VI.

RISK MANAGEMENT AND INTERNAL CONTROLS

THIS PAGE INTENTIONALLY LEFT BLANK

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

In 2019, DOF-RMIC continued to enhance the FDIC's Enterprise Risk Management program. ERM program accomplishments include, but were not limited to:

- Enhancing the ERM program's governance structure,
- Confirming the FDIC's risk appetite statement and risk profile,
- Relaunching the Model Risk Management program, and
- Providing Project Risk Manager support for certain complex IT projects.

During 2020, DOF-RMIC will continue enhancing the ERM program. DOF-RMIC will focus on raising ERM awareness in the FDIC regional offices, better 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 2019, DOF-RMIC evaluated DRR processes responsible for achieving two Insurance Program strategic objectives and related performance goals.

Strategic Objective and Related Performance Goal Evaluated:

- The FDIC resolves failed IDIs in the manner least-costly to the DIF.
  - Market failing institutions to all known qualified and interested potential bidders.

The FDIC maintains a database of qualified and interested potential bidders for failed financial institutions. In developing the potential bidders list, the FDIC identifies well-capitalized and well-managed banks that are expected to be interested in acquiring the failing institution. During 2019, four financial institutions failed. FDIC marketed these institutions using a secured web-based virtual data room. This approach allowed the FDIC to effectively and efficiently market the failing institution and its assets to potential bidders in a confidential manner. We confirmed in each case that the marketing process was competitive and multiple interested banks submitted bids.

Strategic Objective and Related Performance Goals Evaluated:

- Customers of failed IDIs have timely access to insured funds and financial services.
  - Depositors have access to insured funds within one business day if the failure occurs on a Friday.
  - Depositors have access to insured funds within two business days if the failure occurs on any other day of the week.
  - Depositors do not incur any losses on insured deposits.
  - No appropriated funds are required to pay insured depositors.

The FDIC has procedures in place to ensure that customers have timely access to insured funds and financial services, such as automated teller machines, safe deposit boxes, and wire services. If an institution failure occurs on a Friday, FDIC's target for access to insured funds by customers is one business day. If a failure occurs on any other day of the week, the target is two business days. We confirmed that procedures were up-to-date and appropriate. In 2019, four banks failed. The acquiring institution in three of the failures assumed all deposits and the fourth acquiring institution assumed insured deposits only. In all cases, DRR completed the deposit insurance determination timely and the acquiring institutions re-opened for business by the first business day immediately following the Friday failure. Moreover, no depositors incurred losses on insured deposits and no appropriated funds were used to pay insured deposits.

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—from 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 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 for fraud prevention. 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 2019, there was no systemic fraud identified within the FDIC.

MANAGEMENT REPORT ON FINAL ACTIONS

As required under the provisions of Section 5 (as amended) 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, 2018, through September 30, 2019.

TABLE 1:
MANAGEMENT REPORT ON FINAL ACTION ON AUDITS WITH DISALLOWED COSTS FOR FISCAL YEAR 2019

Dollars in Thousands

(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 2019

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 2019

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
AUD-16-001 10/28/2015	The Acting CIO should assess the Information Security Manager (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 CIOO updated its assessment methodology to help ensure timely completion of assessments and completed assessments consistent with its implementation plan. Status: Completed. Undergoing OIG review.	$0
AUD-17-001 11/2/2016	OIG recommends that the CIO should review existing resource commitments and priorities for addressing data communications Plans of Action and Milestones (POA&Ms) and take appropriate steps to ensure they are addressed in a timely manner.	The CIOO developed and documented its policy risk tolerance levels and timeframes for remediating POA&Ms. The FDIC has achieved a substantial reduction in several aging POA&M performance metrics. Additional time is needed to refine and meet performance benchmarks. Due Date: 6/26/2020.	$0
EVAL-17-007 9/18/2017	The Director, DOA should incorporate a risk assessment of individual separating employees into the FDIC's pre-exit clearance process.	DOA established procedures and protocols for incorporating an employee-specific risk assessment as part of the pre-exit clearance process. Status: Subsequently closed.	$0

TABLE 3:
AUDIT REPORTS WITHOUT FINAL ACTIONS BUT WITH MANAGEMENT DECISIONS OVER ONE YEAR OLD FOR FISCAL YEAR 2019 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
AUD-18-001 10/25/2017	The CIO should implement the Information Security Risk Advisory (ISRA) Council's responsibilities to develop a method and strategy for use by FDIC divisions and offices in the classification of risk ratings and risk profiles of corporate applications and systems. The CIO should implement the ISRA Council's responsibilities to develop and communicate the FDIC's information security risk tolerance level and risk profile used to prioritize risk mitigation activities. The CIO should ensure that the improvements to the FDIC's patch management process result in systems being patched in accordance with FDIC's patch management policy and National Institute of Standards and Technology recommended practices.	The CIOO developed a new methodology for categorizing applications and systems based on their risk profile. However, additional time is needed to fully implement the new methodology. Due Date: 1/31/2020 The FDIC issued its Corporate Risk Appetite Statement, which includes a discussion of technology risk. The CIOO developed risk tolerances and metrics for monitoring key risk indicators. Due Date: 1/28/2020 The FDIC established patch management risk tolerances and is monitoring to ensure that systems are patched within established timeframes. In addition, the FDIC updated its patching policy to incorporate a new process for documenting deferrals and acceptances of risk, when appropriate. Further, the FDIC developed work instructions to ensure the process of monitoring vulnerabilities and tolerance levels is repeatable. Status: Subsequently closed.	$0

TABLE 3:
AUDIT REPORTS WITHOUT FINAL ACTIONS BUT WITH MANAGEMENT DECISIONS OVER ONE YEAR OLD FOR FISCAL YEAR 2019 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
AUD-18-001 10/25/2017 (continued)	The CIO should review and enhance the FDIC's vulnerability scanning processes to ensure that issues associated with conducting credentialed scans are resolved in a timely manner.	The FDIC revised its standard operating procedure for addressing authentication failures. The procedure now requires evidence of successful authentication prior to closing change control tickets generated as a result of authentication failures. The FDIC still needs to demonstrate consistent, effective performance of the new procedures. Due Date: 5/29/2020	$0
	The CIO should develop an approach and implementing procedures for evaluating risk associated with known security weaknesses and vulnerabilities to ensure they collectively remain within established risk tolerance levels.	The CIOO developed standard risk tolerances for information security vulnerabilities, developed a framework to quantify risk, and integrated these items into the CIOO's risk management processes. Additionally, the CIOO updated its Information Security Risk Management directive to align roles, responsibilities, and expectations for reporting risk levels that approach or exceed risk tolerance limits. The CIOO will finalize and publish the directive once the directives review process is complete. Due Date: 5/29/2020	

TABLE 3:
AUDIT REPORTS WITHOUT FINAL ACTIONS BUT WITH MANAGEMENT DECISIONS OVER ONE YEAR OLD FOR FISCAL YEAR 2019 (continued)

Report No. and Issue Date	OIG Audit Recommendation	Management Action	Disallowed Costs
AUD-18-004 7/26/18	The CIO should implement an enterprise architecture that is part of the FDIC's IT Governance Framework and used to guide IT decision-making.	The CIO implemented an enterprise architecture that is part of the FDIC's IT Governance Framework and used to guide IT decision-making. Status: Subsequently closed.	$0
	The CIO should incorporate the revised IT governance processes into applicable FDIC policies, procedures, and charters.	The CIOO combined existing IT governance policies into one overarching directive which will define the FDIC's IT decision-making framework for governing and managing IT resources for enterprise architecture, IT strategy, IT planning, data management, and IT project management. The CIOO will finalize and publish the directive once the directives review process is complete. Due Date: 3/31/2020	
	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. The CIOO will perform the IT workforce assessment against future IT workforce needs as defined in the FDIC's IT Modernization Plan and target IT architecture. Due Date: 9/30/2020	
EVAL-18-004 8/8/2018	The Director, Division of Risk Management Supervision should issue a comprehensive policy guidance document defining Forward-Looking Supervision, including its purpose, goals, roles, and responsibilities.	RMS issued a comprehensive document describing its risk-focused supervision program, including how the FDIC implemented Forward-Looking Supervision concepts. Status: Subsequently closed.	$0