V. Management Control

Enterprise Risk Management

The Office of Enterprise Risk Management, under the auspices of the Chief Financial Officer organization, is responsible for corporate oversight of internal control and enterprise risk management (ERM). This includes ensuring that the FDIC's operations and programs are effective and efficient and that internal controls are sufficient to minimize exposure to waste and mismanagement. The FDIC recognizes the importance of a strong risk management and internal control program and has adopted a more proactive and enterprise-wide approach to managing risk. This approach focuses on the identification and mitigation of risk consistently and effectively throughout the Corporation, with emphasis on those areas/issues most directly related to the FDIC's overall mission. As an independent government corporation, the FDIC has different requirements than appropriated federal government agencies; nevertheless, its ERM program seeks to comply with the spirit of the following standards, among others:

- Federal Managers' Financial Integrity Act (FMFIA);
- Chief Financial Officers Act (CFO Act);
- Government Performance and Results Act (GPRA);
- Federal Information Security Management Act (FISMA); and
- OMB Circular A-123.

The CFO Act extends to the FDIC the FMFIA requirements for establishing, evaluating and reporting on internal controls. The FMFIA requires agencies to annually provide a statement of assurance regarding the effectiveness of management, administrative and accounting controls, and financial management systems.

The FDIC has developed and implemented management, administrative, and financial systems controls that reasonably ensure that:

- Programs are efficiently and effectively carried out in accordance with applicable laws and management policies;
- Programs and resources are safeguarded against waste, fraud, and mismanagement;
- Obligations and costs comply with applicable laws; and
- Reliable, complete, and timely data are maintained for decision-making and reporting purposes.

The FDIC's control standards incorporate the *Government Accountability Office's (GAO) Standards for Internal Control in the Federal Government*. Good internal control systems are essential for ensuring the proper conduct of FDIC business and the accomplishment of management objectives by serving as checks and balances against undesirable actions or outcomes.

As part of the Corporation's continued commitment to establish and maintain effective and efficient internal controls, FDIC management routinely conducts reviews of internal control systems. The results of these reviews, as well as consideration of the results of audits, evaluations, and reviews conducted by the GAO, the Office of Inspector General (OIG) and other outside entities, are used as a basis for the FDIC's reporting on the condition of the Corporation's internal control activities.

Material Weaknesses

Material weaknesses are control shortcomings in operations or systems that, among other things, severely impair or threaten the organization's ability to accomplish its mission or to prepare timely, accurate financial statements or reports. The shortcomings are of sufficient magnitude that the Corporation is obliged to report them to external stakeholders.

To determine the existence of material weaknesses, the FDIC has assessed the results of management evaluations and external audits of the Corporation's risk management and internal control systems conducted in 2009, as well as management actions taken to address issues identified in these audits and evaluations. At the end of the 2009 audit, GAO identified a material weakness in loss-share estimation processes and a significant deficiency in the information technology (IT) security area. The FDIC is addressing the control issues raised by GAO, related to its 2009 financial statement audits.

Description of Material Weakness

GAO identified deficiencies in controls over FDIC's process for deriving and reporting estimates of losses to the DIF from resolution transactions involving loss-sharing arrangements. These deficiencies resulted in errors in the draft 2009 DIF financial statements that went undetected by FDIC and that necessitated adjustments in finalizing the financial statements. Although the net effect of these errors, less than 0.4 percent of net receivables, was ultimately not material in relation to the financial statements taken as a whole, the nature of the control deficiencies identified that resulted in these errors occurring and going undetected is such that there is a reasonable possibility that they could have led to material misstatements to DIF's financial statements that would not have been timely detected and corrected.

Corrective Actions and Target Completion Dates

Several corrective actions were in process or have been completed prior to release of this publication. Remaining actions include:

- Implement revised guidance and procedures over the least cost test analysis, including, improving the review checklists for peer review—June 2010
- Require a monthly review of a sample of completed analyses—July 2010.
- Implement a process to improve the documentation and approval of the changes to the least cost test model and loss-share worksheet—June 2010
- Implement an independent review of the LLR templates—June 2010

Additionally, FDIC management will continue to focus on high priority areas, including the six Program Management Office organizations, IT systems security, resolution of bank failures, and privacy, among others.

Management Report on Final Actions

As required under amended Section 5 of the Inspector General Act of 1978, the FDIC must report information on final action taken by management on certain audit reports. For the federal fiscal year period October 1, 2008, through

September 30, 2009, there were no audit reports in the following categories:

Table 1: Management Report on Final Action on Audits with Disallowed Costs

Table 2: Management Report on Final Action on Audits with Recommendations to Put Funds to Better Use

The following table provides information on audit reports over one year old:

Table 3: Audit Reports Without Final Actions But With Management Decisions Over One Year Old for FY 2009

Report No. and Issue Date	OIG Audit Finding	Management Action	Disallowed Costs
1. AUD-08-006 03-12-2008	The OIG recommended that the FDIC should update Circular 1380.3, Safeguarding FDIC Information Technology (IT) Hardware, to reflect the FDIC's current business environment for managing its laptop computer inventory and to define policy for the disposal of hard drives.	The FDIC is completing the update and approval process for Circular 1380.3, Safeguarding FDIC Information Technology (IT) Hardware. Completed: November 2009	$0
2. EM-08-002 03-05-2008	The OIG recommended that the FDIC should revise Circular 1610.2, Security Policy and Procedures for FDIC Contractors and Subcontractors, to enhance the current process for conducting contractor employee background investigations.	The revisions to Circular 1610.2, Security Policy and Procedures for FDIC Contractors and Subcontractors, have been completed, and DOA has been asked to delay further review due to work being done by the Legal Division to develop security guidelines for contractors. Completed: February 2010	$0
3. EVAL-08-002 12-06-2007	The OIG recommended that the FDIC should revise the FDIC Business Continuity Plans (BCP) and pandemic preparedness plans to more specifically describe the role telework plays in those plans. The OIG also recommended that the FDIC modify FDIC Form 2121.5, Employee/Supervisor Telework Program Agreement, for regular or recurring telework situations to include identifying any sensitive data that may be used during telework to assist management in making the decision to approve or disapprove a telework request.	The FDIC is in the process of finalizing multiple changes to the Business Continuity Plan and coordinating across multiple Divisions and Offices to effect these changes. Additionally, the FDIC is completing the changes to Circular 2121.1, Federal Program Circular and Telework Form 2121.5, Employee/Supervisor Telework Program Agreement. These documents have been circulated for review and comment. Completed: March 2010	$0
4. EVAL-08-005 09-24-2008	The OIG recommended that the FDIC should improve the facilities' infrastructure for monitoring energy management and sustainability efforts by: a) Installing or upgrading building energy management systems, and b) Installing sub-metering capabilities to monitor specific uses of energy.	Several of the electrical sub-meters installed in March 2009 were found to be defective, resulting in erroneous energy consumption data. The defective electrical sub-meters are in the process of being repaired/replaced. Completed: December 2009	$0

This page intentionally left blank.