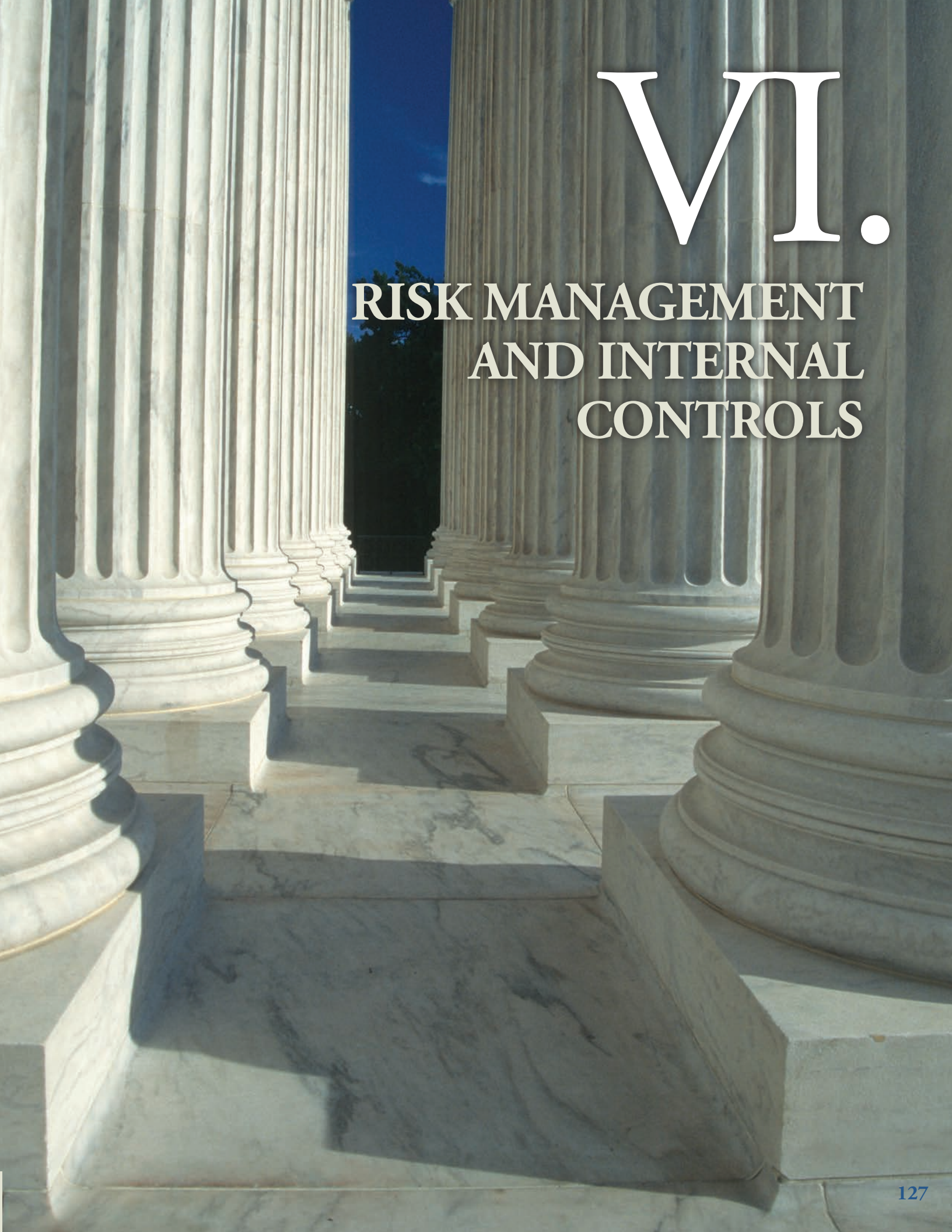

VI.

RISK MANAGEMENT AND INTERNAL CONTROLS

THIS PAGE INTENTIONALLY LEFT BLANK

The FDIC uses several means to maintain comprehensive internal controls, ensure the overall effectiveness and efficiency of operations, and otherwise comply as necessary with the following federal standards, among others:

- Chief Financial Officers' Act (CFO Act)
- Federal Managers' Financial Integrity Act (FMFIA)
- Federal Financial Management Improvement Act (FFMIA)
- Government Performance and Results Act (GPRA)
- Federal Information Security Management Act (FISMA)
- OMB Circular A-123
- GAO's *Standards for Internal Control in the Federal Government*

As a foundation for these efforts, the Division of Finance, Risk Management and Internal Controls Branch oversees a corporate-wide program of relevant activities by establishing policies and working with management in each division and office in the FDIC. The FDIC has made a concerted effort to ensure that financial, reputational, and operational risks have been identified and that corresponding control needs are being incorporated into day-to-day operations. The program also requires that comprehensive procedures be documented, employees be thoroughly trained, and supervisors be held accountable for performance and results. Compliance monitoring is carried out through periodic management reviews and by the distribution of various activity reports to all levels of management. Conscientious attention is also paid to the implementation of audit recommendations made by the FDIC Office of Inspector General, the GAO, and other providers of external/audit scrutiny. The FDIC has received unmodified/unqualified opinions on its financial statement audits for 26 consecutive years, and these and other positive results reflect the effectiveness of the overall management control program.

In 2017, efforts were focused on data mining, continuity of operations, process mapping, process improvements, internal controls of outsourced service providers, continuation of efforts on failed bank data, and systems security. Considerable energy was devoted to ensuring that the FDIC's processes and systems of control have kept pace with the workload, and that the foundation of controls throughout the FDIC remained strong.

During 2018, RMIC will continue to focus on enhancing FDIC's Risk Management program, improving data mining capabilities, identifying performance metrics, mapping key operational areas, exploring opportunities for process improvement, monitoring FDIC's internal controls over outsourced service providers, continuing efforts with stakeholders on failed bank data, and system security. Also, continued emphasis and management scrutiny will be applied to the accuracy and integrity of transactions and oversight of systems development efforts in general.

FRAUD REDUCTION AND DATA ANALYTICS ACT OF 2015

The Fraud Reduction and Data Analytics Act of 2015 was signed into law on June 30, 2016. The law is intended to improve federal agency financial and administrative controls and procedures to assess and mitigate fraud risks, and to improve federal agencies' development and use of data analytics for the purpose of identifying, preventing, and responding to fraud, including improper payments.

The FDIC's enterprise risk management and internal control program considers the potential for fraud and incorporates elements of Principle 8 – Assess Fraud Risk, of the GAO Standards of Internal Control in the Federal Government. The FDIC implemented a Fraud Risk Assessment Framework as a basis for identifying potential financial fraud risks and schemes, ensuring that preventive and detective controls are present and working as intended. Examples of fraud risks are contractor payments, wire transfers, travel card purchases, and theft of cash receipts.

As part of the Framework, potential fraud areas are identified and key controls are evaluated/implemented as proactive measures to fraud prevention. Although no system of internal control provides absolute assurance, the FDIC's system of internal control can provide reasonable assurance that key controls are adequate and working as intended. Monitoring activities include supervisory approvals, management reports, and exception reporting.

FDIC management performs due diligence in areas of suspected or alleged fraud. At the conclusion of due diligence, the matter is either dropped or referred to the Office of Inspector General for investigation.

During 2017, there has been no systemic fraud identified within the FDIC.

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, 2016, through September 30, 2017.

TABLE 1:
MANAGEMENT REPORT ON FINAL ACTION ON AUDITS WITH DISALLOWED COSTS FOR FISCAL YEAR 2017
Dollars in Thousands

	Audit Reports	Number of Reports	Disallowed Costs
A.	Management decisions – final action not taken at beginning of period	1	$55
B.	Management decisions made during the period	2	$6
C.	**Total reports pending final action during the period (A and B)**	**3**	**$61**
D.	1. Recoveries:		
	(a) Collections & offsets	3	$79[1]
	(b) Other	0	$0
	2. Write-offs	0	$0
	3. Total of 1 & 2	**3**	**$79**
E.	Audit reports needing final action at the end of the period	**0**	$0[2]

[1] Amount collected in D1(a) included excess recoveries of $18,000 for one report, EVAL-16-005.

[2] The amount is zero because all recoveries were collected during the reporting period.

TABLE 2:
MANAGEMENT REPORT ON FINAL ACTION ON AUDITS WITH RECOMMENDATIONS TO PUT FUNDS TO BETTER USE FOR FISCAL YEAR 2017
Dollars in Thousands

(There were no audit reports in this category.)

TABLE 3:
AUDIT REPORTS WITHOUT FINAL ACTIONS BUT WITH MANAGEMENT DECISIONS OVER ONE YEAR OLD FOR FISCAL YEAR 2017

Report No. and Issue Date	OIG Audit Finding	Management Action	Disallowed Costs
AUD-14-002 11/21/2013	The Director, Division of Administration (DOA) should coordinate with Division of Information Technology (DIT) and FDIC division and office officials, as appropriate, to address potential gaps that may exist between the 12-hour timeframe required to restore mission essential functions following an emergency and the 72-hour recovery time objective for restoring mission critical applications.	The Chief Information Officer Organization developed cost estimates for recovering applications within 12-72 hours and prepared a Board Case that presented the approach for meeting the associated continuity of operations objectives. Due Date: Subsequently Closed	$0
AUD-15-008 09/16/2015	The Directors of RMS and DCP should coordinate to assess the effectiveness of the FDIC's supervisory policy and approach with respect to the issues and risks discussed in this report after a reasonable period of time is allowed for implementation.	RMS, jointly with DCP, is developing the scope and methodology for the Survey, which will include participation of a cross-section of personnel in three regions to assess their implementation and understanding of supervisory guidance. The Survey will include a final written document summarizing the results. Due Date: 3/30/2018	$0
AUD-16-001 10/28/2015	The Acting CIO should assess the ISM Outsourced Information Service Provider Assessment Methodology processes supporting information service provider assessments to determine and implement any needed improvements to ensure timely completion of assessments.	The Chief Information Officer Organization has developed a new methodology for managing the process. A transition plan will be developed and executed to ensure timely completion of assessments while the new methodology is being phased in. Due Date: 6/30/2018	$0
AUD-16-004 07/07/2016	The CIO should revise procedures and controls for incident handling, to include major incidents, to ensure that risks associated with these incidents are sufficiently documented and supported by appropriate evidence.	Procedures were revised and controls improved to ensure that risks associated with incidents, to include major incidents, are sufficiently documented and supported by appropriate evidence. Due Date: Completion undergoing independent review.	$0