VI.

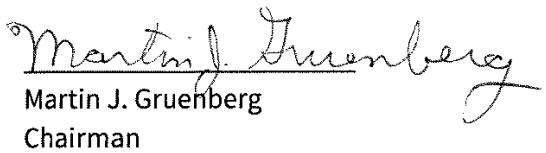
RISK MANAGEMENT AND INTERNAL CONTROLS

FDIC
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Office of the Chairman

Federal Deposit Insurance Corporation
Statement of Assurance

FDIC management is responsible for managing risks and maintaining effective internal controls. During the year, the FDIC conducted its assessment of risk and internal control in the spirit of OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. Based on our assessment and internal management evaluations, we can provide reasonable assurance that the objectives of Section 2 (internal controls) and Section 4 (financial management systems) of the Federal Managers' Financial Integrity Act of 1982 have been achieved, and that the FDIC has no material weaknesses. During 2023, we effectively remediated a significant deficiency in our internal control over contract documentation and contract payment review processes. We are committed to maintaining effective internal controls corporate-wide in 2024.

The FDIC also assessed the reliability of the performance data contained in this report in accordance with the Reports Consolidation Act of 2000. We found no material inadequacies and the data are considered to be complete and reliable.



Martin J. Gruenberg
Chairman

February 15, 2024

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 laws and 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 Office of Risk Management and Internal Controls (ORMIC) oversees a corporate-wide program of risk management and internal control activities and works closely with FDIC's 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 and their employees 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 32 consecutive years, and these and other positive results reflect the effectiveness of the overall management control program.

In 2023, the FDIC strengthened acquisition-related controls, expanded internal control testing efforts, enhanced the Division of Finance's internal control program, enhanced the fraud reporting structure, and matured our supply chain risk management program. ORMIC will continue these efforts in 2024 and will also implement an agency-wide enterprise change management program.

In September 2023, Stacie Alboum (left) and Jill Lennox (right) spoke at the ERM Risk Awareness Symposium.

In September 2023, ORMIC held its second annual ERM Risk Awareness Symposium where FDIC risk management experts shared information about significant risks facing the FDIC and how the agency is managing and addressing these risks and planning for the future. Presenters discussed deposit insurance coverage, IT modernization efforts, the FDIC's Intelligence and Threat Sharing Unit, and the Dodd-Frank Act's requirements for certain financial firms to create "living wills" that describe their strategies for effecting a rapid and orderly resolution in the event of material financial distress or failure.

Program Evaluation

ORMIC periodically evaluates selected program areas responsible for achieving FDIC strategic objectives and annual performance goals. During 2023, ORMIC evaluated the Division of Complex Institution Supervision and Resolution (CISR) processes for achieving the following strategic objective and related performance goal from the FDIC's 2023 Annual Performance Plan. The objective and goal evaluated and summary results follow.

Strategic Objective: In the event of the failure of a large, complex financial institution (LCFI), the FDIC carries out the resolution in an orderly manner in accordance with statutory mandates.

Performance Goal: Continue to build the FDIC's operational readiness to administer the resolution of LCFIs, including those designated as systemically important.

Targets:

1) Continue to refine plans and strategic options to ensure the FDIC's operational readiness to administer a resolution of LCFIs;
2) Continue to deepen and strengthen working relationships with key foreign jurisdictions, both on a bilateral basis and through multilateral fora.

The objective of ORMIC's evaluation was to determine if CISR has processes in place to achieve the performance goal and confirm that there is documentary support evidencing that the performance goal was met.

ORMIC reviewed CISR's 2023 Business Plan; the *2022-2024 FDIC Strategic Plan*; output from tracking systems used for monitoring implementation of two strategic goals and objectives; the Corporate Performance Goal Reporting System; a number of materials supporting steps taken to strengthen operational readiness, including the schedule of International Engagements – including descriptions, key outputs, and deliverables; the Trilateral Principal-Level Exercise (TPLE) Overview Presentation, the TPLE 2023 Senior Staff Communications Exercise – Post Exercise Survey Results, and the TPLE 2022 Briefing materials; Financial Stability Board Resolution Steering Group (ReSG) membership and Schedule of Meetings – including main agenda items; and Risk Assessment Process Questionnaires for Central Counterparties (CCP) Survey Responses and Information Needs for CCP Resolution Planning.

ORMIC held meetings with senior officials and staff from CISR's Operations Branch, and leveraged familiarity with CISR operations from ongoing risk management and internal control-related collaboration activities.

ORMIC evaluated CISR's processes related to this performance goal and noted that processes were in place to:

- Track goal milestones through completion;
- Track overall goals and objectives and CISR-led FDIC Performance Goals on a bi-weekly and quarterly basis, respectively;
- Continue to improve resolution planning by identifying and addressing gaps;
- Continue to engage with key stakeholders from domestic regulatory authorities, as well as foreign jurisdictions, and conduct simulation exercises to further support readiness;
- Hold TPLEs and information exchanges resulting in policy discussions, development of playbooks, and resolution strategies; and
- Hold TPLE Senior Staff Communications Exercises – with Post Exercise Survey Results.

ORMIC validated the processes in place by reviewing a variety of documents and deliverables, including the ReSG schedule of meetings, schedule of international engagements, agendas and agenda items, lists of participants, and outputs from the tracking systems. ORMIC

concluded that CISR has effective processes in place to achieve this performance goal and related targets for building and maintaining the FDIC's operational readiness to administer the resolution of LCFIs.

Additionally, ORMIC reviewed the OIG's recent evaluation entitled *The FDIC's Orderly Liquidation Authority*. CISR is currently addressing recommendations made by the OIG in their evaluation report to supplement the FDIC's resolution readiness capabilities. ORMIC tracks OIG recommendations and corrective actions through implementation and closure.

Internal Control Program – Fraud Risk Management

The FDIC's enterprise risk management 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*.[21] 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 reporting, and exception reporting.

FDIC management performs due diligence in areas of suspected or alleged fraud. In addition, the FDIC promptly refers instances of suspected fraud to the Office of Inspector General for investigation. FDIC continues to maintain a robust internal control environment designed to deter and detect fraud.

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 actions taken by management on audit reports for the federal fiscal year period October 1, 2022, through September 30, 2023.

[21] GAO's *Standards for Internal Control in the Federal Government* is available at https://www.gao.gov/products/gao-14-704g.

Table 1:
Management Report on Final Action on Audits with Disallowed Costs for Fiscal Year 2023

(There were no audit reports in this category.)

Table 2:
Management Report on Final Action on Audits with Recommendations to Put Funds to Better Use for Fiscal Year 2023

Dollars in Thousands

		Number of Reports	Funds Put To Better Use
A.	Management decisions – final action not taken at beginning of period	0	$0
B.	Management decisions made during the period	1	$1,500
C.	Total reports pending final action during the period (A and B)	1	$1,500
D.	Final action taken during the period:	0	$0
	1. Value of recommendations implemented (completed)	0	$0
	2. Value of recommendations that management concluded should not or could not be implemented or completed	0	$0
	3. Total of 1 and 2	0	$0
E.	Audit reports needing final action at the end of the period (September 30, 2023) * Note, the OIG closed this recommendation on December 4, 2023.	1	$1,500

Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2023

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
EVAL-20-001 10/28/2019	OIG recommends that the Deputy to the Chairman and Chief Operating Officer provide enhanced contract portfolio reports to FDIC executives, senior management, and the Board Directors.	The Division of Administration (DOA)'s Acquisition Services Branch (ASB) has identified the specific contract portfolio reporting enhancements that would be useful to FDIC executives, senior management, and the Board of Directors; and is determining the extent to which such reporting is producible using existing data and technology. DOA is working to identify reliable and efficient data sources to meet reporting needs. Due Date: 6/30/2024	$0
EVAL-21-002 3/31/2021	OIG recommends that the Deputy to the Chairman and Chief Operating Officer implement periodic reviews for procured Critical Functions, including for the Basic Ordering Agreements (BOAs) and task orders for Managed Security Services Provider and Security and Privacy Professional Services. OIG recommends that the Deputy to the Chairman and Chief Operating Officer determine when and how to assess for contractor overreliance as part of the management oversight strategy.	Status: Subsequently closed. Status: Subsequently closed.	$0

Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2023 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
EVAL-21-002 3/31/2021 (Continued)	OIG recommends that the Deputy to the Chairman and Chief Operating Officer implement corrective actions when the FDIC determines it is over-reliant on a contractor for a procured Critical Function.	Status: Subsequently closed.	
	OIG recommends that the Deputy to the Chairman and Chief Operating Officer report to the Board about the Procurement Risk Assessments, Management Oversight Strategies, and contract provisions that address identified risks for planned Critical Functions during the procurement planning phase of the acquisition, for its consideration.	DOA ASB implemented its template for essential contracts and revised its Acquisition Procedures and Guidance Manual (APGM) accordingly. DOA ASB is working to incorporate essential contracts into its report to the Board. Efforts are being made to include essential contracts in the Board Report for the fourth quarter of 2023. Due Date: 3/31/2024	
	OIG recommends that the Deputy to the Chairman and Chief Operating Officer report to the Board about the Contract Award Profile Reports and corresponding status reports for procured Critical Functions during the contract management phase of the acquisition process on an individual and aggregate contract basis, for its consideration.	DOA ASB implemented its template for essential contracts and revised its Acquisition Procedures and Guidance Manual (APGM) accordingly. DOA ASB is working to incorporate essential contracts into its report to the Board. Efforts are being made to include essential contracts in the Board Report for the fourth quarter of 2023. Due Date: 3/31/2024	

Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2023 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
REV-22-001 1/4/2022	We recommend that the Deputy to the Chairman, Chief Operating Officer, and Chief of Staff, in coordination with the General Counsel, develop and implement procedures for the FDIC to ensure contractors carry out their obligations under the Whistleblower Rights Notification Clause, including methods for verification that (1) all contractor and subcontractor employees of the FDIC are notified of their whistleblower rights and protections, and (2) clauses are appropriately included in subcontracts.	DOA ASB issued its Procurement Administrative Bulletin (PAB) 2022-07, Contractor Employee Whistleblower Rights, dated December 9, 2022. The PAB revises the clause to inform employees of Whistleblower Rights and requires the contractor and subcontractor to distribute a brochure pertaining to whistleblower information to employees working in support of the contract. Additional time is needed to add a certification requirement, which must be submitted through a lengthy process involving posting it in the *Federal Register*. Due Date: 8/31/2024	$0
AUD-22-003 1/18/2022	We recommend that the Director, RMS, coordinate with the Legal Division to establish and implement procedures for RMS threat information sharing activities.	RMS is addressing this corrective action together with a similar recommendation that was issued in the Sharing of Threat and Vulnerability Information with Financial Institutions report (EVAL-23-002) on August 29, 2023. Due Date: 3/31/2024	$0

Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2023 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
EVAL-22-003 3/1/2022	We recommend that the FDIC Senior Accountable Official for SCRM (Deputy to the Chairman and Chief Financial Officer) establish and implement metrics and indicators to continuously monitor and evaluate supply chain risks at the FDIC. We recommend that the Chief Information Security Officer implement SCRM controls of the NIST Risk Management Framework (RMF) for IT procurements.	Status: Recommendation closure package was submitted to the OIG. Due Date: 12/31/2023 The FDIC has selected the appropriate security controls from the SCRM control family from NIST SP 800-53 Rev 5. The SCRM team is coordinating across Divisions and Offices to implement the controls. Additional time is needed for Divisions and Offices to implement the selected SCRM controls, but staff anticipates this will be completed by the end of the first quarter of 2024. Due Date: 3/31/2024	$0

Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2023 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
EVAL-22-003 3/1/2022 (Continued)	We recommend that the FDIC Senior Accountable Official for SCRM (Deputy to the Chairman and Chief Financial Officer) in cooperation with the Deputy to the Chairman, Chief Operating Officer, and Director, Division of Administration develop and implement a process and procedures for conducting supply chain risk assessments.	Status: Recommendation closure package was submitted to the OIG. Due Date: 12/31/2023	
	We recommend that the FDIC Senior Accountable Official for SCRM (Deputy to the Chairman and Chief Financial Officer) in cooperation with the Deputy to the Chairman, Chief Operating Officer, and Director, Division of Administration: conduct supply chain risk assessments prior to entering into contracts with new suppliers/vendors.	Status: Recommendation closure package was submitted to the OIG. Due Date: 12/31/2023	

Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2023 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
EVAL-22-003 3/1/2022 (Continued)	We recommend that the FDIC Senior Accountable Official for SCRM (Deputy to the Chairman and Chief Financial Officer) in cooperation with the Deputy to the Chairman, Chief Operating Officer, and Director, Division of Administration: conduct supply chain risk assessments prior to substantive contract actions, including renewals, extensions, and exercising option periods.	Status: Recommendation closure package was submitted to the OIG. Due Date: 12/31/2023	
AUD-22-004 9/27/2022	We recommend that the CIO address the 31 Plan of Action and Milestones (POA&Ms) identified as of June 21, 2022, associated with NIST SP 800-53 Rev. 5 control SI-2 (Flaw Remediation).	The Acceptance of Risk for eight POA&Ms expired. The FDIC decided not to renew the Acceptance of Risk and instead focus on remediation. Additional time is needed to address the remaining POA&Ms due to competing priorities. Due Date: 10/31/2024	$0