VI. RISK MANAGEMENT AND INTERNAL CONTROLS

THIS PAGE INTENTIONALLY LEFT BLANK

The FDIC uses several means to 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 (RMIC) oversees a corporate-wide program of relevant activities by establishing policies and working with management in each division and office in the FDIC. The FDIC has made a concerted effort to ensure that financial, reputational, and operational risks have been identified and that corresponding control needs are being incorporated into day-to-day operations. The program also requires that comprehensive procedures be documented, employees be thoroughly trained, and supervisors be held accountable for performance and results. Compliance monitoring is carried out through periodic management reviews and by the distribution of various activity reports to all levels of management. Conscientious attention is also paid to the implementation of audit recommendations made by the FDIC Office of Inspector General, the GAO, and other providers of external/audit scrutiny. The FDIC has received unmodified opinions on its financial statement audits for 27 consecutive years, and these and other positive results reflect the effectiveness of the overall management control program.

In 2018, efforts were focused on enhancing FDIC's Risk Management program (updating the enterprise risk management and internal control directive, drafting the risk appetite statement, updating the risk profile), improving data mining capabilities, identifying performance metrics, mapping key operational areas, exploring opportunities for process improvement, monitoring FDIC's internal controls over outsourced service providers, continuing efforts with stakeholders on failed bank data, and system security. Considerable energy was devoted to ensuring that the FDIC's processes and systems of control have kept pace with the workload, and that the foundation of controls throughout the FDIC remained strong.

During 2019, RMIC will focus on the Corporate Enterprise Risk Management Program, Model Risk Management validation, enhancing the internal control program, exploring opportunities for process improvement, monitoring FDIC's internal controls over outsourced service providers, and system security. Also, continued emphasis and management scrutiny will be applied to the accuracy and integrity of transactions and oversight of systems development efforts in general.

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, of 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, ensuring that preventive and detective controls are present and working as intended. Examples of fraud risks are contractor payments, wire transfers, travel card purchases, and theft of cash receipts.

As part of the Framework, potential fraud areas are identified and key controls are evaluated/implemented as proactive measures to fraud prevention. Although no system of internal control provides absolute assurance, the FDIC's system of internal control can provide 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 2018, 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, 2017, through September 30, 2018.

TABLE 1:
MANAGEMENT REPORT ON FINAL ACTION ON AUDITS WITH DISALLOWED COSTS FOR FISCAL YEAR 2018
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 2018
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 2018

Report No. and Issue Date	OIG Audit Finding	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 FDIC needs additional time to bring the 22 remaining contracts into compliance consistent with recently developed transition and action plans. Due Date: 4/30/2019	$0
EVAL-17-004 2/14/2017	The Director, RMS should continue to communicate to Financial Institutions (FIs) the importance of: fully considering and assessing the risks that Technology Service Providers (TSPs) could have on the FI's ability to manage its own business continuity and incident response planning efforts; ensuring that contracts with TSPs include specific provisions that address FI-identified risks, protect FI interests, and provide details necessary to allow FIs to manage their own business continuity planning and incident response and reporting efforts through TSP operations; and clearly defining key contract terms that would be important in understanding FI and TSP rights and responsibilities in the event of a business disruption or computer security incident particularly for those contracts that FIs identify as critical or that have access to sensitive or personally identifiable information.	Due to the significant coordination required with many agencies, the review and editing of the draft Federal Financial Institutions Examination Council's (FFIEC) Business Continuity Planning Booklet and FFIEC Outsourcing Booklet have experienced significant delays. The agencies are attempting to make the booklets more user-friendly. Due Date: 12/31/2019	$0

TABLE 3:
AUDIT REPORTS WITHOUT FINAL ACTIONS BUT WITH MANAGEMENT DECISIONS OVER ONE YEAR OLD FOR FISCAL YEAR 2018 (continued)

Report No. and Issue Date	OIG Audit Finding	Management Action	Disallowed Costs
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.	Additional time is needed for DOA to assess currently-available operational and analytical tools to determine what tools can be used in supporting the Insider Threat and Counterintelligence Program (ITCIP). DOA will continue to analyze existing internal analytic capabilities and work with the CIOO to establish cybersecurity monitoring and mitigation capabilities (e.g., forensics, incident management systems, and data loss prevention methodologies) while protecting individual legal and privacy rights. The procedures and protocols will be drafted for appropriate review once the tools are identified and put into place. Due Date: 3/29/2019	$0
	The Director, DOA, should work with the FDIC's Chief Information Officer to establish appropriate policy for using Data Loss Prevention (DLP) to support the FDIC's pre-exit clearance process.	More time is needed to complete the revisions to the Directive and to allow for sufficient time for the Directive Review Process. Due Date: 3/29/2019	
	The Director, DOA, should work with the FDIC's Chief Information Officer to develop an expanded and better defined use of the Data Loss Prevention (DLP) tool for separating contractors.	As the process for notification for contractor personnel is different than the process for employees, more time is needed to effectuate this change so that the Computer Security Incident Response Team (CSIRT) is notified in a timely fashion. Due Date: 2/18/2019	