5 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:

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

At the end of the 2009 audit, GAO identified a material weakness in the loss-share estimation processes and a significant deficiency in the information technology security area. Subsequent implementation of enhanced controls has eliminated the material weakness and the significant deficiency.

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 2010, as well as management actions taken to address issues identified in these audits and evaluations. Based on this assessment and application of other criteria, the FDIC concludes that no material weaknesses existed within the Corporation's operations for 2010.

Additionally, FDIC management will continue to focus on high priority areas, including implementation of Dodd-Frank Act, the 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. The tables on the following pages provide information on final action taken by management on audit reports for the federal fiscal year period October 1, 2009, through September 30, 2010.

TABLE 1: Management Report on Final Action on Audits with Disallowed Costs for Fiscal Year 2010

	Audit Reports	Number of Reports	Disallowed Costs
Dollars in Thousands			
A.	Management decisions – final action not taken at beginning of period	0	$0
B.	Management decisions made during the period	4	$34,037
C.	Total reports pending final action during the period (A and B)	4	$34,037
D.	Final action taken during the period:		
	1. Recoveries:		
	(a) Collections & offsets	2	$8,127
	(b) Other	0	$0
	2. Write-offs	2	$837
	3. Total of 1(a), 1(b), & 2	2[1]	$8,964
E.	Audit reports needing final action at the end of the period	2	$25,148[2]

[1]Two reports have both collections and write-offs, thus the total of 1(a), 1(b), and 2 is two.

[2]Amount collected in D3 included excess recoveries of $75,000, not reflected in line E.

TABLE 2: Management Report on Final Action on Audits with Recommendations to Put Funds to Better Use for Fiscal Year 2010

	Audit Reports	Number of Reports	Funds Put to Better Use
Dollars in Thousands			
A.	Management decisions – final action not taken at beginning of period	0	$0
B.	Management decisions made during the period	2	$410
C.	Total reports pending final action during the period (A and B)	2	$410
D.	Final action taken during the period:		
	1. Value of recommendations implemented (completed)	1	$151
	2. Value of recommendations that management concluded should not or could not be implemented or completed	2	$259
	3. Total of 1 and 2	2[3]	$410
E.	Audit reports needing final action at the end of the period	0	$0

[3]One report had both implemented and unimplemented values.

TABLE 3: Audit Reports without Final Actions But with Management Decisions over One Year Old for Fiscal Year 2010

Management Action in Process

Report No. and Issue Date	OIG Audit Finding	Management Action	Disallowed Costs
AUD-10-002 12/11/09	The OIG recommended that the FDIC should review and revise (where appropriate) its risk assessment methodology, to ensure adequate consideration of the risks associated with electronic transactions involving the Internet.	The FDIC will formally document and further integrate its existing e-authentication risk assessments into the overall risk assessment methodology. Also, the FDIC will reassess the e-authentication risk assessment process for FDICconnect. **Completed: February 2011**	$0