

VI.

RISK MANAGEMENT AND INTERNAL CONTROLS





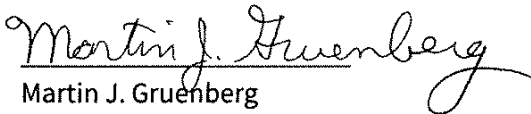
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

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. We are working to address a significant deficiency identified by the U.S. Government Accountability Office in our internal control over the contractor payment review process, and we are committed to maintaining effective internal controls corporate-wide in 2023.

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 9, 2023

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 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 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 31 consecutive years, and these and other positive results reflect the effectiveness of the overall management control program.

In 2022, the FDIC completed an agency-wide effort to raise risk awareness and continued to mature the Enterprise Risk Management (ERM) program and associated Risk Profile and Risk Inventory. The FDIC also enhanced contract administration and oversight management controls and increased independent testing of contract invoices and compliance with FDIC acquisition policies.

During 2023, ORMIC will continue to strengthen acquisition-related controls, expand internal control testing efforts, enhance the DOF internal control program, enhance the fraud reporting structure, and mature our supply chain risk management program.



PROGRAM EVALUATION

ORMIC periodically evaluates selected program areas responsible for achieving FDIC strategic objectives and performance goals. During 2022, ORMIC evaluated the Division of Risk Management Supervision (RMS) processes for achieving a strategic objective and related performance goal from the FDIC's 2022 Annual Performance Plan. The objective, the goal evaluated, and summary results follow.

Strategic Objective: The FDIC exercises its statutory authority, in cooperation with other primary federal regulators and state agencies, to promote safe-and-sound practices at FDIC-insured depository institutions, including appropriate risk management.

Performance Goal: Conduct on-site risk management examinations to assess the overall financial condition, management practices and policies, and compliance with applicable laws and regulations of FDIC-supervised depository institutions. When problems are identified, ensure IDIs promptly implement appropriate corrective programs and follow up to ensure that identified problems are corrected.

Targets: 1) Conduct all required risk management examinations within the timeframes prescribed by statute and FDIC policy; 2) For at least 90 percent of IDIs that are assigned a composite CAMELS rating of 2 and for which the examination report identifies "Matters Requiring Board Attention" (MRBAs), review progress reports and follow up with the institution within six months of the issuance of the examination report to ensure that all MRBAs are being addressed.

The objective of ORMIC's evaluation was to determine if RMS has processes in place to achieve the performance goal and confirm that there is documentary support confirming that the performance goal was met. ORMIC reviewed the National Examination Scheduling System (NESS) User Manual, RMS' Manual of Examination Policies, the Examination Summary Report, several Delinquency Reports, the RMS Monthly Trend Charts, the MRBA Summary Report, several RMS Director Memos to the Regional Directors on guidance, instructions, recording and tracking MRBA, the Virtual Supervisory Information on the Net System (ViSION) Procedures and Polices Reference Guide, an RMS Director Memo to Regional Directors on key supervisory information in ViSION, and relevant information on FDIC's external website and RMS' internal website. RMS provided ORMIC staff walkthroughs of the NESS and reports from ViSION. Additionally, ORMIC conducted interview sessions with senior officials and staff from RMS' Business Analysis and Decision Support Section. ORMIC is familiar with the RMS operations from on-going risk management and internal control-related collaboration activities.

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

- Determine when examinations are due,
- Determine the statutory required due date,
- Track examinations by hours, and by regions,
- Monitor examinations completed and delinquent examinations,

RISK MANAGEMENT AND INTERNAL CONTROLS

- Send reminders of examinations that are due,
- Provide dashboard reports and status reports to management,
- Perform data quality checks,
- Effectuate consistency in report of examination transmittal,
- Track and monitor IDI responses to MRBAs, and
- Report performance metrics and other pertinent information.

ORMIC validated the processes in place by reviewing manuals, guidance, systems data and reports generated. ORMIC concluded that RMS has effective processes in place to achieve this performance goal and targets; that is, conducting required risk management examinations, reviewing progress reports and following up timely with institutions on MRBA.

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
- 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—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 reporting, 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 2022, 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 actions taken by management on audit reports for the federal fiscal year period October 1, 2021, through September 30, 2022.

**Table 1:
Management Report on Final Action on Audits with Disallowed Costs
for Fiscal Year 2022**

(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 2022**

(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 2022 | | | |
|--|--|--|--|
| 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. | <p>DOA's Acquisition Services Branch (ASB) has developed a "Get to Green" Plan to clarify and focus its efforts to address certain unresolved audit recommendations that have presented a particular challenge to the division. In addition, ASB is developing a Strategic Framework that encompasses goals and objectives for providing acquisition lifecycle services and solutions in support of FDIC's mission, one aspect of which is optimizing data and reporting to drive business decisions. This recommendation is included in the scope of both the Plan and Framework.</p> <p>Moving forward, ASB plans to (1) identify the specific contract portfolio reporting enhancements that would be useful to FDIC executives, senior management, and the Board Directors; (2) determine the extent to which such reporting is producible using existing data and technology; (3) evaluate, from a cost-benefit standpoint, whether to develop, collect, or procure additional data or technology necessary to support enhanced reporting; and (4) provide enhanced contract portfolio reports to FDIC executives, senior management, and the Board Directors.</p> <p>Due Date: 6/30/23</p> | \$0 |

RISK MANAGEMENT AND INTERNAL CONTROLS

**Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old
for Fiscal Year 2022 (continued)**

| Report No. and Issue Date | OIG Audit Recommendation | Management Action | Disallowed Costs |
|--|---|---|-----------------------------|
| EVAL-20-003 2/4/2020 | OIG recommends that the FDIC establish, document, and implement policy and procedures for conducting retrospective cost benefit analyses on existing rules, including a regulatory risk assessment, as well as roles and responsibilities for the business line Divisions, Chief Economist, and Division of Insurance and Research/Regulatory Analysis Section (DIR/RAS). | Status: Subsequently closed. | \$0 |
| AUD-21-003 3/29/2021 | OIG recommends that the Deputy to the Chairman and Chief of Staff and COO ensure that Oversight Managers assigned to other FDIC contracts have verified the completion of Information Security and Privacy Awareness Training and Insider Threat and Counterintelligence Awareness Training for contractor and subcontractor personnel without network access. | DOA ASB has completed agreed-upon corrective actions and is working with the OIG to close this recommendation. Status: 2/15/2023 | \$0 |

**Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old
for Fiscal Year 2022 (continued)**

| Report No. and Issue Date | OIG Audit Recommendation | Management Action | Disallowed Costs |
|----------------------------------|--|---|---------------------|
| <p>EVAL-21-002 3/31/2021</p> | <p>OIG recommends that the Deputy to the Chairman and Chief Operating Officer incorporate the provisions of OMB Policy Letter 11-01 guidance into the FDIC Acquisition Policy Manual (August 2008) and Acquisition Procedures, Guidance and Information document (January 2020).</p> <p>OIG recommends that the Deputy to the Chairman and Chief Operating Officer identify Critical Functions during the procurement planning, award, and contract management phases of the acquisition process.</p> <p>OIG recommends that the Deputy to the Chairman and Chief Operating Officer conduct a procurement risk assessment for Critical Functions during the procurement planning process, for each contract involving Critical Functions. As part of the procurement risk assessment, OIG recommends inclusion of a cost effectiveness analysis.</p> | <p>ORMIC met with DOA ASB to discuss their findings to resolve these recommendations. Meetings have been held to outline next steps.</p> <p>Due Date: 4/15/2023</p> <p>DOA ASB, working with ORMIC, Legal and OIG, developed a template for determining essential contract needs. DOA ASB is working to incorporate the template into its acquisition policy.</p> <p>Due Date: 3/31/2023</p> <p>DOA ASB, working with ORMIC, Legal and OIG, developed a template for determining essential contract needs. DOA ASB is working to incorporate the template into its acquisition policy.</p> <p>Due Date: 3/31/2023</p> | <p>\$0</p> |

**Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old
for Fiscal Year 2022 (continued)**

| Report No. and Issue Date | OIG Audit Recommendation | Management Action | Disallowed Costs |
|---|--|--|---------------------|
| EVAL-21-002 3/31/2021 (continued) | <p>OIG recommends that the Deputy to the Chairman and Chief Operating Officer develop and implement a management oversight strategy for Critical Functions during the procurement planning process, for each contract involving Critical Functions.</p> <p>OIG recommends that the Deputy to the Chairman and Chief Operating Officer determine the contract structure during the solicitation and award process for the procurement of a Critical Function.</p> <p>OIG recommends that the Deputy to the Chairman and Chief Operating Officer revise the management oversight strategy for the procured Critical Functions performed under the Basic Ordering Agreements (BOAs) for Managed Security Services Provider (MSSP) and Security and Privacy Professional Services (SPPS) to ensure that the strategy aligns with best practices.</p> | <p>DOA ASB, working with ORMIC, Legal and OIG, developed a template for determining essential contract needs. DOA ASB is working to incorporate the template into its acquisition policy.</p> <p>Due Date: 2/15/2023</p> <p>DOA ASB, working with ORMIC, Legal and OIG, developed a template for determining essential contract needs. DOA ASB is working to incorporate the template into its acquisition policy.</p> <p>Due Date: 3/31/2023</p> <p>Following the FDIC’s study discussed in response to recommendation 1, the CIOO will assess whether any additional enhancements to the management oversight strategy for the MSSP and SPPS BOAs and task orders are needed beyond those already incorporated.</p> <p>Due Date: 6/30/2023</p> | \$0 |

**Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old
for Fiscal Year 2022 (continued)**

| Report No. and Issue Date | OIG Audit Recommendation | Management Action | Disallowed Costs |
|--|--|---|---------------------|
| <p>EVAL-21-002 3/31/2021 (continued)</p> | <p>OIG recommends that the Deputy to the Chairman and Chief Operating Officer identify missing or insufficient controls in the BOAs and task orders for Managed Security Services Provider and Security and Privacy Professional Services, and implement appropriate corrective actions or compensating controls.</p> <p>OIG recommends that the Deputy to the Chairman and Chief Operating Officer implement periodic reviews for procured Critical Functions, including for the BOAs and task orders for Managed Security Services Provider and Security and Privacy Professional Services.</p> <p>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.</p> | <p>Following the study discussed in response to Recommendation 1, the CIOO will assess whether any additional enhancements are needed for the MSSP and SPPS BOAs and task orders beyond those already incorporated.</p> <p>Due Date: 6/30/2023</p> <p>The FDIC will complete an annual performance review of MSSP and SPPS contractors. In addition, following the FDIC's study and actions in response to Recommendation 1 of the OIG report, the CIOO will assess the need for additional periodic reviews of such contracts and whether additional enhancements are required beyond the controls already incorporated.</p> <p>Due Date: 6/30/2023</p> <p>ORMIC met with DOA ASB to discuss their efforts to resolve these recommendations. Additional meetings have been held to outline next steps.</p> <p>Due Date: 10/15/2023</p> | |

**Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old
for Fiscal Year 2022 (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. | ORMIC met with DOA ASB to discuss their efforts to resolve these recommendations. Additional meetings have been held to outline next steps. Due Date: 10/15/2023 | |
| | 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. | ORMIC met with DOA ASB to discuss their efforts to resolve these recommendations. Additional meetings have been held to outline next steps. Due Date: 10/15/2023 | |
| | 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. | ORMIC met with DOA ASB to discuss their efforts to resolve these recommendations. Additional meetings have been held to outline next steps. Due Date: 10/15/2023 | |

**Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old
for Fiscal Year 2022 (continued)**

| Report No. and Issue Date | OIG Audit Recommendation | Management Action | Disallowed Costs |
|---------------------------------|---|--|---------------------|
| <p>AUD-21-004 8/3/2021</p> | <p>OIG recommends that the CIOO should update mobile device policies and relevant guidance that aligns with applicable federal regulatory requirements including NIST controls and will consider implementing recommended practices issued by authorities such as the GAO based on the FDIC’s operating environment, current business practices, and the results of the risk assessment the CIOO will conduct in response to Recommendation 1 of the OIG’s report.</p> <p>OIG recommends that the CIOO should establish a process to ensure Divisions and Offices provide approvals from managers to support the continued business need for zero usage devices and take actions accordingly.</p> | <p>CIOO updated the relevant directives below and submitted to Records and Information Management Unit (RIMU) for clearance: 3100.2 - Guidelines for the Use of Voice Telecommunications Services; 3100.4 - Wireless Telephone and Pager Assignments, Usage, Safeguards and Asset Management; and 1300.4 - Acceptable Use Policy for FDIC Information Technology.</p> <p>Status: Under ORMIC review</p> <p>The CIOO has established a process (i.e., the Wireless Audit Review Program) to report the details of zero use mobile and MiFi devices to the Divisions and Offices. The wireless device authorizing official from each Division or Office is then required to review the data and provide a decision within 30 days on whether or not to keep the service for device holders under their purview. The CIOO then terminates any services based on the audit results that have not been approved to remain in service.</p> <p>Status: Under ORMIC review</p> | <p>\$0</p> |

RISK MANAGEMENT AND INTERNAL CONTROLS

**Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old
for Fiscal Year 2022 (continued)**

| Report No. and Issue Date | OIG Audit Recommendation | Management Action | Disallowed Costs |
|--|---|---|-----------------------------|
| AEC-21-002 9/1/2021 | OIG recommends that the Deputy to the Chairman, Chief Operating Officer, and Chief of Staff develop and implement a process to collect and analyze the relevant data regarding employee retention across the FDIC and provide the data and analyses to Divisions and Offices. | DOA's Human Resources Branch (HRB) is collaborating with OMWI to review available source data for further analysis and reporting to Divisions and Offices. This effort will be thoughtful of privacy considerations and include the development and reporting of additional corporate retention metrics. Due Date: 3/31/2023 | \$0 |