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 2022.

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 GRUENBERG Digitally signed by MARTIN GRUENBERG

Martin J. Gruenberg
Acting Chairman

February 10, 2022

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

In 2021, ORMIC 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 formulation process.

During 2022, ORMIC will continue to enhance the ERM program, strengthen acquisition-related controls, and expand internal control testing efforts.

Program Evaluation

ORMIC periodically evaluates selected program areas responsible for achieving FDIC strategic objectives and performance goals. During 2021, ORMIC evaluated Division of Depositor and Consumer Protection (DCP) processes for achieving a strategic objective and related performance goal from the FDIC's 2021 Annual Performance Plan. The objective and goal evaluated and summary results follow.

Strategic Objective: Consumers have access to accurate and easily understood information about their rights and the disclosures due them under consumer protection and fair lending laws.

Performance Goal: Effectively investigate and respond to written consumer complaints and inquiries about FDIC-supervised financial institutions.

Targets: 1) Respond to 95 percent of written consumer complaints and inquiries within timeframes established by policy, with all complaints and inquiries receiving at least an initial acknowledgement within two weeks; 2) Publish, through the Consumer Response Center (CRC), an annual report regarding the nature of the FDIC's interactions with consumers and depositors; and 3) Publish on the FDIC's public website (https://www.fdic.gov) and regularly update performance metrics regarding FDIC's responsiveness to requests from the public for FDIC assistance.

The objective of ORMIC's evaluation was to determine if DCP 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 Center for Consumer and Depositor Assistance (NCDA) Consumer Response Unit (CRU) Operations Manual, the Discrimination Complaint Investigation Procedures, the CRU Consumer Complaints and Inquires Dashboard, the Transparency and Accountability: Consumer Protection and Deposit Annual Report, the Public Requests for FDIC Assistance Report, and relevant information on FDIC's external website and DCP's internal website. DCP provided ORMIC staff a walkthrough of the consumer complaints processing system and procedures. Additionally, ORMIC held interview sessions with senior officials and examination specialists from DCP's National Center for Consumer and Depositor Assistance Section, and the Internal Control and Review Unit, respectively. ORMIC is familiar with the DCP operations from on-going risk management and internal control-related collaboration activities.

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

- Promptly record complaints in the official system of record,
- Track complaint status and resolution through closure,
- Monitor stages and response times,
- Effectuate consistency in handling correspondence with similar issues,
- Perform quality control reviews, and
- Report performance metrics and other consumer information.

ORMIC validated the timeliness of the process by random selection of a complaint entered in the system and following it through from inception to completion. ORMIC concluded that DCP has an effective process in place to achieve its performance goal and targets; responding timely to written consumer complaints and inquiries, and makes consumer complaint information publicly available.

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 2021, 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, 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, 2020, through September 30, 2021.

Table 1:
Management Report on Final Action on Audits with Disallowed Costs for Fiscal Year 2021

(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 2021

(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 2021

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 OCIO 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. Substantial progress has been made in closing out several aging POA&Ms. 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. Status: Undergoing ORMIC Review	$0

Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2021 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
AUD-20-001 10/23/2019	OIG recommends that the CIO monitor employee and contractor compliance with policy requirements for properly safeguarding sensitive electronic and hardcopy information.	The CIOO has established a plan, in coordination with relevant stakeholders, to monitor the security of hardcopy information in common areas via facility walkthroughs. This plan was implemented in phases starting with facility walkthroughs of common office areas. Using existing communications channels, the CIO reminded Division and Office leadership of policy requirements applicable to protecting sensitive electronic and hardcopy information by employees and contractors. Status: Undergoing ORMIC Review	$0

Table 3: Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2021 (continued)

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 Information Technology (DIT), working with Division of Administration (DOA) Acquisition Services Branch (ASB), developed a report: Report of Increased/ Decreased Award Amounts for Contracts and TOs (Task Orders) to capture key data to enhance the analyses and reporting to support the contracting program. Additional changes have since been made to the data within the Report and to its format based on feedback received by ASB. FDIC met with the OIG staff to discuss these changes. DOA is assessing the need to add any additional information to the Report. Due Date: 6/30/2022	$0

Table 3:
Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2021 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
AUD-20-003 12/18/2019	OIG recommends that the CIO/CPO (Chief Privacy Officer)develop and provide privacy plans for all information systems containing PII consistent with OMB Circular A-130.	The FDIC Privacy Program has implemented a Privacy Continuous Monitoring (PCM) program that ensures that Privacy Plans are developed and approved for all information systems containing PII consistent with OMB Circular A-130. As indicated in the FDIC's IT systems Assessment and Authorization Process Guide (A&A Guide), the identification, selection, and periodic assessment of privacy controls has been fully integrated within FDIC's assessment and authorization process, which incorporates a risk management framework consistent with NIST 800-37. It guides and informs the categorization of Federal information and information systems; the selection, implementation, and assessment of security and privacy controls; the authorization of information systems and common controls; and the continuous monitoring of information systems. Status: Undergoing ORMIC Review	$0

Table 3: Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2021 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
AUD-20-003 12/18/2019 (continued)	OIG recommends that the CIO/CPO coordinate with the Chief Operating Officer (COO) to update policies and procedures to reflect the current organizational structure of the Privacy Program and responsibilities of agency personnel and component offices that support the FDIC's Privacy Program.	The CIOO has amended Privacy Program Directive (1360.20) which, upon finalization, will supersede this existing directive and will also supersede privacy program related directives: 1360.19 (Privacy Impact Assessment Requirements), 1311.1 (Measuring and Customizing User Activity on FDIC External Websites), and 1031.1 (Administration of the Privacy Act). Status: Undergoing ORMIC Review	$0

Table 3: Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2021 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
AUD-20-003 12/18/2019 (continued)	OIG recommends that the CIO/CPO develop and implement controls to ensure that PII stored in network shared drives and in hard copy is regularly monitored and reviewed for compliance with privacy laws, regulations, policy and guidelines.	All employees and contractors were sent global emails containing important guidance on protecting sensitive information. Additionally, FDIC has implemented the Physical Walkthrough Plan. To monitor compliance with policy requirements for safeguarding sensitive electronic information, the CIOO has developed and implemented a Standard Operating Procedure (SOP). The SOP includes identifying network shares with overly broad permissions, coordinating with the owning division or office, and restricting permissions appropriately. Status: Undergoing ORMIC Review	$0

Table 3: Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2021 (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 cost benefit analyses, including when and how the cost benefit analyses will be performed.	DIR developed a corporate directive to ensure the robust and consistent application of the principles established in the Statement of Policy on the Development and Review of Regulations and Policies approved by the FDIC Board of Directors. The directive details the process for analyzing the potential effects of regulatory actions and outlines specific roles and responsibilities for FDIC staff, including when such analysis will be performed. In addition, DIR developed staff guidance on analysis of FDIC regulations as a resource for FDIC staff involved in agency regulatory actions. The guidance outlines general concepts and best practices for regulatory analysis for staff use when preparing evaluations of the expected effects, costs and benefits of FDIC regulatory actions, and discusses how the analysis will be performed. Due Date: 3/31/2022	$0

Table 3: Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2021 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
EVAL-20-003 2/4/2020 (continued)	OIG recommends that the FDIC establish, document, and implement policy and procedures that clearly define the roles and responsibilities for the Regulatory Analysis Section (RAS), and early involvement for the RAS in participating in and framing the initial policy direction of a rule.	The FDIC has drafted a corporate directive and procedures for these recommendations. The directive and guidance are currently under final review. Due Date: 3/31/2022	$0
	OIG recommends that the FDIC establish, document, and implement policy and procedures that clearly define the Chief Economist's roles and responsibilities for reviewing and concurring on cost benefit analyses performed.	The FDIC has drafted a corporate directive and procedures addressing these recommendations. The directive and guidance are currently under final review. The cost benefit directive and cost benefit analysis guidance will be implemented when the directive is issued and the guidance is finalized. Due Date: 3/31/2022	

Table 3: Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2021 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
EVAL-20-003 2/4/2020 (continued)	OIG recommends that the FDIC establish, document, and implement policy and procedures that address how cost benefit analyses and supporting information, such as scope and methodology, analyses, conclusions, and reconciliation to the Agency's final policy decision will be documented and published in the *Federal Register* to ensure transparency.	The FDIC has drafted a corporate directive and procedures addressing the recommendations. The directive and guidance are currently under final review. The cost benefit directive and cost benefit analysis guidance will be implemented when the directive is issued and the guidance is finalized. Due Date: 3/31/2022	$0

Table 3: Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2021 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
EVAL-20-007 9/30/2020	OIG recommends that the Director, Division of Risk Management Supervision (RMS) train examiners on the importance of understanding and documenting the independence and qualifications of internal auditor(s), and reviewing internal audit work papers and results.	RMS has completed the development of the Wheatfield Bank case study. This case study is based on the Enloe State Bank In-Depth Review and highlights the importance of early identification of risk and the subsequent use of appropriate supervisory responses. Participants analyze and discuss how unresolved weaknesses could affect various areas of the fictional bank. Participants also assess the effectiveness of regulatory supervision and consider other actions the FDIC could have taken to encourage the Board to implement timely corrective action. Status: Subsequently closed.	$0

Table 3: Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2021 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
EVAL-20-007 9/30/2020 (continued)	OIG recommends that the Director, RMS train examiners on the importance of adequate annual external financial audit coverage, and under what circumstances and with what justifications banks may obtain reviews in place of audits.	RMS has completed the development of the Wheatfield Bank case study. This case study is based on the Enloe State Bank In-Depth Review and highlights the importance of early identification of risk and the subsequent use of appropriate supervisory responses. Participants analyze and discuss how unresolved weaknesses could affect various areas of the fictional bank. Participants also assess the effectiveness of regulatory supervision and consider other actions the FDIC could have taken to encourage the Board to implement timely corrective action. Status: Subsequently closed.	$0

Table 3: Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2021 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
EVAL-20-007 9/30/2020 (continued)	OIG recommends that the Director, RMS enhance case study training to incorporate the lessons learned from Enloe State Bank in regard to performing additional procedures related to the bank's loan related activity.	RMS has completed the development of the Wheatfield Bank case study. This case study is based on the Enloe State Bank In-Depth Review and highlights the importance of early identification of risk and the subsequent use of appropriate supervisory responses. Participants analyze and discuss how unresolved weaknesses could affect various areas of the fictional bank. Participants also assess the effectiveness of regulatory supervision and consider other actions the FDIC could have taken to encourage the Board to implement timely corrective action. Status: Subsequently closed.	$0

Table 3: Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2021 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
EVAL-20-007 9/30/2020 (continued)	OIG recommends that the Director, RMS train examiners on the importance of ensuring that information system user access controls be adequately tested.	RMS conducted nationwide training for all Commissioned Examiners, Case Managers, Commissioned Examination Specialists, and RMS Managers. The comprehensive training reinforces the principles of the existing statutory framework and supervisory guidance in its case study library as well as incorporating additional elements of fraud into its case study library. Status: Subsequently closed.	$0
	OIG recommends that the Director, RMS train examiners to perform additional procedures to determine the likelihood of fraud once a dominant official designation is made at a bank with a weak internal control environment.	RMS conducted nationwide training for all Commissioned Examiners, Case Managers, Commissioned Examination Specialists, and RMS Managers. The comprehensive training reinforces the principles of the existing statutory framework and supervisory guidance in its case study library as well as incorporating additional elements of fraud into its case study library. Status: Subsequently closed.	

Table 3: Audit Reports Without Final Actions but with Management Decisions over One Year Old for Fiscal Year 2021 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
EVAL-20-007 9/30/2020 (continued)	OIG recommends that the Director, RMS train examiners on indicators of fraud and how individual issues identified during an examination should be considered holistically to facilitate fraud detection.	RMS conducted nationwide training for all Commissioned Examiners, Case Managers, Commissioned Examination Specialists, and RMS Managers. The comprehensive training reinforces the principles of the existing statutory framework and supervisory guidance in its case study library as well as incorporating additional elements of fraud into its case study library. Status: Subsequently closed.	$0