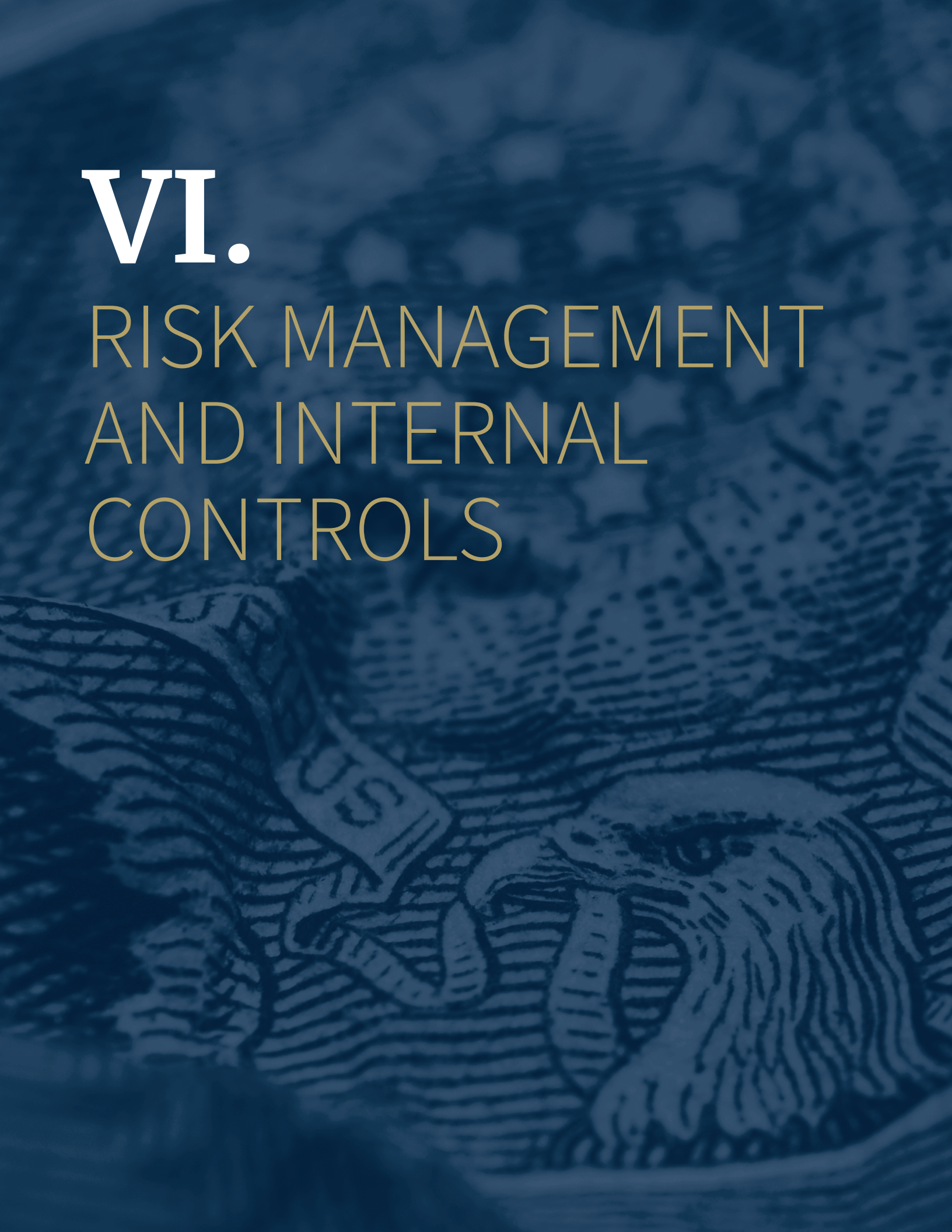

VI.

RISK MANAGEMENT AND INTERNAL CONTROLS

The FDIC uses several means to identify and address enterprise risks, 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 Modernization Act of 2014 (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 (DOF-RMIC) oversees a corporate-wide program of risk management and internal control activities and works closely with FDIC division and office management. The FDIC has made a concerted effort to identify and assess financial, reputational, and operational risks and incorporate corresponding controls into day-to-day operations. The program also requires that divisions and offices document comprehensive procedures, thoroughly train employees, and hold supervisors accountable for performance and results. Divisions and offices monitor compliance through periodic management reviews and various activity reports distributed to all levels of management. The FDIC also takes seriously FDIC Office of Inspector General and GAO audit recommendations and strives to implement agreed upon actions promptly. The FDIC has received unmodified opinions on its financial statement audits for 29 consecutive years, and these and other positive results reflect the effectiveness of the overall management control program.

In 2020, DOF-RMIC continued to enhance the FDIC's Enterprise Risk Management (ERM) program. The focus was raising awareness of ERM in the FDIC regional offices and initial actions to integrate the program with the FDIC's strategic planning and budget process.

During 2021, DOF-RMIC will continue integrating the ERM program with FDIC's strategic planning and budget process, enhancing the internal control program, and exploring opportunities for process improvements.

PROGRAM EVALUATION

DOF-RMIC periodically evaluates selected program areas responsible for achieving FDIC strategic objectives and performance goals. During 2020, DOF-RMIC evaluated DIR processes for achieving one of the Insurance Program's strategic objectives and related performance goals from the FDIC's 2020 Annual Performance Plan. The objective and goal evaluated and summary results follow.

Strategic Objective: The DIF and system remain strong and adequately financed.

Performance Goal: Monitor the status of the DIF reserve ratio and analyze the factors that affect fund growth. Adjust assessment rates as necessary.

Targets: 1) Provide updated fund balance projections to the FDIC Board of Directors semiannually; and 2) Recommend changes to deposit insurance assessment rates to the FDIC Board of Directors, as necessary.

The objective of DOF-RMIC's evaluation was to determine if DIR has effective processes in place to achieve the performance goal. DOF-RMIC reviewed FDIC Board briefing materials for the semiannual projection of the DIF balance and Reserve Ratio, the FDIC Quarterly Banking Profile, the Summary of Assessments Changes Report, a DIR memorandum to the FDIC Board regarding Restoration Plan recommendations, and relevant information on DIR's internal website. Additionally, DOF-RMIC held interview sessions with senior officials and economists from DIR's Financial Risk Management, Large Bank Pricing, and Banking and Regulatory Policy sections. DOF-RMIC is familiar with the DIR operations from ongoing risk management and internal control-related collaboration activities.

The evaluation noted that DIR has systems and processes in place to:

- Compute assessments based on risk profiles of insured institutions,

- Monitor growth in the assessment base and changes in the assessment rates,
- Track overall banking industry trends,
- Forecast future investment income, and
- Collaborate and review data on problem institutions and potential bank failures.

DOF-RMIC concluded that DIR has an effective process in place to achieve the performance goal and targets and to make sound DIF and reserve ratio projections and recommendations to the FDIC Board.

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 ERM and internal control program considers the potential for fraud and incorporates elements of Principle 8—Assess Fraud Risk—from the GAO's *Standards for 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 and ensuring that preventive and detective controls are present and working as intended. Examples of transactions more susceptible to fraud include contractor payments, wire transfers, travel card purchases, and cash receipts.

As part of the Framework, management identifies potential fraud areas and implements and evaluates key controls as proactive measures to prevent fraud. Although no system of internal control provides absolute assurance, the FDIC's system of internal control provides 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 closed or referred to the Office of Inspector General for investigation.

During 2020, there was no systemic fraud identified within the FDIC.

MANAGEMENT REPORT ON FINAL ACTIONS

As required under the provisions of Section 5 of the Inspector General Act of 1978, as amended, 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, 2019, through September 30, 2020.

TABLE 1:
MANAGEMENT REPORT ON FINAL ACTION ON AUDITS WITH DISALLOWED COSTS FOR FISCAL YEAR 2020

	Audit Reports	Number of Reports	Disallowed Costs
A.	Management decisions – final action not taken at beginning of period	0	$0
B.	Management decisions made during the period	1	$47,489
C.	**Total reports pending final action during the period (A and B)**	**1**	**$47,489**
D.	Final action taken during the period:		
	1. Recoveries:		
	(a) Collections & offsets	1	$0
	(b) Other	0	0
	2. Write-offs	0	0
	3. Total of 1 & 2	**1**	**$0**
E.	Audit reports needing final action at the end of the period	1	$47,489

TABLE 2:
MANAGEMENT REPORT ON FINAL ACTION ON AUDITS WITH RECOMMENDATIONS TO PUT FUNDS TO BETTER USE FOR FISCAL YEAR 2020

(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 2020

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
AUD-17-001 11/2/2016	OIG recommends that the CIO should review existing resource commitments and priorities for addressing data communications (DCOM) plan of actions & milestones (POA&Ms) and take appropriate steps to ensure they are addressed in a timely manner.	The CIOO worked with teams to develop risk tolerances levels for the FDIC Policy 19-001, on Management of POA&Ms, which reflect the level of risk associated with open POA&Ms, including the acceptable amount of time needed to address them. Furthermore, an Integrated Project Team has been established to work with System Owners to ensure timely remediation of POA&Ms and to conduct root cause analyses to develop a revised process to prevent overdue POA&Ms that fall outside of tolerance levels. Substantial progress in addressing DCOM POA&Ms in a timely manner has been achieved. Due Date: 6/30/2021	$0
AUD-18-004 7/26/2018	The CIO should identify and document the IT resources and expertise needed to execute the FDIC's IT Strategic Plan.	The CIOO developed a workforce planning guide that outlines the process that will be used to document the IT resources and expertise needed to execute the FDIC's IT Strategic Plan. Status: Completed. Undergoing OIG review.	$0

TABLE 3:
AUDIT REPORTS WITHOUT FINAL ACTIONS BUT WITH MANAGEMENT DECISIONS OVER ONE YEAR OLD FOR FISCAL YEAR 2020 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
AUD-19-003 12/10/2018	The Deputy to the Chairman and Chief Operating Officer should determine the portion of the $7,510 in unsupported labor charges that should be disallowed and recover that amount. The Deputy to the Chairman and Chief Operating Officer should determine whether the remaining labor charges under Task Orders 4 and 5 are unsupported charges that should be disallowed. The Deputy to the Chairman and Chief Operating Officer should determine the portion of the $39,979 in unallowable labor charges that should be disallowed and recover that amount. The Deputy to the Chairman and Chief Operating Officer should determine whether additional labor charges should be disallowed for off-site work performed under Task Orders 4 and 5 that were not covered by the audit.	On June 23, 2020, DOA sent a demand letter to Pragmatics identifying $103,634.36 in unsupported and disallowed labor charges invoiced to the FDIC. Pragmatics agreed to pay back the $103,634.36. The funds have been collected from Pragmatics. Status: Subsequently closed.	$47,489
EVAL-19-001 4/9/2019	The Deputy to the Chairman and Chief Operating Officer should document the justifications for the physical security activities that the FDIC has taken in response to recommendations, including decisions to accept risk or regarding expenditures for security countermeasures above the recommended standards for an assigned facility security level.	The revised Circular 1610.1 is in the directives review process. Comments have been received and are being reviewed. Status: Subsequently closed.	$0

TABLE 3:
AUDIT REPORTS WITHOUT FINAL ACTIONS BUT WITH MANAGEMENT DECISIONS OVER ONE YEAR OLD FOR FISCAL YEAR 2020 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
EVAL-19-002 9/24/2019	We recommend that the Directors of RMS and DCP establish, implement, and document a process to assess the effectiveness of the MDI Program supervisory strategies. We recommend that the Directors of RMS and DCP issue guidance to the Regional Offices defining the types of activities that comprise technical assistance, as distinct from training, education, and outreach.	RMS and DCP updated examiner instructions to require preparation of a separate written document, at the conclusion of each examination, which outlines the elements of the prior supervisory strategy, evaluates the effectiveness of those elements and recommends any changes in strategy or escalation of responses. These assessments will be submitted to the MDI Program Office, which will conduct periodic horizontal reviews of the individual assessments. Any key trends or findings from the horizontal reviews will be communicated back to the regional offices for use in enhancing future supervisory strategies. In developing the instructions, the FDIC reviewed prior supervisory strategies to incorporate best practices. Status: Subsequently closed. RMS and DCP have prepared the definitions for technical assistance, training and education, and outreach and they are contained in an update to the MDI Regional Director Memo. Status: Subsequently closed.	$0