (for purposes of internal reporting). OERM indicated that division and office disclosure of second-tier issues is a positive step, because it affords management the opportunity to devote resources to address those issues and to better plan risk management activities.

Opportunities to Enhance the FDIC's Information and Communication Efforts

OERM internal reporting on ERM activities could be enhanced. For example,

- While OERM briefs executive management and produces a bi-weekly Audit Status report, we identified no further examples of ERM reporting from OERM to the Chairman's Office or the FDIC Board.
- OERM discontinued the practice of providing monthly status reports to executive management in 2005, based on a corporate-wide initiative to streamline reporting.
- OERM has also discontinued its practice of periodically meeting with internal control liaisons from FDIC divisions and offices to discuss internal control and ERM issues. Several liaisons indicated that these meetings were helpful and allowed the liaisons to share ideas with their counterparts in other divisions and offices. Several liaisons indicated that they would like to resume meeting on a quarterly or some other periodic basis.

OERM Assurance Statement: OERM officials stated that they are not required to prepare an assurance statement regarding OERM's controls and activities because OERM compiles the division and office annual assurance statements and preparing its own would constitute submitting an assurance statement to itself. OERM officials also stated that other offices such as CFO and COO do not prepare assurance statements. We note that divisions and offices address their assurance statements to the Chairman, not OERM. Thus, submitting an assurance statement would not constitute OERM reporting to itself. We also note that OERM has other responsibilities in addition to facilitating the assurance statement process, including:

- the FDIC's ERM Program,
- internal control reviews and program evaluations of the FDIC's business lines,

- monitoring audit follow-up and resolution activities,
- Audit Committee activities,
- maintaining the audit tracking system,
- serving as risk managers for major IT projects, and
- the Post-Project Review program.

Without submitting an assurance statement, OERM has not provided the Chairman with documentation supporting positive assurance that the ERM program and other OERM program responsibilities are effective and efficient, have sufficient internal controls, follow relevant laws and regulations, or are supported by documented procedures.

Financial Management Systems Assurance: Opportunities also exist for the FDIC to improve external reporting of ERM activities. The FDIC Chairman's assurance statement in the Corporation's 2005 and 2006 Annual Reports indicates that the FDIC can provide reasonable assurance that the objectives of FMFIA Section 2 (internal controls) and Section 4 (financial management systems) have been achieved.[10] However, OERM has not developed agency-wide procedures regarding Section 4 assurances and reporting, and we were unable to confirm the basis or support for the Section 4 assertion related to financial management systems.

Government corporations, including the FDIC, are required by the CFO Act to prepare an annual management report that is consistent with agency statements on internal accounting and administrative control systems, as provided in FMFIA. The FMFIA also gives the Director, OMB, authority to issue implementing guidelines. OMB has done so in Circulars A-123, *Management's Responsibility for Internal Control* and A-127, *Financial Management Systems*. The FDIC has concluded that it is not required to comply with these circulars but relies on OMB's guidance to achieve compliance with the underlying statutory requirements.

According to A-123, FMFIA Section 4 requires an annual statement on whether the entity's financial management systems conform to government-wide requirements. These government-wide requirements are set forth in part in OMB Circular A-127, section 7, which, among other things, requires agencies to have financial management systems that meet various requirements, including the ability to:

- Provide timely and useful financial information, including internal and external reporting requirements, and ensuring the integrity of financial data through monitoring;
- Produce financial information required to measure program, financial, and financial-management for budget program-management and financial statement presentation; and
- Prepare, execute, and report on the agency's budget in accordance with OMB instructions.

Section 7 of A-127 also states that financial management systems shall be maintained to ensure efficiency and effectiveness and be clearly and currently documented per applicable guidance. These systems shall include a system of internal controls that ensure that resource use complies

[10] OMB Circular A-123 includes a provision for FMFIA Section 4 reporting for an annual statement on whether an agency's financial management systems conform to government-wide requirements mandated by the FFMIA and section 7 of OMB Circular A-127, *Financial Management Systems*.

with applicable laws, regulations, and policies; that resources are safeguarded; and reliable data is produced and reported. Lastly, users of the systems are to be adequately trained and appropriately supported.

Moreover, under section 9.a.3 of A-127, agencies shall ensure that "appropriate reviews" of their financial management systems are conducted. These reviews must comply with policies for (1) reviews of internal control in accordance with OMB guidance for purpose of FMFIA and Circular A-123; (2) reviews of conformance of financial management systems with Circular A-127, section 7, in accordance with OMB's FMFIA guidance; and (3) reviews of systems and security reviews under OMB Circular A-130, *Management of Federal Information Resources*. Lastly, section 9.a.4 requires agencies to issue, update, and maintain agency-wide financial management directives to reflect policies defined in the Circular (A-127).

In implementing either Circulars A-123 or A-127, OMB has provided agency heads with much discretion, since the Circulars do not contain any detailed process by which agency heads are to make their Section 4 assurances. Further, A-127 does not define or describe what is meant by "appropriate review." In any case, agencies are required to have financial management directives that address A-127's provisions.

We have not identified any OERM or FDIC written procedures on how the Section 4 assurance statement is to be supported and reported upon. Additionally, although we note that legal analyses have been prepared for Circulars A-123 and A-127, these analyses have not specifically addressed the issue of support for the statements of assurance, including the effect of reviews conducted under A-127, section 9. OERM and the CFO told us that there is no one specific document or review that would constitute the support or basis for the FDIC's assurance statement regarding FMFIA Section 4 reporting. Instead, OERM stated that the basis for the Chairman's Section 4 assertion consists of many things taken together in regard to the FDIC's core financial management system – New Financial Environment (NFE) and other systems that interface with NFE, including:

- GAO's Audit of the FDIC's Financial Statements – the audit work and the results of the audit;
- FISMA reviews and reports, including security self-assessments and the OIG's annual FISMA evaluation;
- FDIC internal control reviews; and
- The FDIC's system development life cycle processes.

We noted that GAO's financial statement audit report (*Federal Deposit Insurance Corporation Funds' 2006 and 2005 Financial Statements*, dated February 2007, GAO-07-371) omitted mention of financial management systems under FMFIA, and we confirmed with GAO that the scope of its financial statement audit did not include FMFIA Section 4 (financial management systems) reporting. While some elements of the FISMA review and internal control reviews performed by FDIC divisions and offices may touch upon financial management system aspects, such as information security, we concluded that support for Section 4 reporting was undocumented, indirect, and fragmented and could be improved.

Given the statutory nature of the FDIC's Annual Report[11], there should be adequate support behind the Chairman's statements of assurance regarding FMFIA Sections 2 and 4. To help ensure the adequacy of such support, the FDIC should develop and document procedures that consider the provisions of OMB's Circulars A-123 and A-127 and other relevant authorities, in general, and the following topics, in particular:

- what financial management systems reviews should be performed,
- the organization(s) responsible for the reviews,
- what supporting documentation is needed for the assurance statement, and
- to whom and in what manner or form the results of financial management system reviews should be reported.

A more clearly defined process for Section 4 reporting would also help ensure that the Director, OERM, has sufficient information for determining whether any weaknesses identified in the financial systems reviews need to be reflected in the Chairman's assurance statement and/or warrant reporting for purposes of OMB Circulars A-123 and Circular A-127.

[11] Federal Deposit Insurance Act, section 17, and the CFOA.

COSO ERM Framework

Monitoring:

The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or a combination of the two.

According to COSO, ongoing monitoring occurs in the normal course of management activities. The scope and frequency of separate evaluations depends primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. ERM deficiencies are reported upstream, with serious matters reported to top management and the board.

Monitoring Activities at the FDIC

Examples of monitoring of internal operations through ongoing management activities include:

- periodic reports to the COO, CFO, FDIC Chairman, and FDIC Board, detailing the use of delegated authority by FDIC staff;
- budget variance analyses and mid-year budget review; and
- assignment of oversight managers and technical monitors to procurement efforts.

Examples of separate evaluations of internal operations at the FDIC include:

- audits and studies of FDIC programs, operations, and financial statements from the GAO;
- audits and evaluations of programs and operations conducted by the OIG; and
- internal control reviews and program reviews conducted by division and office internal review units.

OERM Monitoring Activities: OERM indicated that it has conducted reviews and studies in areas such as:

- performing quality assurance work to ensure the data integrity of the Office of Diversity and Economic Opportunity case processing systems and completeness of case files,
- assisting the Privacy Program Manager in developing aspects of a privacy program,
- analyzing the number of management reports submitted to the FDIC Board and Chairman's Office, and
- reviewing DOF and DIR procedures for updates required by the implementation of Deposit Insurance Reform.

OERM also has one staff member who participates in DSC regional office reviews with DSC's Internal Control and Review Section and performs internal control reviews of DSC operations. For example, OERM provided internal control review reports related to determining: whether a regional office's published policies were current and complete; how another regional office utilized DSC Scorecard information, and how the regional office managed the accuracy of Corporate Human Resources Information System staffing tables and salary cost allocations to corporate programs.

Opportunities to Enhance ERM monitoring

Under the FDIC Bylaws, OERM also has responsibility for conducting program evaluations of the Corporation's business lines (DSC, DIR, DRR) as contemplated under GPRA. In this regard, we recommended in a recent report[12] that OERM take steps to add greater independence and structure to its program evaluation efforts, such as developing an annual evaluation schedule, defining the scope and methodology of procedures performed, and reporting recommendations for program improvements.

OERM also has desk officers who are assigned to each division and office throughout the FDIC. The desk officers indicated that they are involved in monitoring certain second-tier issues through frequent communication with their respective divisions and offices. OERM does not formally document its reviews but predominantly uses informal communication channels. The COSO ERM framework allows that many aspects of enterprise risk management are informal and undocumented, yet are regularly performed and highly effective. However, in this regard, COSO also states that an appropriate level of documentation usually makes evaluations more effective and efficient.

Finally, although the CFO indicated that he is responsible for overseeing OERM, we did not see a formal program or process for monitoring OERM's implementation of ERM. Such oversight should ensure that OERM implements ERM infrastructure and the basic components of COSO's ERM Framework and that the ERM program delivers risk management information that is useful and actionable.

Recommendations

The FDIC's overall ERM program varies in some respects from what is recommended by COSO. Although organizations have latitude and flexibility in implementing ERM to meet specific needs, the FDIC may wish to take action to more closely align corporate practices with the COSO framework and thereby maximize the effectiveness and efficiency of the various risk management activities currently in place throughout the Corporation.

1. We recommend that the Chairman further study variances between the FDIC's overall internal ERM efforts and the COSO ERM Framework as discussed in this report and take steps to address the variances where it will add value to the FDIC's ERM program. Areas for potential focus include:

    - Defining and communicating the Corporation's risk appetite and ensuring that corporate objectives are aligned with that appetite.
    - Establishing and documenting corporate-wide processes for identifying, assessing, and responding to internal risks.
    - Establishing effective channels for OERM to communicate risk management information throughout the organization, such as through periodic status reports and meetings with divisional risk management/internal review units.

[12] *Evaluation of the FDIC's Use of Performance Measures* (Report No. EVAL-07-002), dated May 2007.

- Identifying the process for monitoring the implementation of ERM through ongoing activities or separate evaluations of division and office risk management programs and OERM's enterprise risk management program.

2. We recommend that the Director, OERM, take necessary steps to develop and issue an annual assurance statement to the Chairman related to the ERM program and other OERM responsibilities.

3. We recommend that the Director, OERM, coordinate with the Legal Division to review section 4 reporting requirements to determine the FDIC's reporting responsibilities.

4. Based on the results of recommendation 3, we recommend that the Director, OERM, issue guidance for FMFIA section 4 reporting and the work required to support an assertion on financial management systems.

Structure of the FDIC's Internal ERM Program

Implementing ERM: ***An entity's size, complexity, industry, culture, management style, and other attributes will affect how the framework's concepts and principles are most effectively and efficiently implemented.***

The COSO ERM Framework notes that organizations implement ERM differently, but indicates there are common broad-based steps taken by entities that have successfully implemented ERM, such as conducting a current state risk assessment, developing an entity-wide ERM vision, and ensuring capability development, which includes defining roles and responsibilities; policies, processes, tools, techniques, information flows and technologies; and competencies. These capabilities are also collectively known as the ERM Infrastructure. Table 1 presents some common elements of ERM infrastructure.

Table 1: Common Elements of ERM Infrastructure

ERM Infrastructure Elements	
• CEO commitment (tone and message from the top), • Risk policies and/or mission statements, including adapting any company risk or audit committee charter to incorporate ERM, • Reporting to business units, executives, and the board, • Adoption or development of a risk framework, • Adoption or development of a common risk language,	• Techniques for identifying risk, • Tools for assessing risks, • Tools for reporting and monitoring risks, • Incorporating risk into appropriate employees' job descriptions and responsibilities, • Incorporating risk into the budgeting function, and • Integrating risk identification and assessment into the strategy of the organization.

Source: Institute of Management Accountants, Statement on Management Accounting, *Enterprise Risk Management: Tools and Techniques for Effective Implementation*, 2007.

The FDIC's Bylaws state that the Director, OERM, is responsible for administering the enterprise-wide risk management program that monitors and manages risks by maintaining partnerships with the divisions and offices, providing training, and addressing internal control deficiencies. Among other things, the Bylaws provide that the Director, OERM, shall:

- develop policies and procedures for the development, maintenance, and evaluation of a comprehensive ERM program;
- design and implement corporate-wide ERM training programs;
- conduct outreach activities to explore best practices found in public and private sectors;
- conduct corporate internal control reviews; and
- serve as the risk manager for certain large IT projects that fall under the CIRC.

In addition, the Position Description for the Director, OERM, includes the following duties:

- designing OERM's governance model for internal risk;
- establishing policies and procedures to manage enterprise-wide internal risk;

- developing an integrated risk management program for the FDIC that entails identifying, prioritizing, measuring, monitoring, and managing/controlling the most material internal control and operating/other risks facing the Corporation;
- developing risk quantification techniques that facilitate appropriate risk/reward choices across the organization;
- implementing a consistent risk management framework across FDIC business areas and developing, implementing, and measuring the effectiveness of appropriate risk mitigation strategies; and
- developing and providing appropriate briefing material to the Chairman and Board.

In general, more needs to be done if the Corporation wants to establish an ERM infrastructure as envisioned in the Bylaws and the Position Description for the Director, OERM, particularly in the areas of defining roles and responsibilities, developing procedures and guidance, and developing corporate-wide ERM training programs.

Roles and Responsibilities

The CFO told us that he is responsible for overseeing OERM; however, the FDIC has chosen not to formally establish roles and responsibilities for overseeing the internal ERM Program, specifically the roles that the FDIC Chairman, the FDIC Board, and the Audit Committee should play. Such oversight could help ensure that OERM implements ERM infrastructure and the basic components of COSO's ERM Framework and that the ERM program delivers risk management information that is useful and actionable.

Chairman and Board: The COSO ERM Framework notes that the Chief Executive Officer (CEO) is ultimately responsible and should assume ownership of ERM. This includes seeing that all components of ERM are in place. The CEO generally fulfills this duty by:

- providing leadership and direction to senior managers, including developing the entity's risk management philosophy, risk appetite, and culture, and
- meeting periodically with senior managers to gain knowledge of risks inherent in operations, risk responses, control improvements required, and the status of ERM efforts under way.

The COSO ERM Framework notes that the Board provides important ERM oversight by:

- knowing the extent to which management has established effective ERM;
- being aware of, and concurring with, the entity's risk appetite;
- reviewing the entity's risk portfolio and considering it against the entity's risk appetite; and
- being apprised of the most significant risks and whether management responds appropriately.

Neither the Bylaws nor the FDIC's ERM policy specifies the role of the Chairman or the FDIC Board in implementing or overseeing internal ERM. Further, the Director, OERM, stated that the FDIC Board does not have a role in internal ERM because the Board's focus is on external

risks facing the Corporation. We believe that the Chairman and the FDIC Board should have clearly-defined roles in ERM as suggested by the COSO ERM Framework. We also note that the COSO approach is consistent with what the FDIC expects of boards of directors for FDIC-supervised financial institutions. Specifically, an FDIC corporate governance presentation for new bank directors states that board member responsibilities include identifying the risk profile for the institution and establishing a risk appetite and risk framework within which to identify, measure, monitor, and control the risks of the institution.

Audit Committee: The COSO ERM Framework notes that it is not uncommon for oversight responsibility for ERM to be assigned to the audit committee. COSO notes that with its focus on internal control over financial reporting, and possibly a broader focus on internal control, the audit committee already is well positioned to expand its responsibility to overseeing ERM.

OMB Circular A-123 also encourages agencies to consider establishing a Senior Management Council to assess and monitor deficiencies in internal control. Such councils generally recommend to the agency head which reportable conditions are deemed to be material weaknesses to the agency as a whole and may be responsible for (1) overseeing the timely implementation of corrective actions related to material weaknesses and (2) determining when reportable conditions or material weaknesses have been corrected.

The FDIC established an Audit Committee as a Standing Committee to the Board. The delegation of authority establishing the FDIC Audit Committee includes, among other things, the following responsibilities:

- overseeing the Corporation's financial reporting and internal controls,
- reviewing and approving management's annual plan for compliance with the CFOA, and
- assessing the sufficiency of the Corporation's internal control structure.

OERM's Circular 4010.3 does not address whether the Audit Committee plays a role in overseeing ERM or internal control program efforts. OERM's Web site does indicate that the Audit Committee reviews and discusses OERM activities and we have observed this on occasion. Accordingly, considering the Audit Committee for a broader oversight role would be consistent with the COSO ERM Framework, OMB Circular A-123, and Audit Committee practices.

OERM's Role and Responsibilities: As discussed throughout this report, we identified variances between the requirements for the OERM Director's position as outlined in the FDIC Bylaws and the day-to-day operations of OERM. Many of OERM's efforts relate to serving in an audit liaison capacity and monitoring the status of on-going audits and corrective actions taken in response to audit recommendations. Secondarily, we observed that OERM provides assistance to other divisions and offices as needed to work on special projects, such as the Privacy Program developed by DIT and the Deposit Insurance Reform initiative.

The OERM Director and OERM staff described much of their risk management efforts as consisting of meetings and/or briefings with division and office staff on specific topics of interest. Thus, much of our understanding of OERM's risk management efforts is based on

testimonial evidence as opposed to documentary evidence. Nevertheless, the CFO and COO indicate that they are pleased with OERM's contribution to risk management and key internal initiatives. Given the differences between the Bylaws description of OERM responsibilities and OERM's actual efforts, we are suggesting that the FDIC reconcile the two to promote a common understanding of OERM's risk management role and responsibilities.

Policies and Procedures

OERM has issued high-level policy related to ERM, but OERM could do more to provide detailed procedures and guidance related to methodologies, models, and systems that divisions and offices should use in identifying, assessing, mitigating, and reporting risk information. For example, Circular 4010.3 sets forth policy[13] related to implementing an ERM Program, stating that every FDIC operating and policy area should possess the following fundamental requirements:

- current and documented procedures,
- reasonable controls incorporated into those procedures,
- employees trained in the proper execution of their duties, and
- supervisors and managers who are both empowered and held accountable.

Further, the policy indicates that each manager should:

- identify key activities within his or her area of responsibility,
- seek to determine what impediments (risks) might threaten the ability to achieve success,
- evaluate the impediments in terms of likelihood of occurrence and potential impact, and
- take actions as deemed necessary to mitigate risk.

Further, OERM issues guidance to divisions and offices annually related to preparing assurance statements on the adequacy of internal and management/financial system controls. OERM has also issued guidelines to OERM staff serving as risk managers on CIRC projects.

However, OERM has not issued implementing procedures or guidance to assist divisions and offices in implementing ERM. According to OERM, it is up to individual division and office managers to decide how best to implement ERM. As presented in Appendix II, we saw differences in divisions' and offices' ERM programs. Most were still using traditional "accountability unit" approaches which are based on functional areas, as opposed to the identification, assessment, and mitigation of risks emanating from strategic objectives.[14] Further, one division and one office expressed a need for guidance from OERM. With clear, uniform guidance, OERM could increase consistency in FDIC divisions and offices' approach to internal ERM.

---

[13] The circular also lists GAO's *Standards for Internal Control in the Federal Government* and other OERM program responsibilities such as coordinating the annual assurance statement and performing audit follow-up and resolution activities.

[14] It should be noted that Circular 4010.3 does suggest that key activities, from a broad perspective, could be tied to CPOs.

In our view, Circular 4010.3 does not meet the level of detailed procedures contemplated in the Bylaws, the Position Description for the OERM Director, or the COSO ERM Framework. Moreover, OMB Circular A-123 notes that agency management should have a clear, organized strategy with well-defined documentation processes that contain an audit trail, verifiable results, and specify documentation retention periods so that someone not connected with the procedures can understand the assessment process.

OERM officials told us that they have made no decision in regard to issuing additional ERM directives or policy. OERM indicated that it had planned to issue procedures for special projects and studies, but OERM told us it had not made progress on this initiative due to other competing priorities. We did note that OERM updated its Web site in August 2007.

Training Programs

OERM has not designed and implemented corporate-wide ERM training programs, as required by the FDIC Bylaws. Competency development is one of the elements of ERM infrastructure and is important in ensuring that entity employees speak and understand a common risk management language and that people with the requisite knowledge, expertise, and experience are put in place to implement the ERM function.

OERM assisted the FDIC's Legal Division in presenting ERM training to Legal Division managers but could do more to provide ERM training to other divisions and offices. The Director, OERM, also indicated that he has spoken about ERM at several divisional conferences; however, OERM could not provide detailed information about the content of the OERM Director's speaking engagements.[15]

The Institute of Management Accountants has issued Statements on Management Accounting related to ERM frameworks and implementing ERM.[16] Table 2 presents examples of ERM-related training topics.

Table 2: Examples of ERM-Related Training Topics

• Understanding the nature of risk • Understanding risk management legal and regulatory requirements • Knowledge of ERM frameworks • Facilitation skills • Expertise in identifying risks • Knowledge in building risk maps • Reporting structures and options (what to report to the CEO, board, and audit committee)	• Software training • Financial risk training (options, hedging strategies, insurance options, derivatives, etc.) • Refocused strategy training and how risk interacts with strategy • Building and understanding control solutions • Developing and monitoring performance metrics related to risks • Change management

Source: Institute of Management Accountants, Statement on Management Accounting, *Enterprise Risk Management: Tools and Techniques for Effective Implementation*, 2007.

[15] OERM's Web site indicates that OERM has developed ERM and internal control training programs that are open to all division and office staff.

[16] *Enterprise Risk Management: Frameworks, Elements, and Integration*, 2006, and *Enterprise Risk Management: Tools and Techniques for Effective Implementation*, 2007.

We are recommending that OERM take steps to add greater structure to the ERM program in the form of defined roles and responsibilities, detailed procedures, and corporate-wide training programs.

Maturity Level of the FDIC's Internal ERM Program

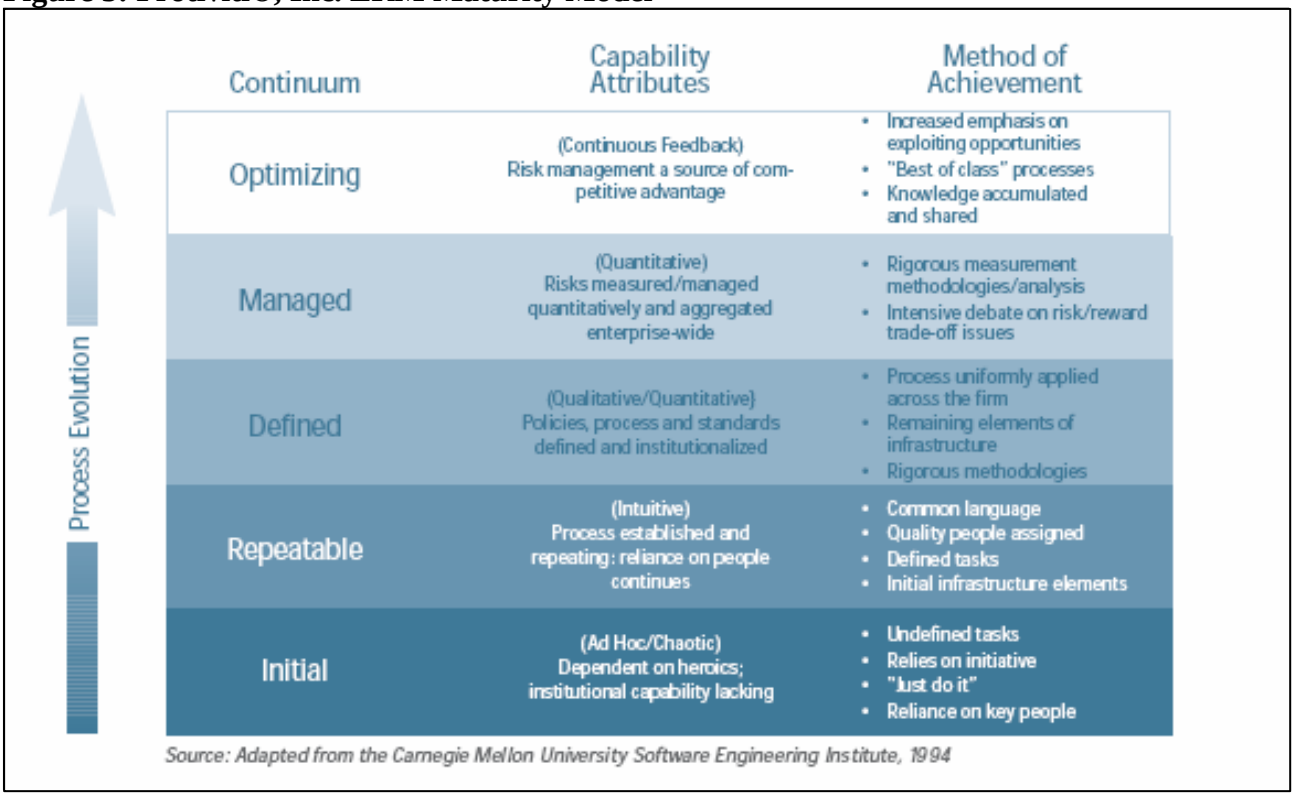
A number of organizations recognize the importance of using ERM maturity models to assess an organization's progress and status in implementing ERM. The Institute of Internal Auditors issued an article[17] stressing that maturity models should be easily understandable by management and should address the key components of best-practice ERM frameworks. The article identifies areas usually covered in maturity models, including the following:

- Extent of leadership awareness within the organization.
- Alignment of business objectives with risks and action plans.
- Extent to which risk management roles and responsibilities of all employees are articulated.
- Extent of communication and training on ERM.
- Rigor of monitoring and management oversight of employees and committees.

We evaluated the status of the FDIC's internal ERM program as administered by OERM against an ERM capability maturity model developed by Protiviti®, Inc. The model provides a framework for evaluating the maturity of an organization's risk management capabilities and ranking those activities on a continuum of five stages of maturity from an *Initial State* to an *Optimizing State*. Figure 3 presents the stages, attributes, and methods of achievement for the maturity model.

[17] *Moving Forward with ERM*, published in the Institute of Internal Auditors' June 2007 issue of *Internal Auditor*.

Figure 3: Protiviti®, Inc. ERM Maturity Model



Source: Protiviti®, Inc.

The capability maturity model can be used to target needed risk management capability improvements in six elements of ERM infrastructure suggested by Protiviti®, Inc.: (1) Business Policies, (2) Processes, (3) Competencies (people and organization), (4) Management Reports, (5) Methodologies, and (6) Systems and Data. To illustrate, at the *Initial State*:

- Business policies are undocumented or vague.
- Business processes are informal and reactionary.
- There is very little accountability either because a clearly designated risk owner has not been identified or there are so many owners of risk that no one can be held accountable.
- Management reports are sporadic, ad hoc, and informal.
- Methodologies are over-simplified.
- Systems and data quality are poor.

Attributes of risk management capabilities at the *Repeatable State* include the following:

- Business plans and risk policy are articulated, and policy is being followed.
- Policies are documented and process gaps are being identified and corrected.
- Risk owners are clearly defined and supported with staff, roles and commitments are explicitly defined and understood, and people are trained in the process.
- Regular actionable reports are issued consistently and timely.
- Risk measures are improved but not yet integrated, and a mechanism is in place to capture process and methodology improvements.

- Systematic data collection exists for a few risks and is facilitating improved reporting and increasing overall confidence in management reports.

Maturity Assessment of the FDIC's Internal ERM Program

We concluded that the internal ERM program is in the *Initial State*, but possesses certain attributes of the *Repeatable State*, the second level of maturity. Generally, characteristics of the *Repeatable State* include a basic policy structure, basic risk management processes, and basic control activities, which, as we previously reported, the internal ERM program possesses. However, the *Repeatable State* is also described as having explicitly defined and understood roles and commitments, people trained in the ERM process, independent spreadsheet models, and regular actionable reports—areas in which the FDIC's ERM Program has not progressed as far since the FDIC established the program in May 2004. Protiviti®, Inc., notes that while there are concrete things any organization can do that will make an impact on ERM within 12 months, it estimates that most organizations will require from 3 to 5 years to accomplish their objectives in fully implementing their ERM solution.

Recommendations

OERM is responsible for administering a comprehensive ERM program at the FDIC. However, we noted that OERM's activities and focus vary from the FDIC Bylaws and policy governing the Corporation's ERM program. We are making the following recommendations to help OERM achieve attributes of a more mature ERM program.

5. We recommend that the Chairman clarify the roles and responsibilities of the Chairman, the Board, and the Audit Committee in relation to the FDIC's ERM program. We also suggest that the Chairman reconcile OERM's current operations with the Bylaws and determine whether the Bylaws should be revised or whether OERM should expand certain aspects of its operations.

6. We recommend that the Director, OERM, draft and issue detailed procedures for a comprehensive ERM program as envisioned in the Corporate Bylaws.

7. We recommend that the Director, OERM, take steps to develop and present corporate-wide training to FDIC employees on the ERM program as envisioned in the Corporate Bylaws.

Other Matter for Consideration: Integrating Enterprise Risk Management at the FDIC

According to COSO, enterprise risk management requires an entity to take a portfolio view of risk. This means considering activities at all levels of the organization -- from enterprise-level activities such as strategic planning to business unit activities and business processes.

As COSO notes, ERM requires management to consider interrelated risks from an entity-level portfolio perspective. Risks for individual units of the entity may be within the units' risk tolerances but, taken together, may exceed the risk appetite of the entity as a whole. With a composite view at each succeeding level of the organization, senior management is positioned to determine whether the entity's overall risk portfolio is commensurate with its risk appetite.

Enterprise Risk Management at the FDIC

As discussed throughout this report, FDIC business line divisions (DIR, DSC, DRR) are primarily responsible for managing external risks, while OERM focuses principally on internal risks.

External Risk Management: During a recent study of the FDIC,[18] GAO reported that the FDIC has an extensive system for assessing and monitoring external risks. GAO noted that in addition to its supervisory oversight of individual institutions, the FDIC conducts a wide range of other activities to monitor and assess risk at a broader level, from a regional perspective to a national view. Specifically, the FDIC's risk assessment and monitoring process includes input from the:

- Regional Risk Committees, which evaluate regional economic and bank trends and risks;
- National Risk Committee (NRC), which meets monthly to identify and evaluate the most significant external business risks facing the FDIC and the banking industry;
- Risk Analysis Center, which is an interdivisional forum for discussing significant, cross-divisional, risk-related issues and which provides reports and analysis to the NRC;
- Financial Risk Committee, which quarterly recommends an amount for the Deposit Insurance Fund's contingent loss reserve—the estimated probable loss attributable to failure of institutions in the coming 12 months; and
- DIR, which has a leading role in delivering a key set of semiannual reports[19] that the Board uses as a basis for setting the Deposit Insurance Fund's premium (deposit insurance assessments) schedule.

[18] *Federal Deposit Insurance Corporation: Human Capital and Risk Assessment Programs Appear Sound, but Evaluations of Their Effectiveness Should be Improved* (GAO-07-255, February 2007).

[19] These key reports include the Risk Case, which summarizes national economic conditions and banking industry trends and discusses emerging risks in banking, and the Rate Case, which recommends a premium schedule based on analysis of likely losses to the fund from failures; growth of insured deposits; investment income; and other factors.

GAO also noted that the FDIC has developed broad plans and specific strategies for handling an increase in troubled or failed institutions. In this regard, the Resolution Policy Committee[20] is responsible for developing plans to handle potential or actual failure of the largest institutions, and DRR has created a detailed blueprint for managing the failure of a large institution.

GAO concluded that the FDIC could do more to monitor and evaluate its external risk management activities. GAO also reported that an unclear line of responsibility could be contributing to weaknesses in some of the FDIC's evaluations of its risk activities and suggested that the FDIC would benefit by designating official(s) or an office, or establishing procedures, to ensure that evaluation and monitoring of risk activities are conducted regularly and comprehensively. GAO recommended developing policies and procedures that clearly define how the FDIC will systematically evaluate and monitor its risk assessment activities and ensure that required evaluations are conducted in a comprehensive and routine fashion. In response, the FDIC indicated that an interdivisional committee would perform an in-depth review of its current risk assessment activities and evaluation procedures.

Internal Risk Management: As discussed throughout this report, OERM is responsible for internal enterprise risk management at the FDIC. In this regard, the CFO issued an e-mail to all FDIC employees in April 2004, on the subject of *Office of Enterprise Risk Management*, which stated:

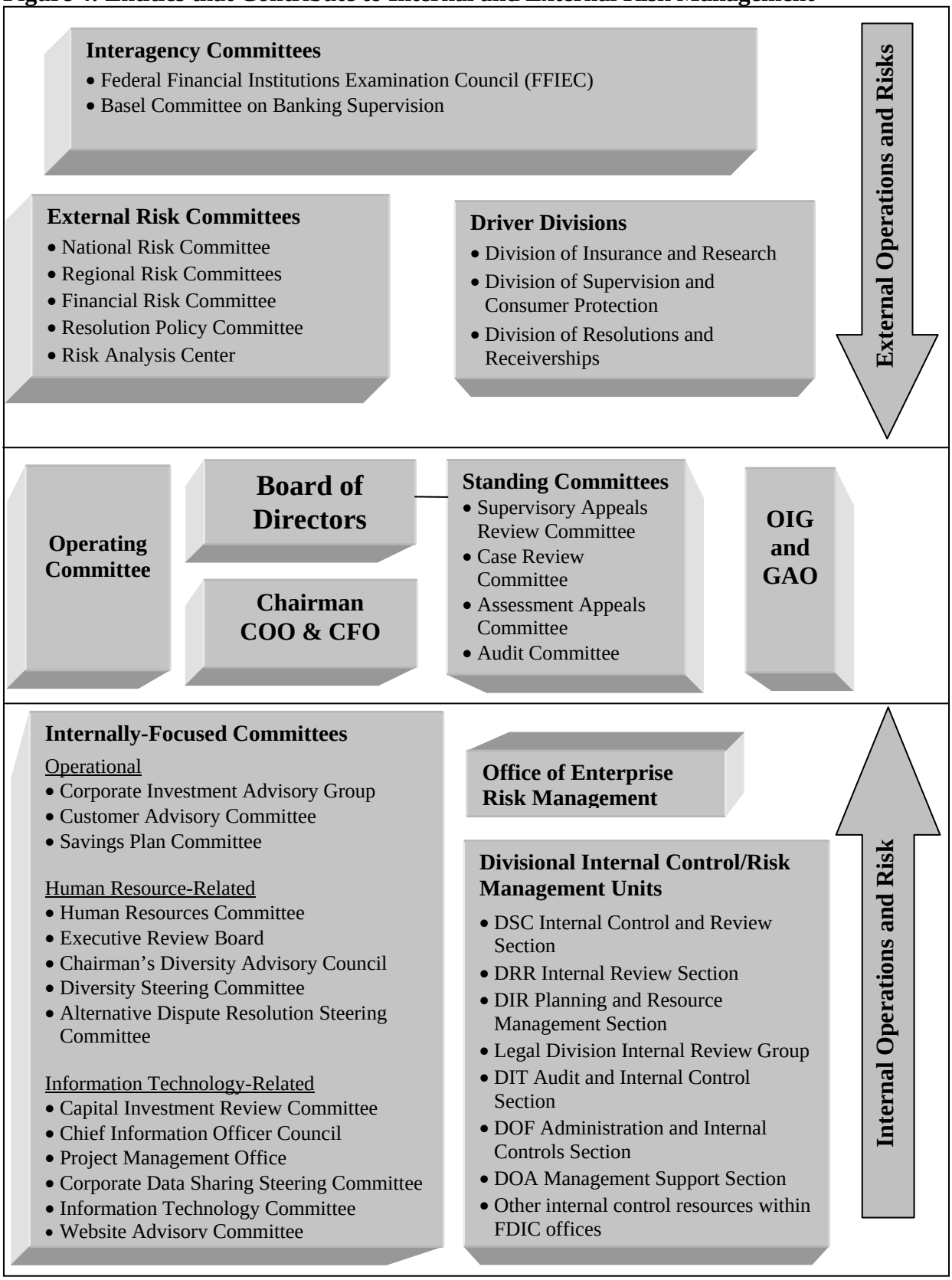
> Effective immediately, the name of the **Office of Internal Control Management** (OICM) is changed to the **Office of Enterprise Risk Management** (OERM). A review of risk management best practices in the public and private sectors found that internal controls have evolved to a more proactive and enterprise-wide approach. The proactive approach focuses on the identification, quantification, and mitigation of risk, instead of the traditional control evaluation and audit tracking model. We firmly believe this is the appropriate direction in which the OERM should proceed.
>
> Unlike many other organizations that manage *all* risk, both internal and external to the entity, the OERM will focus principally on risks internal to the FDIC, such as serving as the Risk Manager for several of the largest Information Technology (IT) projects which fall under the Capital Investment Review Committee (CIRC). External risk management will continue to be the primary responsibility of DIR, DSC, DRR, and other divisions and offices throughout the Corporation.

OERM carries out its internal ERM role by meeting with division and office representatives to discuss internal control issues, conducting internal control reviews—mostly of internal corporate issues, serving as a risk management advisor on large IT projects, and coordinating the annual assurance statement process.

Figure 4 on the next page illustrates our understanding of the entities that contribute to the FDIC's external and internal risk management activities.

[20] Resolution Policy Committee members are: the COO (serves as chair), CFO, General Counsel, and Directors of DSC, DIR, and DRR.

Figure 4: Entities that Contribute to Internal and External Risk Management



Source: OIG Analysis

Opportunities to Enhance ERM at the FDIC

As discussed above, the FDIC ERM Program is limited to internal FDIC operations, by design. This approach is contrary to the fundamental COSO ERM Framework tenet that ERM should be applied across the enterprise, at every level and unit, and should include taking an entity-level portfolio view of risk. Without an enterprise-wide view of risk, the FDIC may not be in a position to align and integrate varying views of risk management across the organization or effectively assess systemic risks.

We are suggesting that the FDIC consider whether the Corporation's internal and external risk management activities should be integrated and, if so, ensure that such integration is done efficiently and effectively.

CORPORATION COMMENTS AND OIG EVALUATION

After discussing the draft report findings, suggestions, and recommendations with the Chairman, management provided us a written response, dated October 18, 2007. As noted in management's response, we provided an executive briefing to the Chairman and senior officers of the Corporation on September 26, 2007, regarding our draft report. The Inspector General further discussed our recommendations with the CFO and Chairman subsequent to the executive briefing. Management's response is presented in its entirety in Appendix II. Appendix III contains a summary of management's responses to our recommendations.

It is important to note that, as discussed in management's response, if there is an unresolved dispute between management and the OIG on any given audit report recommendation, the Audit Committee provides input to the Chairman, who makes all final determinations regarding such disputes in her role as the FDIC's Audit Follow-Up Official (AFO). Accordingly, in this instance, because the Chairman has been involved in the response process, management's written comments constitute the FDIC's final determinations regarding the suggestions and recommendations in our draft report.

In its written response, management indicated that over the past 4 years, the Corporation has diligently sought to streamline and improve the integration and effectiveness of its internal risk management processes, employing a number of "best practices" and generally following the GAO blueprint outlined in GAO's 2005 testimony before the Subcommittee on Government Management, Finance, and Accountability/Committee on Government Reform, entitled, *Financial Management: Effective Internal Control is Key to Accountability*.

The response further noted that management gave careful thought to the seven recommendations in our report, as well as the two suggestions we offered. After discussions with the Chairman, management stated that it intends to adopt certain items in the draft report and has alternative actions underway that may address some of the concerns underlying these recommendations and suggestions.

The Corporation's response to the recommendations and suggestions is summarized below, together with our evaluation of the response. The recommendations and suggestions are presented in the same order as they appear earlier in the report.

FDIC Committees and Groups that Contribute to Internal Risk Management: We suggest that the Chairman's Office, in coordination with the COO and the CFO, articulate and document how the various committees and groups interrelate in managing internal risk.

Management's response indicated that the COO and the CFO will look at developing a more comprehensive blueprint to enhance the coordination and documentation of these committees and groups, where appropriate, during 2008.

We agree with management's planned action.

Recommendation 1: We recommend that the Chairman further study variances between the FDIC's overall internal ERM efforts and the COSO ERM Framework as discussed in this report and take steps to address the variances where it will add value to the FDIC's ERM program.

Management stated in its response that it agreed that there is value to more clearly defining and communicating the Corporation's risk appetite and ensuring that corporate objectives are aligned with this appetite. The Chairman's office will be considering a variety of vehicles to do this for 2008 and beyond, such as developing a corporate risk statement to accompany the planning and budgeting process that produces Corporate Performance Objectives. Further, management stated that it believes there is merit to exploring improved communication channels regarding internal risk management and will look for opportunities to add value and enhance these channels, including the possible augmentation of certain existing reports and/or expanding Audit Committee and other management briefings.

We agree with management's planned action.

Recommendation 2: We recommend that the Director, OERM, take necessary steps to develop and issue an annual assurance statement to the Chairman related to the OERM program and other OERM responsibilities.

Management stated in its response that OERM is an extension of the CFO's office and, by design, needs to maintain a certain level of independence for the annual assurance statement process. Management described OERM's quality assurance role in that process and stated that it believes the substance of this process is more effective than just having OERM sign a statement to the Chairman.

We accept management's response and consider this recommendation closed. However, we maintain that it would be prudent for OERM, consistent with all other divisions and offices, to provide documented assurance to the Chairman that its own program is achieving, or assisting other divisions and offices in achieving, all relevant control objectives.

Recommendation 3: We recommend that the Director, OERM, coordinate with the Legal Division to review section 4 reporting requirements to determine the FDIC's reporting responsibilities.

Recommendation 4: Based upon the results of recommendation 3, we recommend that the Director, OERM, issue guidance for FMFIA section 4 reporting and the work required to support an assertion on financial management systems.

Management stated in its response that the FDIC's responsibilities under Section 4 of FMFIA are clear: the FDIC must provide a statement of assurance as to whether or not its financial management systems, including its internal controls, are effective. Management further stated that it believes that OMB Circulars A-11, A-123, A-127, A-130, FFMIA, and FISMA provide additional variables to consider in determining what the Corporation must do to fulfill its responsibilities in these matters. According to management, while only a portion of this body of guidance directly applies to the FDIC from a legal perspective, management has coordinated with the Legal Division over the years and developed an integrated approach for providing assurance that it believes more than satisfies the letter (as applicable) and the spirit of the requirements. Finally, the FDIC believes that its process for assurance reporting emphasizes substance over form and has been successfully integrated into the day-to-day management of DOF, DIT, and others in the FDIC who have a role in NFE.

We noted that management's response detailed the FDIC's efforts to meet the requirements of Section 4 and OMB Circular A-127, *Financial Management Systems*, in a comprehensive manner that did not exist when we conducted our evaluation. This newly documented framework is a positive step toward meeting the intent of report recommendations 3 and 4. However, we believe it would be prudent for the FDIC to establish this framework formally outside of management's response to this evaluation. As noted in the report and in management's response, we and the Corporation have received different information regarding GAO's position on the scope of its financial statement audit as it relates to coverage of Section 4, financial management systems. We encourage the CFO and OERM—possibly in conjunction with the Audit Committee—to formally discuss this matter with GAO so that all parties are in agreement on the scope of the 2008 financial statement audit regarding Section 4 coverage. We would also suggest that the FDIC include discussion of Section 4, financial management systems, in FDIC management's assertions to GAO. These assertions help to form the basis and scope of the financial statement audit.

As discussed above, we believe that the FDIC should take further action to address Recommendations 3 and 4. As a result, we disagree with management's decision on these recommendations. However, because the Chairman as the FDIC's AFO has already been consulted on and concurred with management's response, we will not be pursuing the recommendations any further and consider them closed.

Recommendation 5: We recommend that the Chairman clarify the roles and responsibilities of the Chairman, the Board, and the Audit Committee in relation to the FDIC's ERM program. We also suggest that the Chairman reconcile OERM's current

operations with the Bylaws and determine whether the Bylaws should be revised or whether OERM should expand certain aspects of its operation.

Management stated in its response that it would clarify the roles of the Chairman, the Board, and the Audit Committee in relation to the FDIC's ERM program. We agree with management's planned action on this aspect of the recommendation. The Corporation's response to reconciling OERM's current operations with the Bylaws is discussed further in Recommendations 6 and 7.

Recommendation 6: We recommend that the Director, OERM, draft and issue detailed procedures for a comprehensive ERM program as envisioned in the Corporate Bylaws.

Recommendation 7: We recommend that the Director, OERM, take steps to develop and present corporate-wide training to FDIC employees on the ERM program as envisioned in the Corporate Bylaws.

Management stated in its response that it recognizes the need for a comprehensive ERM program; the OIG's concern about consistent, detailed internal control procedures at the Division/Office level; and the benefits of appropriate training to meet the needs of the FDIC. However, management does not believe that there are any discrepancies between OERM's current operation and the respective Bylaws, and management continues to fully support OERM's efforts in developing and implementing a comprehensive ERM program and appropriate training program. Management's response described various OERM activities that it believes provide for a consistent internal control framework across the Corporation.

We contend that an effective and efficient ERM program begins with a sound and mature ERM infrastructure. As discussed in our report, OERM has not:

- Established procedures for the development, maintenance, and evaluation of a comprehensive ERM program: In this regard, our report notes several sources of criteria beyond the Bylaws that call for a well-defined and documented risk management program. For example, OMB Circular A-123, *Management's Responsibility for Internal Control*, notes that agency "...management should have a clear, organized strategy with well-defined documentation processes that contain an audit trail, verifiable results, and specify documentation retention periods so that someone not connected with the procedures can understand the assessment process." As discussed in our report, we saw limited implementing procedures for the internal risk management program and few recommended tools or techniques for identifying, assessing, and reporting risks. Further, as one consequence of the lack of established procedures, we found inconsistent practices between the various divisional internal review units.

- Designed and implemented corporate-wide ERM training programs: Our report notes that competency development is a key element of ERM infrastructure and that it is important to ensure that employees speak and understand a common risk management language and have the knowledge and skills to implement the ERM program. The Corporation's response indicates that training and development programs are available and notes that OERM encourages divisions and offices to contact OERM if there is a need for training. We agree

that the OERM Web site states that training related to ERM, internal control, and assurance statements is available at divisions', offices' or individuals' request. However, OERM provided few examples of divisions or offices that had actually received training.

Our evaluation concluded that OERM's internal risk management program was at a relatively low level of maturity, in part because of a lack of procedures and formal training programs. During a discussion of the results of our review, the CFO and COO stated that they generally agreed with our maturity assessment. Thus, we disagree with the Corporation's response to Recommendations 6 and 7, which were intended to assist the FDIC in increasing the maturity level of its internal risk management program. As with Recommendations 3 and 4, because the Chairman as the FDIC's AFO has concurred with management's response, we will not pursue the recommendations further. We consider the recommendations closed but will look for opportunities to engage in a continuing dialogue with the Corporation regarding the maturity of its ERM infrastructure.

Opportunities to Enhance ERM at the FDIC: We are suggesting that the FDIC consider whether the Corporation's internal and external risk management activities should be integrated and, if so, ensure that such integration is done efficiently and effectively. Doing so would be consistent with the fundamental COSO ERM Framework tenet that ERM should be applied across the enterprise, at every level and unit, and should include taking an entity-level portfolio view of risk.

In its response, management stated that the COSO ERM Framework is not appropriate for universal application to the FDIC. Management further stated that rather than focusing on housing all external and internal risk management activities in one office or under one person, the FDIC utilizes a risk matrix approach, with virtually all risk management activities reporting to either the COO and/or CFO, on behalf of the Chairman. Further, according to the response, these activities are optimized by extensive communication channels upward and throughout the FDIC, and are directly linked into the FDIC's corporate planning, budget, and performance measurement process.

As noted in the report, we did not do extensive work in this area. In addition, management's planned action to develop a more comprehensive blueprint to enhance the coordination and documentation of committees and groups involved in risk management will help ensure integration exists, where appropriate. Further, in response to GAO's Report No. GAO-07-255, referred to earlier in our report, the FDIC formed a committee to review its risk management activities and evaluation procedures, make recommendations for strengthening the Corporation's risk management framework, and establish a plan for implementing the committee's recommendations. Therefore, we accept management's position on this suggestion.

Tracking Management's Planned Actions. At a November 2007 meeting between the FDIC Chairman and the Inspector General, the Chairman committed to tracking those corrective actions agreed to by management. Accordingly, management's planned actions in response to (1) our suggestion regarding documenting how the various committees and groups interrelate in managing internal risk and (2) Recommendations 1 and 5 should be included in the Corporation's Internal Risks Information System, along with expected completion dates.

Objective, Scope, and Methodology

The objective of our review was to assess (1) the extent to which the FDIC has implemented an enterprise risk management program consistent with applicable government-wide guidance and (2) OERM's implementation of FDIC Circular 4010.3, *FDIC Enterprise Risk Management Program*, dated September 25, 2006. To accomplish our objective, we assessed:

- the extent to which the FDIC's enterprise risk management program addresses Office of Management and Budget Circular A-123, *Management's Responsibility for Internal Control*, dated December 21, 2004, and the Treadway Commission's Committee of Sponsoring Organizations report entitled *Enterprise Risk Management – Integrated Framework* (September 2004), and
- OERM's administration of, and FDIC division and office participation in, the FDIC's enterprise risk management program.

Scope and Methodology

We performed field work in the FDIC divisions and offices located in Washington, D.C., and Arlington, Virginia. We performed our evaluation from December 2006 through June 2007, in accordance with the *Quality Standards for Inspections*. To accomplish our objective, we performed the following:

We identified and reviewed pertinent sections of applicable laws, regulations, and other criteria on Enterprise Risk Management:

- Budget and Accounting Procedures Act of 1950, which includes the Accounting and Auditing Act of 1950.
- Federal Deposit Insurance Act.
- Federal Managers' Financial Integrity Act of 1982 (FMFIA).
- Chief Financial Officers Act of 1990 (CFO Act).
- Government Performance and Results Act of 1993 (GPRA).
- Federal Financial Management Improvement Act of 1996 (FFMIA).
- Reports Consolidation Act of 2000.
- Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*, dated December 21, 2004, effective for Fiscal Year 2006.
- OMB Circular A-127, *Financial Management Systems*.
- GAO *Standards for Internal Control in the Federal Government*, November 1999 (GAO/AIMD-00-21.3.1).
- FDIC Directive 4010.3, *FDIC's Enterprise Risk Management Program*, dated September 25, 2006.
- COSO *Enterprise Risk Management -- Integrated Framework*, September 2004.
- FDIC Bylaws dated February 22, 2005.

We researched and reviewed:

- GAO Report No. GAO-05-321T, *Financial Management: Effective Internal Control Is Key to Accountability*, February 16, 2005.
- GAO Report No. GAO-05-881, *Financial Management: Achieving FFMIA Compliance Continues to Challenge Agencies*, September 2005.
- GAO Report No. GAO-07-255, *Federal Deposit Insurance Corporation: Human Capital and Risk Assessment Programs Appear Sound, but Evaluations of Their Effectiveness Should Be Improved*, February 2007.
- November 23, 2005 Memorandum from the Director, OERM, to Division and Office Directors Regarding Update on ERM in the FDIC.
- OERM Guidance for Assurance Statements, 2005, 2006, and 2007.
- Office of Internal Control Management *FDIC Internal Control and Risk Management Manual*, April 1998.

We reviewed the FDIC's:

- 2005-2010 Strategic Plan.
- 2006 and 2007 Annual Performance Plans.
- 2003, 2004, 2005, 2006 Annual Reports.
- 2006 Annual Assurance Statements from Divisions and Offices.

We obtained and reviewed the prior related OIG reports:

- *Evaluation of the FDIC's Use of Performance Measures*, (Evaluation Report Number EVAL-07-002), dated May 2007.
- *Strategies for Enhancing Corporate Governance*, (Audit Report Number 04-032), dated September 3, 2004.

We interviewed Internal Control Liaisons and internal review officials in all divisions and two offices to inquire about their respective risk management programs and activities, and we reviewed and analyzed material provided by the officials we interviewed.

We met with Office of Thrift Supervision and OCC officials to obtain best practice information regarding their respective risk management programs.

We researched and reviewed *Guide to Enterprise Risk Management: Frequently Asked Questions*, prepared by Protiviti®, Inc., dated January 2006. We also reviewed a Protiviti®, Inc. publication entitled, *Enterprise Risk Management: Practical Implementation Ideas*.

We reviewed the Institute of Management Accountants' Statements on Management Accounting entitled, *Enterprise Risk Management: Frameworks, Elements, and Integration*, 2006 and *Enterprise Risk Management: Tools and Techniques for Effective Implementation*, 2007. We reviewed the Institute of Internal Auditors publication entitled, *The Audit Committee: A Holistic View of Risk.*

Evaluation of Internal Controls

We gained an understanding of relevant control activities within the FDIC's ERM Program by reviewing:

- organization charts,
- policies stipulated in FDIC Circular 4010.3,
- procedures outlined in guidance issued annually to divisions and offices in regard to annual assurance statements, and
- the assurance statement process.

Laws and Regulations and Fraud and Illegal Acts

We reviewed the various statutes and implementing regulatory guidance identified in this report for purposes of determining the legal context in which OERM's activities operate. Where appropriate, given the objective of this evaluation, we have identified areas in which compliance with pertinent legal provisions could be enhanced. The nature of our evaluation objective did not require that we assess the potential for fraud and illegal acts. However, throughout the evaluation, we were alert to the potential for fraud and illegal acts, and no instances came to our attention.

Division and Office Risk Management/Internal Review Programs

The extent to which FDIC divisions and offices are participating in the FDIC's ERMP varies from (1) some organizations revamping their respective programs from the traditional internal control review approach toward an ERM approach to (2) other divisions and offices either making minor changes or no revisions to their traditional programs because the respective organizations viewed their internal control programs as being enterprise-wide risk focused.

The resources involved in the internal risk management program are shown in Table 3. It should be noted that some staff participate in risk management activities on a collateral basis performing duties such as budgeting, special projects, IT, and details to assist senior management. Further, senior management executives are not counted in these numbers.

Table 3: Division and Office Internal Review Staffing

Divisions/ Offices	Staffing	Description
Legal	7	Four Attorneys, 2 Management Analysts, and 1 Paralegal Specialist.
DIT	3	One Corporate Manager (CM), 1 CG-14, and 1 CG-13
DSC	12	12 permanent staff, supplemented by regional and field office detailees.
DRR	9	Two managers and 7 internal review specialists
ODEO	3	One CG-14 and 2 CG-13
DOA	6	One CM, 3 CG-14, 2 CG-13
DIR	3	One CM and 2 CG-14 (All Collateral Duty)
DOF	11	One CM, 3 CG-14, 6 CG-13, and 1 CG-12
OIG	1	CG-14 – Collateral duty
CU	2	One Manager – Collateral duty, One collateral duty detailee

Source: Interviews with division and office staff.

We interviewed Internal Control Liaisons (ICL) for the 10 divisions and offices shown above to inquire about their respective risk management programs and activities. We specifically asked the ICLs to: (1) provide an overview of the risk management program established in their respective divisions and offices to support division and office management in reaching program goals and objectives and using resources efficiently and effectively – a division and office responsibility outlined in Circular 4010.3, and (2) discuss their internal control/internal review programs and processes. The following sections reflect the ICLs' responses to our inquiries.

DSC Internal Control and Review Section (ICRS): is responsible for developing, implementing, overseeing, and coordinating DSC's internal risk management activities. DSC has a comprehensive regional and field office review program that is risk-focused and has standardized review work programs.

- The DSC field territory review process primarily focuses on the overall quality of supervisory work products produced by each field territory. A statistical and judgmental

sample of supervisory work products is reviewed for each field territory.

- The scope of the regional office reviews is determined based upon four areas: risk profile, findings of the field territory reviews conducted in each region, findings in previous regional office reviews, and requests/recommendations from the Division Director.

During 2006, ICRS started 38 Field Territory Reviews (23 Risk Management Territories and 15 Compliance Territories). The review program includes DSC internal review staff as well as detailees from regions and field offices. Subject Matter Experts, such as IT specialists, from Headquarters also accompany the team. During 2006, DSC detailed 32 staff to work on these reviews.

DRR Internal Review Section: conducts an annual Risk Assessment during the fourth quarter of each year to determine areas on which to focus internal control reviews. Using the DRR Strategic Plan as a foundation, DRR grouped the 2007 risk areas into five (5) broad categories:

- Ineffective Use of Human Resources
- Loss of Personal and/or Sensitive Information
- Lack of Readiness
- Incomplete IT Projects
- Failure to Maintain Daily Operations

Based upon the risks listed above and feedback received from DRR management regarding the risks they see for their respective functional areas, DRR identified about 16 potential areas for review over the next 18 months.

DRR indicated that the Division addresses risk management from an enterprise level, (i.e., looking at management of risk associated with an activity or function across all of DRR functions), and that doing so allows the flexibility to review business processes and work flows across all affected areas to mitigate risk from a cross-functional perspective.

DIR Planning and Resource Management Section: modeled its internal review program after DSC's structured internal review program. DIR uses AUs in its program and has five AUs:

1. Call Report.
2. Risk Information System.
3. Risk Analysis (Operations) – Risk analysis program offices are reviewed every 2 years.
4. Central Data Repository.
5. Assessments.

DIR's regional/area offices are subject to an internal review once every 2 years conducted in accordance with a review program that contains objectives, structure, and review procedures. DIR's review program states that the results of the office reviews are used to: (1) provide feedback to Regional Managers, (2) inform other regions of best practices, (3) serve as tangible feedback regarding the effectiveness of DIR's policies, practices, and procedures, and (4) test the various control objectives established in DIR's annual strategic plan and AU management control plans.

Legal Division Internal Review Group (IRG): In 2006, IRG developed an enterprise risk management program that identifies, monitors, and manages risks found in the Legal Division. The program seeks to concentrate on major or significant risks facing the division that could grow into serious problems for the Corporation. IRG, with assistance from OERM, looked at the Legal Division's eight AUs[21] and IRG reduced the number of AUs to three —Legal Division Management, Litigation, and Information Systems. For example, IRG determined that while outside counsel management and ethics were still risk factors, these AUs no longer rose to the level of individual reporting and were placed into the new Legal Division Management AU. IRG prepared Internal Control Review Forms for each AU, and identified 3 to 4 risks or potential vulnerabilities for each AU.

After discussions with OERM, IRG recommended discontinuing the stove-piped site visitation program and replacing it with division-wide risk management reviews. Under the new program, each AU would be assigned to a team of two IRG staff, and each team would conduct an annual review of its assigned AU throughout the Legal Division, as appropriate.

Division of Information Technology Internal Review: DIT has an initiative to change its entire internal review process to a new industry practice for information technology. DIT has adopted the COBIT© framework, which is a governance framework and supporting toolset that helps management bridge the gaps between internal control requirements, risk management, and technical issues. COBIT© provides a framework to help ensure that IT functions are adequately aligned with the business, resources are used responsibly, and risks are well managed. COBIT© is an international IT controls and governance standard that organizes IT activities into 34 processes. COBIT© helps managers ensure that their IT investments are aligned with business goals and objectives and that IT-related risks and opportunities are appropriately managed.

Division of Administration Management Support Section (MSS): MSS has changed its internal reviews from a compliance perspective to a more collaborative process in conjunction with management of important and risky areas. Further, in late 2006, the MSS stated in correspondence to senior DOA managers that MSS will focus on high-impact areas during the upcoming year. MSS defines its workload based on meetings with DOA management, consulting with OERM and reviewing recent audit conditions, analyzing emerging trends, and relying on professional judgment.

Division of Finance Administration & Internal Control Section (AICS): AICS has three major functions, namely (1) internal control reviews, (2) business process reviews, and (3) support to the Director and Deputy Director for special projects. In 2006, DOF's inventory of AUs consisted of the following.

1. Budget.
2. Assessments.
3. Manage Cash and Investments.
4. Disbursements.

[21] The eight AUs were: (1) Outside Counsel Management, (2) Official Records of the Board of Directors, (3) Freedom of Information Act/Privacy Act, (4) Rulemaking Process, (5) Employee Ethics, (6) Data Quality, (7) Legal Division Litigation, and (8) Legal Division Management.

5. Receipts.
6. Accounting Operations/Corporate Operations.
7. Financial Reporting.
8. Accounting and Financial Information Systems.

As an example of a business process review, AICS provided a 2006 NFE Business Process Review Project Plan that included a risk management section that identified objectives and five steps of the risk management process, namely (1) identify the risks, (2) assess the risks, (3) plan the risk response, (4) monitor the risk, and (5) document the lessons learned.

ODEO: ODEO uses AUs but merged its three AUs into one AU that includes (1) Complaint Processing, (2) Diversity and Affirmative Action, and (3) Minority and Women Outreach. ODEO conducts an internal control review of complaint processing every year, and the other two programs are reviewed every 2 years. Through a memorandum of understanding dated July 5, 2002, OERM provides routine assistance to ODEO in the following activities:

- Planning the internal control program.
- Performing internal control reviews of the Complaint Processing Program.
- Implementing and monitoring corrective actions for the Complaint Processing Program.

Corporate University (CU): CU does not have a formal internal review program. Controls over CU include a governing board that is comprised of division and office directors. In addition, the FDIC Human Resources Committee provides high-level oversight and control over CU. In 2006, CU had one AU, Contractor Oversight, ranked as a medium risk.

OIG: OIG's ICL is responsible for the OIG internal control program. The OIG has AUs corresponding to its major functions and operations -- audits, evaluations, investigations, Counsel's operations, and management and congressional relations. OIG operations undergo internal quality control reviews and external peer reviews.

CORPORATION COMMENTS

FDIC
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Deputy to the Chairman and CFO

October 19, 2007

MEMORANDUM TO: Jon T. Rymer
Inspector General

FROM: Steven O. App [Signed]
Deputy to the Chairman and
Chief Financial Officer

James H. Angel, Jr. [Signed]
Director
Office of Enterprise Risk Management

SUBJECT: Management Response to Draft Report Entitled
"***Evaluation of FDIC's Internal Risk Management Program (Assignment No 2007-002)***"

We have reviewed the Office of Inspector General (OIG) draft report entitled *"Evaluation of FDIC's Internal Risk Management Program (Assignment No. 2007-002)"* and are providing you with our response, after discussing the draft report findings, suggestions, and recommendations with the Chairman. We were especially pleased that your evaluation recognized that the Federal Deposit Insurance Corporation has a number of internally-focused committees and groups that help to keep the Board of Directors, Chairman, and senior executives informed of management operations and internal risks facing the Corporation and aid them in their decision making. In addition, you noted that, taken collectively, these committees and groups, as well as their respective reports and briefings, provide a comprehensive means for managing internal risks and establishing transparency. As you know, over the past four years, we have diligently sought to streamline and improve the integration and effectiveness of our internal risk management processes, employing a number of "best practices" and generally following the Government Accountability Office (GAO) blueprint outlined in their 2005 testimony before the Subcommittee on Government Management, Finance, and Accountability/Committee on Government Reform, entitled, "Financial Management: Effective Internal Control is Key to Accountability."

We appreciate the executive briefing you provided to the Chairman and senior officers of the Corporation on September 26, 2007, regarding your draft report. We found the discussion to be beneficial in clarifying certain assumptions, findings, and respective positions on what additional steps could be taken to enhance the FDIC's internal risk management program. In our discussion of the *Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management -- Integrated Framework (COSO ERM Framework)*, which the OIG used as a benchmark during its evaluation, we emphasized some of its relevant principles for internal risk

management and discussed the limited applicability to the FDIC of adopting the framework in its entirety.

During the briefing, we also emphasized that the Chairman and the Board have statutory responsibilities to manage the external risks in the banking industry, the risks within the supervised banks, as well as internal Corporate risks, all of which affect the Deposit Insurance Fund (DIF). Consequently, as an organization whose primary mission is risk management, many of the competitive marketplace tenets of the COSO ERM Framework are in the FDIC's unique risk management framework using other means and methodologies. This framework includes internal committees and organizations purposefully designed to identify, manage, and mitigate both external and internal risks. The Office of Enterprise Risk Management (OERM) supports the Chief Financial Officer (CFO) in administering his responsibilities under the Chief Financial Officers Act of 1990, and related Corporate Bylaws, to coordinate the FDIC's internal control and risk management program. OERM has developed a cooperative and collaborative working relationship with all internal Divisions and Offices, addressing risk management issues through periodic meetings with senior management, regular contact with the respective internal control liaisons, and a series of joint initiatives to mitigate risk. In addition, there is an interagency bank regulatory structure, the Federal Financial Institutions Exam Council (FFIEC) that coordinates interagency risk management initiatives and activities. The aforementioned discussion items from our executive briefing provide the background and rationale for our ensuing response to the OIG suggestions and recommendations contained in the referenced draft report.

We have given careful thought to the seven recommendations in your report, as well as the two suggestions you offered. Again, after discussions with the Chairman, we describe both our intentions to adopt certain items in the draft report and the alternative actions underway that may address some of the concerns underlying these recommendations and suggestions. During discussions on October 3, 2007, you indicated that, since this is an evaluation, there is no need to follow the normal concur or non-concur format. Rather, you asked for a detailed explanation of the Corporation's position on each issue. Therefore, each response will follow this format and we will consider each recommendation and suggestion "Closed" for audit follow-up purposes with the issuance of this response. Based on the organization of the OIG draft report, our response is divided into the following corresponding sections addressed first to the Chairman, and second to the CFO and OERM Director.

RECOMMENDATIONS AND SUGGESTIONS ADDRESSED TO THE CHAIRMAN

Recommendation 1: We recommend that the Chairman further study variances between the FDIC's overall internal ERM efforts and the COSO ERM Framework as discussed in this report and take steps to address the variances where it will add value to the FDIC's ERM program. Areas for potential focus include:

- **Defining and communicating the Corporation's risk appetite and ensuring that corporate objectives are aligned with that appetite.**
- **Establishing and documenting corporate-wide processes for identifying, assessing, and responding to internal risks.**

- **Establishing effective channels for OERM to communicate risk management information throughout the organization, such as through periodic status reports and meetings with divisional risk management/internal review units.**
- **Identifying the process for monitoring the implementation of ERM through ongoing activities or separate evaluations of division and office risk management programs and OERM's enterprise risk management program.**

Management's Response: We plan to take action on this recommendation, again with the caveat that much of the COSO ERM Framework does not apply directly to the FDIC, nor has the FDIC adopted this framework in its entirety. As we look at the key principles of the COSO ERM Framework that may be applicable, we do agree that there is value to more clearly defining and communicating the Corporation's risk appetite and ensuring that corporate objectives are aligned with this appetite. The Chairman's office will be considering a variety of vehicles to do this for 2008 and beyond, such as developing a Corporate risk statement to accompany our already established planning and budgeting process that produces our Corporate Performance Objectives. Further, we believe there is merit to exploring improved communication channels, regarding internal risk management. In the past, the CFO and OERM Director have briefed the Audit Committee on selected matters, including ongoing internal risk management activities, and audit resolution and follow-up activities. It is our intention to continue these briefings to the Audit Committee Chairman and determine if additional topics warrant discussion. In addition, OERM interacts daily with Division and Office staff, and ensures that any potentially material issues are communicated to the CFO and Chief Operating Officer (COO) for appropriate handling. The CFO and COO often discuss these issues during regularly scheduled weekly meetings with the Chairman and senior management. Building upon these practices, we will look for opportunities to add value and enhance these channels for communicating internal risk management activities, including the possible augmentation of certain existing reports and/or expanding the aforementioned briefings.

Recommendation 5: We recommend that the Chairman clarify the roles and responsibilities of the Chairman, the Board, and the Audit Committee in relation to the FDIC's ERM program. We also suggest that the Chairman reconcile OERM's current operations with the Bylaws and determine whether the Bylaws should be revised or whether OERM should expand certain aspects of its operation.

Management's Response: In our briefing with the OIG, it was indicated that the primary concern of the OIG underlying this recommendation was the role of the Audit Committee vis-à-vis the traditional role of an Audit Committee in a private, corporate setting. During our briefing, we emphasized that the roles of the Chairman and Board are clear, both statutorily and in the Bylaws, regarding ERM, with all major external and internal risk management matters being decided by the Board. Similarly, the Chairman provides direction on related day-to-day risk matters that do not require Board attention. However, we will clarify these roles, per our discussion.

With respect to the Audit Committee, it is a committee established by the Board to primarily review all OIG audit reports prior to full Board consideration. In accordance with the Bylaws, the Audit Committee also oversees the Corporation's financial reporting, reviews and approves management's annual plan for compliance with the CFO Act, assesses the sufficiency of the Corporation's internal control structure, and ensures compliance with applicable laws and regulations and internal and external audit recommendations, all for the purpose of rendering advice to the Chairperson of the Board of Directors with respect to any matter relating to the Committee's responsibilities. Finally, if there is an unresolved dispute between management and the OIG on any given audit report recommendation, the Audit Committee provides input to the Chairman, who makes all final determinations regarding such disputes in her role as the FDIC's Audit Follow-Up Official (AFO). Other traditional private sector Audit Committee roles, such as selecting the financial statement auditor, are obviated by statute (e.g., the GAO is the FDIC's auditor for financial reporting purposes by statute). Nevertheless, the FDIC Audit Committee will be encouraged to bring any summary insights or trends it deems appropriate to the Board's attention and, again, will be provided reports and/or be briefed periodically by the CFO and/or OERM Director on internal financial and operational risk issues. Also, as was discussed, management does not perceive any discrepancies between OERM's current operation and the respective Bylaw, which clearly delineates OERM's responsibilities as limited to supporting the CFO on internal control and operational risk, versus external risk matters.

Suggestion for Management – FDIC Committees and Groups that Contribute to Internal Risk Management: As discussed, the FDIC has a number of internally-focused committees and groups that collectively contribute to internal ERM and good corporate governance. More could be done, however, to institutionalize how these entities interact to manage internal risks facing the Corporation and for the purpose of preserving continuity in the event of senior management changes. Accordingly, we suggest that the Chairman's Office, in coordination with the COO and the CFO, articulate and document how the various committees and groups interrelate in managing internal risk.

Management's Response: We understand the basic intent of this suggestion and will take appropriate action to add more clarity to the interaction and interdependencies of the existing committees. As we discussed during our briefing, the vast majority of the committees and groups depicted on page 41 of the OIG draft report are engaged in both external and internal risk management, have well-documented charters and procedures, and are subject to specific delegations by the Board for both performance and required reporting. Nevertheless, the COO and the CFO will look at developing a more comprehensive blueprint to enhance the coordination and documentation of these committees and groups, where appropriate, during 2008.

Suggestion for Management - Opportunities to Enhance ERM at the FDIC: As discussed above, the FDIC ERM Program is limited to internal FDIC operations, by design. This approach is contrary to the fundamental COSO ERM Framework tenet that ERM should be applied across the enterprise, at every level and unit, and should include taking an entity-level portfolio view of risk. Without an enterprise-wide view of risk, the FDIC may

not be in a position to align and integrate varying views of risk management across the organization or effectively assess systemic risks.

We are suggesting that the FDIC consider whether the Corporation's internal and external risk management activities should be integrated and, if so, ensure that such integration is done efficiently and effectively.

Management's Response: Again, as mentioned at the outset of our response, the COSO ERM Framework is not appropriate for universal application to the FDIC. The FDIC risk management framework depicted on page 41 of the OIG draft report is a robust, integrated, and effective alternative risk model that does, in fact, provide an extensive enterprise-wide view of risk to accomplish the FDIC's mission. Rather than focusing on housing all external and internal risk management activities in one office or under one person, the FDIC utilizes a risk matrix approach, with virtually all risk management activities reporting to either the COO and/or CFO, on behalf of the Chairman. Further, these activities are optimized by extensive communication channels upward and throughout the FDIC, and are directly linked into our corporate planning, budget, and performance measurement process.

RECOMMENDATIONS ADDRESSED TO THE CHIEF FINANCIAL OFFICER AND OFFICE OF ENTERPRISE RISK MANAGEMENT DIRECTOR

As a preface to specific comments on the recommendations directed to the CFO and OERM Director, it may be useful to consider various aspects of the background, philosophy, and results to date of the internal enterprise risk management program. It is also important to note that any such change initiatives, especially those that streamline processes, present certain challenges to the incumbent staff in Divisions and Offices who have been in charge of existing programs.

Background

OERM was created by the CFO in 2004, with the concurrence and approval of the FDIC Board, in part because of the then executive management's perception of the need to change the program which the Office of Internal Control Management (OICM) had overseen since 1996. In a general sense, the Corporation was nearing the end of its prolonged period of downsizing, and greater emphasis was being placed on establishing processes that were more reflective of current needs. It was executive management's stated objective for OERM to be more pro-active in managing controls and risks, than had been the case in the earlier environment. A few characteristics of the internal control environment overseen by OICM included: (1) the program was largely viewed by Divisions/Offices as a once per year reporting exercise, whereby hundreds of pages of completed documents were forwarded for review; (2) the program focused primarily on procedural compliance, rather than broader management issues or risks; (3) risk identification in each Division/Office was bottom-up from mid-level employees, rather than top-down from managers; (4) OICM was viewed by much of the Corporation as being an extension of, or a conduit to, the OIG, resulting in few requests for participation in internal risk management projects/initiatives; and (5) the annual assurance process was both cumbersome and costly.

Philosophy

Since its creation, and under the direction of the CFO, OERM has issued various documents which set the tone for the evolution of the internal enterprise risk management program and provided guidance to Divisions and Offices. Key among those documents were a memo entitled "Update on ERM in the FDIC", and "Directive 4010.3 FDIC Enterprise Risk Management Program." In conjunction with other communications and actions, OERM thus shared components of its vision and philosophy, some aspects of which include: (1) stressing a management focus on key issues and risks, rather than on procedural compliance reviews; (2) encouraging the Corporation to view the management of internal risks and controls as part of, and integrated into, the everyday working environment, rather than a once per year paperwork exercise; (3) promoting the concept of having a sound foundation in place in all areas, including having documented procedures and controls, trained employees, and supervisors and managers who are held accountable for performance and results; (4) providing principle-based guidance and empowering management to attend to its control and risk issues, based primarily on its knowledge of operational challenges and priorities; (5) shifting emphasis to have control activities seen as part of the process of meeting broader Corporate goals and objectives, rather than being separate, stand-alone objectives; and (6) establishing a balance in management's relationship with its auditors.

Results to Date

Although OERM's vision continues to evolve, many positive conditions have developed and/or have been sustained throughout the Corporation resulting in: (1) the elimination of paper-intensive control processes, allowing internal review groups to focus on more meaningful activities; (2) a more top-down approach to risk identification within Divisions and Offices; (3) OERM being viewed as a trusted partner and leading or participating in numerous control-related projects across the Corporation; and (4) a greater level of openness and transparency on control issues in the Corporation, as evidenced not only by the disclosure of more than 60 "2nd tier" issues during the 2006 assurance statement process, but by OERM having been invited to serve as a neutral party to help manage internal risk within and between Divisions.

In general, there is a much greater level of "continuous improvement" being achieved in the Corporation through the many projects being carried out by OERM and/or the Divisions and Offices themselves. It should be noted that the Corporation continued its record of clean audit opinions with no material weaknesses during this period of transition.

Recommendation 2: We recommend that the Director, OERM, take necessary steps to develop and issue an annual assurance statement to the Chairman related to the OERM program and other OERM responsibilities.

Management's Response: As we indicated earlier in this response, OERM is an extension of the CFO's office and, by design, needs to maintain a certain level of independence for the annual assurance statement process. As the OIG was advised during the review, OERM sends out annual guidance on what needs to be covered during the assurance statement process. The

assurance statements themselves are then prepared by other Division and Office directors and are addressed to the Chairman, for the purposes of establishing accountability, but are sent to OERM for independent review and evaluation. The CFO has directed OERM to administer this entire program, in order to make independent recommendations to the Chairman, through the CFO/COO, on the potential materiality of issues, if any, as well as on what related wording might be considered for inclusion in the annual report. Based on this independent quality control process by OERM, the CFO and OERM Director are then in a position to brief the Chairman on the summary results of this analysis and on all other results attendant to year-end reporting under the CFO Act and related requirements. We believe the substance of this process is more effective than just having OERM sign a statement to the Chairman.

Recommendation 3: We recommend that the Director, OERM, coordinate with the Legal Division to review section 4 reporting requirements to determine the FDIC's reporting responsibilities.

Recommendation 4: Based upon the results of recommendation 3, we recommend that the Director, OERM, issue guidance for FMFIA section 4 reporting and the work required to support an assertion on financial management systems.

Management's Response to Recommendations 3 and 4: While we appreciate the OIG's questions regarding the FDIC's responsibilities under Section 4 of FMFIA, we believe the reporting requirements under this section are clear: FDIC must provide a statement of assurance as to whether or not its financial management systems, including its internal controls, are effective. We believe that OMB Circulars A-11, A-123, A-127, A-130, FFMIA and FISMA provide additional variables to consider in determining what the Corporation must do to fulfill its responsibilities in these matters. While only a portion of this body of guidance directly applies to the FDIC from a legal perspective, management has coordinated with the Legal Division over the years and developed an integrated approach for providing assurance that we believe more than satisfies the letter (as applicable) and the spirit of the requirements.

Prior to explaining our integrated approach, however, it may be useful to mention three considerations that help define the parameters for the overall process for reporting assurance. These are:

- The assurance statement process primarily is the required vehicle for disclosing material weaknesses to the Corporation's external stakeholders. Lesser issues are not included, nor is there an expectation of perfection in operations and controls. Indeed, the overall standard is "reasonable assurance that the objectives of FMFIA have been achieved."
- As explained in OERM's annual guidance, the primary basis for providing assurance should be management's judgment based on knowledge gained from the daily operation of programs and systems. The results of internal reviews, audits, evaluations and similar activities should be viewed as supplements to, not replacements for, management's judgment.

- There are no clear cut rules defining when any problematic issue might cross the line and become a material weakness. Again, with rare exception, materiality is a judgment call made by management or its financial statement auditors.

In developing an integrated approach, management has assimilated the body of guidance and organized it into four broad categories: 1) secure systems; 2) integrated systems; 3) reliable data; and 4) fiscal responsibility. Some of the variables considered in each of these categories are briefly discussed below.

Secure systems – Over the years, management has invested considerable resources toward the establishment of one of the top system security environments in all of the federal government. A few on-going, day-to-day control activities that affect financial systems include: regular vulnerability scanning; up-to-date certifications and accreditations; effective follow-up on known deficiencies; periodic security reviews; effective patch management; reasonable password and access controls; and successfully tested continuity of operations plans. Moreover, OERM has a dedicated system security liaison to DIT, who maintains ongoing involvement on all system security initiatives and issues. The OERM liaison has also overseen the proper resolution of more than 250 OIG/GAO recommendations to DIT/management in 42 audit/evaluation reports issued over the past five years.

Integrated systems – One of OMB's concerns in this area is the inefficiency and inaccuracy that can result from the management of financial systems that are not integrated and where the same data must be entered multiple times, among other shortcomings. Once again, the FDIC is among the government-wide leaders on this requirement. Specifically, the implementation of NFE in 2005 entailed the implementation of 18 PeopleSoft modules, integrating 23 legacy systems, and absorbing 37 systems into the new PeopleSoft modules. Moreover, NFE also eliminated many separate/manual processes and converted them into system-performed tasks, which were tested extensively for accuracy and integrity. All new systems with financial components must be integrated with or otherwise tied to NFE, as a matter of course.

Reliable data - Although little of OMB's guidance on federal accounting standards applies to the FDIC, the Corporation and the Division of Finance (DOF) have dedicated staff who monitor new/changed requirements issued under the accounting standards that do apply to us, including reporting requirements to the Treasury Department tied to the production of the government-wide Consolidated Financial Statements. In addition to the controls associated with NFE system design and compliance with accounting standards, the DOF control environment operates with several daily and monthly reports to help ensure the integrity and accuracy of financial data. Just a few of these items include daily reviews of non-posted items, suspense items, journal error items, corporate trial balance, and a balancing of the ledgers (Corporate/Receivership, etc). Due/to and due/from reports are reviewed monthly, as are certain control reports and account reconciliations. Combined, these and other reviews and reports provide management with a high degree of confidence in the accuracy of our financial data and its use in generating financial reports for internal and external purposes.

Fiscal responsibility – The body of OMB and other guidance also addresses the need for agencies to submit budgets, compare budget and performance, track various expenditures, and maintain systems to support these and related activities. Once again, the Corporation has in place many ongoing processes and controls that, in our opinion, more than meet related requirements. Specifically, the FDIC executes a corporate-wide, comprehensive annual budget process, relevant parts of which are communicated to OMB in support of systems requirements under A-11. DOF also monitors performance against budget throughout the year and includes relevant information in the Corporation's Annual Report, also referred to as the Performance and Accountability Report, which includes the Chairman's assurance statement. Other examples of the Corporation's fiscal responsibility include: the role and activities of the Capital Investment Review Committee (CIRC), which oversees large system development efforts; the Chief Information Officer Council, which oversees expenditures on development projects below the CIRC threshold; the Program Management Office (PMO), which develops structure and standards for smaller development projects; and OERM's multiple roles in supporting the PMO on project management issues, carrying out post project reviews on completed CIRC/other projects, and providing risk management oversight on current CIRC projects.

The results of independent financial statements audits and other pertinent independent audits/evaluations are used to compliment management evaluations and processes in building the assurance statement. It is significant to note that the Comptroller General stated in its 2006 financial statement audit report:

> "FDIC management maintained, in all material respects, effective internal control over financial reporting (including safeguarding assets) and compliance as of December 31, 2006, that provided reasonable assurance that misstatements, losses, or noncompliance material in relation to FDIC's financial statements for each fund would be prevented or detected on a timely basis. **Our opinion is based on criteria established under 31 U.S.C. 3512 (c), (d), [commonly known as the Federal Managers' Financial Integrity Act (FMFIA)]** (emphasis added)."

While we have discussed with the OIG the limitation of the support we can take from the annual GAO audit work, we respectfully assert that the GAO's audit does in fact include a review under Section 4 of FMFIA, and consequently, is appropriately considered by management when making the statement of assurance.

Other controls and reviews, including flowcharted processes, system mapping, and the review and testing of the NFE modules, give further support for our assurance statement on Section 4. NFE is a highly centralized system, under the responsibility of the CFO and DOF Director, who collectively monitor its performance on a monthly basis. This integrated, day-to-day analysis of our financial systems including monthly/quarterly financial reporting is the type of "best practice" articulated in the following excerpt by GAO in its 2005 testimony entitled, *Financial Management: Effective Internal Control is Key to Accountability*, in which GAO noted that,

> "(government programs for internal control) unfortunately had become mired in extensive process and paperwork. Significant attention was focused on creating a paper

> trail to prove that agencies had adhered to the OMB assessment process and on crafting voluminous annual reports that could exceed several hundred pages. It seemed that the assessment and reporting processes had, at least to some, become the endgame. … Unfortunately, many of the more serious and complex internal control and accounting system weaknesses remained largely unchanged and agencies were drowning in paper. The recent December 2004 update to Circular A-123 reflects … changes (that) are intended to strengthen the requirements for conducting management's assessment of internal control over financial reporting. … The Circular correctly recognizes that instead of considering internal control as an isolated management tool, agencies should integrate their efforts to meet the requirements of FMFIA with other efforts to improve effectiveness and accountability. Internal control should be an integral part of the entire cycle of planning, budgeting, management, accounting, and auditing."

In conclusion, the FDIC believes that its process for assurance reporting emphasizes substance over form and has been successfully integrated into the day-to-day management of DOF, DIT, and others in the FDIC who have a role in NFE. Our success in achieving unqualified opinions for 15 years is due in no small part to having an effective program for evaluating internal controls for financial systems.

Recommendation 6: We recommend that the Director, OERM, draft and issue detailed procedures for a comprehensive ERM program as envisioned in the Corporate Bylaws.

Recommendation 7: We recommend that the Director, OERM, take steps to develop and present corporate-wide training to FDIC employees on the ERM program as envisioned in the Corporate Bylaws.

Management's Response to Recommendations 6 and 7: The OIG makes reference in these two recommendations to the level of detail for internal control procedures, and the extent or nature of Corporate internal controls training "envisioned" in the Bylaws. We would respectfully assert that there is no Corporate Governance or Bylaw issue here, as the CFO was the architect of the Bylaws, specifically drafting all of its components, including references to procedures and Corporate training to match the current actitivities which OERM is successfully doing in these areas.

We do recognize the need for a comprehensive ERM program, the OIG's concern about consistent, detailed internal control procedures at the Division/Office level, and the benefits of appropriate training to meet the needs of the FDIC. As noted earlier, management does not believe that there are any discrepancies between OERM's current operation and the respective Bylaws, and management continues to fully support OERM's efforts in developing and implementing a comprehensive ERM program and appropriate training program. Specifically, the OERM Directive 4010.3, entitled "FDIC Enterprise Risk Management Program," serves to provide the general framework for the development, maintenance, and evaluation of a comprehensive Enterprise Risk Management Program at the FDIC and clearly defines the responsibilities of and to the Office of Enterprise Risk Management. Significantly, this includes

the need for Divisions and Offices to document procedures, which is reinforced by the respective Division/Office directors in their attestations in the annual assurance statement.

In addition, the OERM staff maintains daily, ongoing communications with the Divisions and Offices, discusses current and emerging risk management issues or concerns, and provides assistance in addressing these as appropriate. These activities include the development of detailed procedures for new programs and offices, including respectively, Deposit Insurance Reform and the new Office of International Affairs. Most Divisions and Offices continue to maintain an internal review staff that conducts targeted risk focused reviews on areas of concern or interest to management, including the continuous updating of relevant internal procedures for the transactions and processes under their purview. We believe this distributed workload, along with Division/Office flexibility, empowerment, and accountability provide for a consistent internal control framework across the Corporation. OERM has supported, and has been asked to participate, in a number of these reviews.

In addition, OERM is engaged in designing procedures on a broader scale, to encompass processes which transcend Division/Office lines. For instance, OERM serves as Risk Manager on all projects that go before the Capital Investment Review Committee. OERM staff served as risk managers on the Central Data Repository (CDR) Project, the Virginia Square Phase II development project, and the Deposit Insurance Reform Project, and were recognized with the Chairman's Award for their contribution in the successful completion of each project. In addition, OERM has been working with DIT to develop standardized Risk Assessments and reporting for all major IT initiatives. OERM has worked closely with Divisions and Offices in encouraging a risk focused approach to internal controls and risk management, as opposed to the labor and paper intensive all encompassing reviews that had been done in the past. For example, the Division of Supervision and Compliance is now in the second year of their revamped risk focused Regional Office Review Program that is targeted to focus on the specific issues and unique risks facing a particular region. The new process has been well received by both Regional and Washington management.

Regarding Corporate training, the Internal Control Liaisons (ICL) from DSC, DRR, DIR, DOF, DOA, and DIT that are assigned as the primary points of contact with OERM, and previously OICM, have all been working in those positions for more than seven years. The former OICM had provided extensive internal control training and sponsored a number of Best Practices Conferences focusing on internal controls and risk management. In addition, OERM has provided several ERM training sessions to staff from the Legal Division and Division of Finance, and is in the process of delivering additional ERM training to staff from the Division of Administration. The OERM website has a specific Training link that reflects that OERM provides training programs that build and maintain enterprise risk management and internal control skills. OERM's training and development programs are open to all Divisions and Offices, including directors, managers, supervisors, and employees. Current training programs include: Enterprise Risk Management, Internal Controls, Risk Management, Assurance Statements, Strategic Planning/Balanced Scorecard, and Audit Follow-up. Training is available in either a Division or Office specific format, or as a comprehensive program designed to expose attendees to a wide range of ERM or internal control related concepts. The web page lists several examples

of the training and presentations available from OERM, and encourages Divisions and Offices to contact OERM if there is a need for training. OERM will continue to promote the training opportunities that are available, and believes this more tailored approach to Corporate training better serves the needs of the Divisions/Offices than a single, universal training program.

MANAGEMENT RESPONSES 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	Open or Closed[b]
Suggestion	Management will take appropriate action to add more clarity to the interaction and interdependencies of the existing committees. The COO and the CFO will look at developing a more comprehensive blueprint to enhance the coordination and documentation of FDIC committees and groups, where appropriate, during 2008.	To be determined	$0	Yes	Open
1	The Chairman's office will be considering a variety of vehicles to more clearly define and communicate the Corporation's risk appetite and ensure that corporate objectives are aligned with this appetite for 2008 and beyond, such as developing a corporate risk statement to accompany the planning and budgeting process that produces Corporate Performance Objectives. Further, management will look for opportunities to add value and enhance channels for communicating internal risk management activities, including the possible augmentation of certain existing reports and/or expanding Audit Committee and other management briefings.	To be determined	$0	Yes	Open
2	No action planned. Management stated in its response that OERM is an extension of the CFO's office and, by design, needs to maintain a certain level of independence for the annual assurance statement process. Management described OERM's quality assurance role in that process and stated that it believes the substance of this process is more effective than just having OERM sign a statement to the Chairman.	N/A	$0	Yes	Closed

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
3	No action planned. Management stated in its response that the FDIC's responsibilities under Section 4 of FMFIA are clear and that management has coordinated with the Legal Division over the years and developed an integrated approach for providing assurance that more than satisfies the letter (as applicable) and the spirit of the Section 4 requirements.	N/A	$0	Yes	Closed
4	No action planned. Management stated in its response that the FDIC's responsibilities under Section 4 of FMFIA are clear and that management has coordinated with the Legal Division over the years and developed an integrated approach for providing assurance that more than satisfies the letter (as applicable) and the spirit of the Section 4 requirements.	N/A	$0	Yes	Closed
5	Management will clarify the roles of the Chairman, the Board, and the Audit Committee in relation to the FDIC's ERM program. We agree with management's planned action on this aspect of the recommendation. However, management does not believe that there are any discrepancies between OERM's current operation and the respective Bylaws, and management continues to fully support OERM's efforts in developing and implementing a comprehensive ERM program and appropriate training program.	To be determined	$0	Yes	Open
6	No action planned. Management does not believe that there are any discrepancies between OERM's current operation and the respective Bylaws, and management continues to fully support OERM's efforts in developing and implementing a comprehensive ERM program and appropriate training program.	N/A	$0	Yes	Closed

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
7	No action planned. Management does not believe that there are any discrepancies between OERM's current operation and the respective Bylaws, and management continues to fully support OERM's efforts in developing and implementing a comprehensive ERM program and appropriate training program.	N/A	$0	Yes	Closed
Suggestion	No action planned. In its response, management stated that the COSO ERM Framework is not appropriate for universal application to the FDIC. Management further stated that rather than focusing on housing all external and internal risk management activities in one office or under one person, the FDIC utilizes a risk matrix approach, with virtually all risk management activities reporting to either the COO and/or CFO, on behalf of the Chairman. Further, these activities are optimized by extensive communication channels upward and throughout the FDIC, and are directly linked into the FDIC's corporate planning, budget, and performance measurement process.	N/A	$0	Yes	Closed

[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] Once the OIG determines that the agreed-upon corrective actions have been completed and are effective, the recommendation can be closed. In this case, we are closing the recommendations because the Chairman, as the Corporation's AFO, has supported management's response to the report's suggestions and recommendations.