FDIC Office of Inspector General

The FDIC's Information Security Program–2024

Evaluation Report - Final - Audits, Evaluations, and Cyber

September 2024 | **No.** EVAL-24-07

Office of Inspector General

REDACTED VERSION
PUBLICLY AVAILABLE

The redactions contained in this report are based upon requests from FDIC senior management to protect the Agency's information from disclosure.

Integrity • Independence • Accuracy • Objectivity • Accountability

NOTICE

Pursuant to Pub. L. 117-263, section 5274, non-governmental organizations and business entities identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Comments must be submitted to comments@fdicoig.gov within 30 days of the report publication date as reflected on our public website. Any comments will be appended to this report and posted on our public website. We request that submissions be Section 508 compliant and free from any proprietary or otherwise sensitive information.

The FDIC’s Information Security Program - 2024

Date: September 25, 2024

Memorandum To: Sylvia W. Burns
Chief information Officer

/s/
From: Terry L. Gibson
Assistant Inspector General for Audits, Evaluations, and Cyber

Subject The FDIC’s Information Security Program–2024 |
No. EVAL-24-07

Enclosed is the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) report on The FDIC’s Information Security Program–2024.

The FDIC OIG engaged with KPMG, LLP (KPMG) to conduct an evaluation of FDIC’s information security program. The contract required KPMG’s work to be conducted in accordance with the Quality Standards for Inspection and Evaluation issued by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). The objective was to assess the effectiveness of the FDIC’s information security program and practices.

KPMG is responsible for the enclosed report. The OIG reviewed KPMG’s report and related documentation and inquired of its representatives. Our review was not intended to enable the OIG to express, and we do not express, an opinion on the matters contained in the report. Our review found no instances where KPMG did not comply with the Quality Standards for Inspection and Evaluation issued by CIGIE.

We appreciate the cooperation and courtesies that Chief Information Officer Organization management and personnel extended to the OIG and KPMG during this evaluation. If you have any questions, please contact me at (703) 562-2529.

Executive Summary

The FDIC’s Information Security Program–2024 (EVAL-24-07) **September 25, 2024**

What We Did

We engaged with KPMG to assess the effectiveness of the FDIC’s information security program and practices. KPMG considered Federal Information Security Modernization Act (FISMA) requirements, National Institute of Standards and Technology (NIST) security standards and guidelines, the NIST Cybersecurity Framework, Office of Management and Budget policy and guidance, FDIC policies and procedures, and Department of Homeland Security guidance and reporting requirements to plan and perform the work and to conclude on the objective.

Impact on the FDIC

FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce risks to an acceptable level. Without effective controls for safeguarding its information systems and data, the FDIC would be at an increased risk of a cyberattack that could disrupt critical operations and allow inappropriate access to, and disclosure, modification, or destruction of, that FDIC information.

Results

KPMG determined that the FDIC’s overall information security program was operating at a Maturity Level 4 (Managed and Measurable) with respect to the FY 2024 FISMA Metrics. As shown in the table below, KPMG assigned a Managed and Measurable (Level 4) Rating for all five FISMA functions for FY 2024.

2024 Core and Supplemental Scores by Function

Function	Core	Supplemental	Maturity	Effectiveness
Identify	4.33	3.67	Level 4	Effective
Protect	3.50	3.63	Level 4	Effective
Detect	4.00	4.00	Level 4	Effective
Respond	3.50	4.00	Level 4	Effective
Recover	4.50	4.00	Level 4	Effective
Overall	**3.97**	**3.86**	**Level 4**	**Effective**

While KPMG found that the FDIC established a number of information security program controls and practices that were consistent with FISMA requirements, the report describes security control weaknesses that reduced the effectiveness of the FDIC’s information security program and practices. The security control weaknesses identified include:

- The FDIC Did Not Fully Enforce Plan of Actions and Milestones (POA&Ms) Documentation Requirements
- The FDIC Did Not Enforce Role-Based Training Requirements
- The FDIC Did Not Fully Implement Audit Logging Requirements on Assessed Information Systems
- The FDIC Did Not Review Audit Logs at Sufficient Frequency within Cloud Information Systems
- The FDIC Did Not Remediate Overdue POA&Ms Related to Flaw Remediation

Recommendations

KPMG made three new recommendations related to weaknesses identified during this year’s evaluation. In addition, there are two outstanding recommendations from prior FISMA reports along with other time-sensitive activities warranting the FDIC’s continued attention. The FDIC concurred with the recommendations and plans to complete corrective actions by September 30, 2025.

The FDIC’s Information Security Program - 2024

Part I

Part II

Part I

****

Report by KPMG

THE FEDERAL DEPOSIT INSURANCE CORPORATION'S INFORMATION SECURITY PROGRAM – 2024

EVALUATION REPORT

SEPTEMBER 25, 2024

KPMG LLP
1801 K Street NW
Washington DC 20006

TABLE OF CONTENTS

Terry L. Gibson
Assistant Inspector General for Audits, Evaluations, and Cyber
Office of Inspector General
Federal Deposit Insurance Corporation
3501 Fairfax Drive
Arlington, Virginia 22226

Subject: Evaluation of the Federal Deposit Insurance Corporation's Information Security Program – 2024

KPMG, LLP (KPMG) is pleased to submit the attached report detailing the results of our evaluation of the Federal Deposit Insurance Corporation's (FDIC) information security program in accordance with the Federal Information Security Modernization Act of 2014 (FISMA).[1] This report presents the results of our work conducted to address the evaluation objective relative to the FDIC. Our work was performed during the period of January 2024 through July 2024, and our results are as of July 31, 2024.

We conducted this evaluation in accordance with Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation (Blue Book). Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objective.

In addition to the Blue Book, we conducted this evaluation in accordance with Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA).[2] This evaluation did not constitute an audit of financial statements or an attestation level report as defined under Generally Accepted Government Auditing Standards (GAGAS) and the AICPA standards for attestation engagements.

FISMA directs federal agencies to report annually to the Office of Management and Budget (OMB) Director, Comptroller General, and selected congressional committees on the effectiveness of agency information security management programs and practices, and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security management program and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency Inspector General (IG) or an independent external auditor, as determined by the IG.

KPMG cautions that projecting the results of our evaluation to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

[1] The FY 2024 IG FISMA Reporting Metrics were developed by the OMB, the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE). KPMG assisted with the completion of the FY 2024 IG FISMA Reporting Metrics.

[2] Statements on Standards for Consulting Services are issued by the AICPA Management Consulting Services Executive Committee, the senior technical committee designated to issue pronouncements in connection with consulting services and can be found here: https://www.aicpa-cima.com/resources/download/statement-on-standards-for-consulting-services-no-1.

Terry L. Gibson
Federal Deposit Insurance Corporation
September 18, 2024
Page 2 of 2

This report is intended solely for the use of the Office of Inspector General (OIG) at the FDIC, as well as the FDIC management, or otherwise as required or allowed by law, and is not intended to be relied upon by anyone other than these specified parties, or otherwise as required or allowed by law.

Sincerely,

KPMG LLP

INTRODUCTION AND FDIC OVERVIEW

The Federal Information Security Modernization Act of 2014 (FISMA) was passed by Congress and signed into law by the President in 2014.[3] FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce risks to an acceptable level. FISMA assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB) to strengthen information security management programs.

FISMA directs NIST to develop standards and guidelines for helping to ensure the effectiveness of information security controls over information systems that support federal agencies' operations and assets. In response to this mandate, in February 2010, NIST published the *Risk Management Framework for Information Systems and Organizations* (NIST Risk Management Framework)[4] which was subsequently updated in December 2018. This framework is intended to guide agency efforts to establish effective information security management programs in compliance with FISMA. Specifically, the framework provides standards and guidelines to agencies for categorizing information systems, selecting security controls to meet minimum security requirements, performing risk and security controls assessments, authorizing systems to operate, performing monitoring activities to continually assess the adequacy of security controls in supporting agency operations, and developing corrective action plans to mitigate security risks identified throughout a system's lifecycle.

In response to the threat environment and technology ecosystem which continue to evolve and change at a faster pace each year, OMB implemented a new framework regarding the timing and focus of assessments in Fiscal Year (FY) 2022. The goal of this new framework was to provide a more flexible but continued focus on annual assessments for the federal community. This effort yielded two distinct groups of metrics: **Core and Supplemental**.[5] The "Core" metrics are high value controls to be assessed annually, whereas the "Supplemental" metrics are assessed at least once every two years and support the overall effectiveness of a security program. The "Core" and "Supplemental" metrics were developed and selected based on OMB guidance and alignment with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 2021) with the purpose to further modernize federal cybersecurity. OMB provided the following guidance:

- Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (M-22-09)[6]
- Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (M-22-01)[7]

[3] Pub. L. No. 113-283, 128 Stat. 3073 (2014). FISMA's obligations for Federal agencies and for Federal Inspectors General, as relevant to this evaluation, are codified chiefly at 44 U.S.C. §§ 3554 and 3555, respectively. The FDIC has determined that FISMA is legally binding on the FDIC.

[4] Risk Management Framework for Information Systems and Organizations, *NIST Risk Management Framework,* (December 2018) available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[5] FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, issued February 10, 2023.

[6] OMB, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," M-22-09 (January 26, 2022), available at: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[7] OMB, "Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response," M-22-01 (October 8, 2021), available at: https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf.

- Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31)[8]

The Department of Homeland Security (DHS) FISMA Reporting Metrics requires each agency's Inspector General (IG) to assess the effectiveness of their agency's information security program and practices using a maturity model. There are five levels of the maturity model: *Ad Hoc*, *Defined*, *Consistently Implemented*, *Managed and Measurable*, and *Optimized*. Maturity Level 1 (*Ad Hoc*) and Level 2 (*Defined*) are considered foundational, meaning not very mature, while Maturity Level 4 (*Managed and Measurable*) and Level 5 (*Optimized*) are considered advanced, meaning mature. OMB Memorandum M-24-04[9] provides agencies with FY 2024 reporting guidance and deadlines in accordance with FISMA.

According to the DHS FISMA Reporting Metrics, the foundational maturity levels help ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent to which agencies institutionalize those policies and procedures. Maturity Level 3 (*Consistently Implemented*) indicates that the organization has policies and procedures in place but must strengthen its quantitative and qualitative effectiveness measures for its security controls. Within the context of the maturity model, a Maturity Level 4 (*Managed and Measurable*) or higher indicates that the information security program is operating at an effective level of security.[10]

The Federal Deposit Insurance Corporation's (FDIC) Chief Information Security Officer (CISO), who reports directly to the Chief Information Officer (CIO), is delegated responsibility for establishing and maintaining the FDIC's information security and privacy policy, risk assessment, compliance, and oversight. The CISO oversees a group of information technology (IT) security and privacy professionals within the Office of the CISO (OCISO), which is part of the CIO Organization (CIOO).

The FDIC relies heavily on information systems to carry out its responsibilities of insuring deposits; examining and supervising financial institutions for safety, soundness, and consumer protection; making large and complex financial institutions resolvable; and managing receiverships. These systems contain Personally Identifiable Information (PII) and sensitive business information, including Social Security Numbers and bank account numbers for FDIC employees and depositors of failed financial institutions; confidential bank examination information, including supervisory ratings; and sensitive financial data, including credit card numbers. Without effective controls for safeguarding its information systems and data, the FDIC would be at an increased risk of a cyberattack that could disrupt critical operations and allow inappropriate access to, and disclosure, modification, or destruction of, that FDIC information.

[8] OMB, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," M-21-31 (August 27, 2021), available at: https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf.

[9] OMB, "Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements," M-24-04 (December 4, 2023), available at: M-24-04 (whitehouse.gov).

[10] Information regarding the determination of maturity level ratings can be found at https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act.

Evaluation Objective

The objective of this evaluation was to assess the effectiveness of the FDIC's information security program and practices. KPMG considered FISMA requirements, NIST security standards and guidelines, the NIST Cybersecurity Framework, OMB policy and guidance, FDIC policies and procedures, and DHS guidance and reporting requirements to plan and perform our work and to conclude on our evaluation objective. Appendix I contains more information about our scope and methodology to achieve the objective.

DHS FISMA Reporting Metrics and the NIST Cybersecurity Framework

FISMA Reporting Metrics

KPMG assessed the FDIC's implementation of system security controls based on criteria specified in NIST Special Publication (SP) 800-53 Revision (Rev.) 5, Security and Privacy Controls for Federal Information Systems and Organizations[11] and the FY 2024 IG FISMA Reporting Metrics. The following table shows the alignment of the FY 2024 IG FISMA Reporting Metric domain areas with the NIST Cybersecurity Framework Function areas (Table 1).

Table 1: NIST Cybersecurity Framework and Domain Area Alignment

Function Area	Function Area Objective	Domain Area(s)
Identify	Develop an organizational understanding of the business context and the resources that support critical functions to manage cybersecurity risk to systems, people, assets, data, and capabilities.	**Risk Management and Supply Chain Risk Management (SCRM)**
Protect	Implement safeguards to ensure delivery of critical infrastructure services, as well as to prevent, limit, or contain the impact of a cybersecurity event.	**Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training**
Detect	Implement activities to identify the occurrence of cybersecurity events.	**Information Security Continuous Monitoring (ISCM)**
Respond	Implement processes to take action regarding a detected cybersecurity event.	**Incident Response**
Recover	Implement plans for resilience to restore any capabilities impaired by a cybersecurity event.	**Contingency Planning**

Source: FY 2024 IG FISMA Reporting Metrics.

[11] NIST Special Publication 800-53 Revision 5, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Zero Trust Architecture

OMB Memorandum M-22-05[12] identified "Moving to a Zero Trust Architecture" as a key tenet to guide continued reforms under FISMA. OMB Memorandum M-22-09 – *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (dated January 26, 2022) – defined the Zero Trust Architecture Model as an environment in which "no actor, system, network, or service operating outside or within the security perimeter is trusted." M-22-09 defines five security objectives – Identity, Devices, Networks, Applications and Workloads, and Data – that support the Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Architecture Model:

- **Identity**: Federal staff have enterprise-managed accounts, allowing them to access applications while remaining reliably protected from targeted, sophisticated phishing attacks.
- **Devices**: The devices of Federal staff are consistently tracked and monitored, and the security posture of these devices is taken into account when granting access.
- **Networks**: Agency systems are isolated from each other, and the network traffic flowing between and within them is reliably encrypted.
- **Applications and Workloads**: Enterprise applications are tested internally and externally, and can be made available to staff securely over the internet.
- **Data**: Federal security and data teams work together to develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information.

OMB Memorandum M-22-09 directs agencies to achieve its objectives by the end of FY 2024. Starting in FY 2022, OMB began mapping Zero Trust Architecture control activities to specific FISMA Metrics. For example, one Identify function area Metric evaluates the organization's adoption of authentication mechanisms, which is relevant to the Identity objective. The FY 2024 FISMA guidance listed in M-24-04 states OMB will continue to align performance management under FISMA with benchmarks for the implementation of Zero Trust Architecture. Without a fully implemented Zero Trust Architecture, agencies could be at increased risk of cyberattacks, weakened access controls, inadequate data protection, and non-compliance with the memorandum.

In FY 2022, the FDIC developed and submitted a Zero Trust Implementation Plan with thirteen tasks for the FDIC to complete ("Zero Trust Tasks") to OMB in accordance with M-22-09 and assembled a Core Team and Task Force responsible for implementation. During FY 2023, the FDIC developed a Zero Trust Charter that assigns individual task owners to each Zero Trust Task. Responsibilities of the task owners included performing a gap analysis based on a three-level maturity model. In FY 2024, the FDIC continues to make progress towards meeting OMB M-22-09 direction, with six of the remaining thirteen tasks still outstanding. Refer to the bullets below for status of the remaining six tasks:

- Two tasks are scheduled to be completed by the end of FY 2024.
- Two tasks are scheduled to be completed within calendar year 2024.
- One task is scheduled to be completed in FY 2026.

[12] OMB, "Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements," M-22-05 (October 8, 2021), available at: https://www.whitehouse.gov/wp-content/uploads/2021/12/M-22-05-FY22-FISMA-Guidance.pdf.

- The last task does not currently have a planned completion date.

Because the requirements for OMB M-22-09 are not enforced until September 2024, KPMG determined that at the conclusion of fieldwork, FDIC remains in compliance with OMB M-22-09.

Event Logging

On August 27, 2021, OMB released Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents.*[13] The Memo highlighted system logs as a critical resource to detect, investigate, and remediate cyber threats. OMB also established standards for logged events, log retention, and log management, with a focus on ensuring centralized access and visibility for the enterprise security operations center (SOC) for each agency. See Table 2 for a summary of event logging (EL) and timeline requirements of agency implementation:

Table 2: Summary of Event Logging

Event Logging Tiers	Rating	Description	Timeline
EL0	Not Effective	Logging requirements of highest criticality are either not met or are only partially met.	N/A
EL1	Basic	Only logging requirements of highest criticality are met.	Within one year of the date of M-21-31's issuance (August 27, 2022), reach EL1 maturity.
EL2	Intermediate	Logging requirements of highest and intermediate criticality are met.	Within eighteen months of the date of M-21-31's issuance (February 27, 2023), achieve EL2 maturity.
EL3	Advanced	Logging requirements at all criticality levels are met.	Within two years of the date of M-21-31's issuance (August 27, 2023), achieve EL3 maturity.

Source: OMB-21-31 *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*

As of July 10, 2024, the FDIC reached level EL1, as it was able to demonstrate that it could log the required events as well as collect, maintain, and protect event logs. However, FDIC system owners and security personnel were continuing their efforts to meet logging requirements for all logs necessary to reach EL2 and EL3 because the FDIC was awaiting relevant CISA guidance to document the schema of their logs. Since the FDIC has achieved the logging requirements at EL1, established a project plan to meet EL2 and EL3, and awaits CISA guidance, KPMG did not issue a recommendation with respect to FDIC's progress satisfying M-21-31 requirements.

[13] OMB, "*Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*," M-21-31, available at: https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf.

Internet of Things (IoT) Inventory

OMB Memorandum M-24-04 identified “Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements Section II: Internet of Things” as instructions for agencies to have a clear understanding of the devices connected within the information systems. OMB Memorandum M-24-04 directs agencies to inventory their Internet of Things (IoT) devices by the end of FY 2024.

In FY 2024, the FDIC has made progress towards meeting the intent of OMB M 24-04. Specifically, the FDIC has completed creation of an inventory structure and continues to refine the attributes and elements contained within the inventory. KPMG noted the FDIC is also establishing a process to consistently maintain the inventory. KPMG determined that at the conclusion of fieldwork, the FDIC is on track to comply with M-24-04 Section II requirements; however, as the requirements must be implemented by September 30, 2024, the FDIC is at risk of no longer being compliant if the completed inventory becomes delayed or is completed after September 30. Without a fully completed inventory, the FDIC would be unable to effectively track IoT device vulnerabilities and software weaknesses, to include End-of-Life software, across the agency. This could increase the risk of security breaches within the IoT devices.

SUMMARY OF RESULTS

Based on the results of our evaluation, KPMG determined that the FDIC’s information security program is operating at a Maturity Level 4 (*Managed and Measurable*). KPMG used the results of our assessment of the metrics along with other quantitative and qualitative factors and other data points to make a risk-based determination of the assessed maturity levels for each domain, function areas, and the overall program. A security program is considered effective if the calculated average of the FY 2024 Core and Supplemental IG FISMA Metrics are at least at a Maturity Level 4 (*Managed and Measurable)*. Achieving Level 4 does not mean that the FDIC is without risk of cyberattacks or incidents, including the unauthorized access, use, disclosure, disruption, modification, or destruction of information or systems. As described in our evaluation results, there are deficiencies that remain at the FDIC. Tables 3 and 4 provide a breakdown of the maturity level ratings for the Core and Supplemental metrics, respectively, which led us to conclude upon the rating of the FDIC’s overall information security program.

In FY 2024, the DHS FISMA Reporting Metrics used a calculated average rating methodology, wherein the numerical average of the Core and Supplemental metrics in each Domain and Function establishes the foundation of the overall information security program rating level. IGs are encouraged to consider the results of this calculation among multiple data points when determining an overall rating and effectiveness of an organization’s security program. Because of this average rating methodology, it is possible for a Domain or Function to be considered Level 4 while still containing unimplemented or newly identified recommendations.

The Maturity Level score of 4 should not be compared to prior or future years. Under the two-year FISMA reporting cycle, the scope of the Metrics varies year-over-year. These changes, together with anticipated differences in the scope of evaluation work performed in subsequent years, make it inadvisable to compare this year’s maturity level ratings to ratings in both prior and future years.

Table 3: Core Metric Ratings by Function Area and the Overall Information Security Program

Function Area	Domain	Function Area Rating	Overall Rating
Identify	Risk Management	4.33	3.97
	Supply Chain Risk Management		
Protect	Configuration Management	3.50	
	Identity and Access Management		
	Data Protection and Privacy		
	Security Training		
Detect	ISCM	4.00	
Respond	Incident Response	3.50	
Recover	Contingency Planning	4.50	

Source: KPMG's assessment of the FDIC's information security program controls and practices based on the DHS FISMA Reporting Metrics.

Table 4: Supplemental Metric Ratings by Function Area and the Overall Information Security Program

Function Area	Domain	Function Area Rating	Overall Rating
Identify	Risk Management	3.67	3.86
	Supply Chain Risk Management		
Protect	Configuration Management	3.63	
	Identity and Access Management		
	Data Protection and Privacy		
	Security Training		
Detect	ISCM	4.00	
Respond	Incident Response	4.00	
Recover	Contingency Planning	4.00	

Source: KPMG's assessment of the FDIC's information security program controls and practices based on the DHS FISMA Reporting Metrics.

Based on the overall ratings of the core metrics (3.97) and supplemental metrics (3.86), KPMG determined that the FDIC information security program is operating at a Level 4 maturity. A Level 4 maturity is typically categorized as having quantitative and qualitative measures of the effectiveness of policies, procedures, and strategies collected across the organization and then used to assess and make necessary changes.[14]

Specifically, KPMG found that the FDIC established several information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. KPMG noted that the following five

[14] Stated from the FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics https://www.cisa.gov/sites/default/files/2023-02/Final%20FY%202023%20-%202024%20IG%20FISMA%20Reporting%20Metrics%20v1.1_0.pdf.

Domains were identified with no open recommendations reported during the FY 2024 FISMA evaluation and reached an effective, Level 4 maturity rating:

- Risk Management
- Data Protection and Privacy
- Information Security Continuous Monitoring
- Incident Response
- Contingency Planning

In response to the recommendations that remained open as of the report in September 2023, the FDIC also took action to strengthen related security controls. For example, the FDIC:

- Completed corrective actions related to addressing the technical issues preventing enforcement of security and privacy training compliance.
- Finalized the development of its processes and procedures related to SCRM.

However, our report describes security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices. The FDIC can reduce the effect of these weaknesses by improving the confidentiality, integrity, and availability[15] of its information systems and data. In many cases, these security control weaknesses were identified during IG audits and evaluations, or through security and privacy control assessments completed by the FDIC. These unaddressed audit and evaluation findings represent security control weaknesses that continue to pose risk to the FDIC. The security control weaknesses identified include:

- The FDIC Needs to Enforce Plan of Actions and Milestones (POA&Ms) Documentation Requirements to Track Vulnerabilities Identified
- The FDIC Needs to Enforce Role-Based Training Requirements
- The FDIC Did Not Fully Implement Audit Logging Requirements on Assessed Information Systems
- The FDIC Did Not Review Audit Logs at Sufficient Frequency within Cloud Information Systems
- The FDIC Did Not Remediate Overdue POA&Ms Related to SI-2 (Flaw Remediation)

Additionally, the following four Domains were identified as either ineffective or determined to contain open recommendations as noted below during fieldwork:

- Supply Chain Risk Management
- Configuration Management
- Identity Access and Management
- Security Training

In addition, **Appendix II** notes two outstanding recommendations from prior FISMA reports warranting the FDIC's continued attention.

[15] NIST SP 800-12 (Rev.1), *An Introduction to Information Security* defines information security as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability. The effectiveness of these three elements – confidentiality, integrity, and availability – determines the effectiveness of an organization's information security.

EVALUATION RESULTS

This section of the report describes the key controls underlying each Domain and our assessment of the FDIC's implementation of those controls by Function Area and Domain.

IDENTIFY

The *Identify* Function area includes the evaluation of the agency's Risk Management Program and Supply Chain Risk Management.

Risk Management

The *Risk Management* Domain includes controls that address an agency's maturity in the management of cybersecurity risks. These activities include maintaining an inventory of systems, hardware, software, and software licenses; managing risk at the organizational, mission/business process, and information system levels; Enterprise and Information System Architectures and System Categorizations; and utilizing technology to provide a centralized view of cybersecurity risk management activities. As noted above, KPMG assessed the Risk Management Domain as Level 4, Managed and Measurable (Effective).

Supply Chain Risk Management

The *Supply Chain Risk Management* Domain includes controls that address an agency's maturity in a range of activities related to the supply chain management of cybersecurity risks. These activities include implementing and maintaining organization-wide SCRM policies and procedures, as well as processes for managing SCRM Counterfeit Components. Based on the results of our test procedures, KPMG assessed the SCRM Domain as Level 3, Consistently Implemented (Not Effective). In order to reach an effective maturity rating, the FDIC should develop and implement quantitative and qualitative performance measures of their SCRM strategy across the organization to gauge the effectiveness of their strategy and identify areas of improvement.

In the FISMA report for 2021, a recommendation was issued to develop and implement processes and procedures required by FDIC Directive 3720.01, *Supply Chain Risk Management Program,* published in June 2021. During FY 2024, the FDIC has finalized the development of its processes and procedures to address the SCRM finding from the FISMA report for 2021.

In March 2022, the OIG completed an evaluation on the FDIC's implementation of SCRM[16] and found that the FDIC did not implement several of its defined SCRM objectives, identify, or document its SCRM risks, or establish metrics and indicators for SCRM. The OIG issued nine recommendations that directed the FDIC to identify, document, and monitor supply chain risks and conduct supply chain risk assessments. Four of these recommendations were closed prior to the last FISMA report issuance in September 2023, and the following five remaining open recommendations were closed during this evaluation period:

[16] FDIC OIG Report, *The FDIC's Implementation of Supply Chain Risk Management*, March 2022 https://www.fdicoig.gov/reports-publications/audits-and-evaluations/fdics-implementation-supply-chain-risk-management.

- Develop metrics and indicators for gauging and monitoring supply chain risk;
- Implement SCRM controls during the IT procurement process;
- Define a risk-based process for considering supply chain risks in procurement actions;
- Apply a risk-based process for considering supply chain risks when entering into new contracts; and
- Apply a risk-based process for considering supply chain risks when contracts are renewed, extended, or have option periods exercised.

In addition to the above corrective actions the FDIC has also developed and implemented component authenticity/anti-counterfeit training for designated personnel. Visibility into supply chain activities is important for monitoring and identifying high-risk threats and events associated with using external vendors. The FDIC has made substantial changes throughout FY 2024 to address risks and recommendations related to supply chain management, noted above. However, the FDIC should continue to improve its SCRM strategy, to include developing and implementing qualitative and quantitative measures within its SCRM strategy, to reach an Effective rating.

PROTECT

The *Protect* Function area includes the evaluation of the agency's Configuration Management Program, Identity and Access Management, Data Protection and Privacy, and Security Training Programs.

Configuration Management

The *Configuration Management* (CM) Domain includes controls that address an agency's maturity in ensuring the integrity, security, and reliability of any information system by requiring disciplined processes for managing the changes that occur to the system during its life cycle. Such changes include the development of an enterprise-wide configuration management plan; establishing CM roles and responsibilities; installing software patches to address security vulnerabilities; applying software updates, to include application changes, to improve system performance and functionality; and modifying configuration settings to strengthen security. Based on the results of our test procedures, KPMG assessed the CM Domain as Level 4, Managed and Measurable (Effective).

In the FISMA report for FY 2022, a recommendation was issued to address the 31 POA&Ms associated with NIST SP 800-53 Rev. 5 control SI-2 (Flaw Remediation). As of July 31, 2024, the recommendation remains unimplemented. As the FDIC was actively working milestone remediation for the associated 31 POA&Ms, KPMG did not note an impact to the Domain as the agency had an established plan to remediate the remaining open POA&Ms.

Further, during FY 2024, the FDIC's flaw remediation process still needed improvement based on issues identified in its implementation of CM security controls, as noted below.

Failure to Effectively Implement Flaw Remediation Tracking Within POA&Ms

A POA&M is a document that outlines the steps and timeline for addressing and mitigating identified security vulnerabilities and weaknesses within an organization's systems and networks. It serves as a roadmap for implementing necessary controls and measures to improve the overall security posture. The FDIC has implemented a POA&M Management and Acceptance of Risk Process in order to meet these objectives of the POA&M process. Maintaining up-to-date and accurate POA&M information is crucial for effective cybersecurity management. It helps management identify and prioritize security vulnerabilities, track progress in addressing them, and ensure timely remediation to protect critical assets and data.

KPMG noted the FDIC did not effectively implement the process to document POA&Ms, specifically related to control SI-2, Flaw Remediation, in accordance with the FDIC OCISO's, POA&M Management and Acceptance of Risk Process. KPMG identified five open POA&Ms related to control SI-2 within one of the selected systems during testing. Of those five:

- All five had milestones that did not contain sufficient detail to effectively track and remediate vulnerabilities;
- Two were identified as a risk level of "High" with a scheduled completion date of more than 30 days after creation; and
- Two were identified as "Medium" risk with exploitable vulnerabilities identified through Tenable scanning with a scheduled completion date of more than 30 days after POA&M creation.

KPMG noted that management is currently using scanning tools in conjunction with POA&Ms to track vulnerabilities. Because of this, overdue vulnerabilities identified through automated scans are not clearly tracked within POA&Ms. Without clearly defined thresholds for tracking vulnerabilities within POA&Ms, executive management may be unaware of the accurate status of overdue vulnerabilities through the required POA&M Management and Acceptance of Risk Process, which outlines the procedural requirements for documenting POA&Ms. As such, Authorizing Officials may be unaware of relevant risks within information systems. This can lead to systems being authorized to operate outside of the FDIC's risk tolerance.

Additionally, the FDIC updated its POA&M Management and Acceptance of Risk Process document as of July 10, 2024. The updated document does not clearly define the threshold for when a POA&M is required to be documented related to vulnerabilities identified via automated scanning. Additionally, remediation timeframes for vulnerabilities identified via scanning mechanisms are not clearly defined. This update directly conflicts with requirements cited within NIST 800-53 Rev 5, control CA-05.[17]

Without clearly defined milestones, miscommunication and delays may occur within the remediation process. This can lead to inefficient resource allocation, compliance gaps, and increased security risks. Additionally, failure to adhere to required deadlines when remediating vulnerabilities can prolong exposure to security risks. This can result in unauthorized access, data breaches, system disruptions, or other security incidents. As the tested system has externally facing components, it is critical that vulnerabilities within this environment are

[17] NIST Special Publication 800-53 Revision 5, Control CA-5 requires agencies to: "Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system." These POA&Ms are used to: "[…] track planned remedial actions. Plans of action and milestones are required in authorization packages and subject to federal reporting requirements established by OMB." https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

accurately tracked and remediated timely to minimize the impact of the potential exploitation of known vulnerabilities as outlined in Binding Operational Directive (BOD) 19-02.[18]

KPMG recommends the CIO:

1. Update and implement the POA&M Management and Acceptance of Risk Process document to clearly define requirements of when vulnerabilities must be documented within a POA&M, and what the remediation timeline for POA&Ms must be.

Identity and Access Management

The *Identity and Access Management* (IAM) Domain includes controls that address an agency's maturity in implementing a set of capabilities to help ensure that only authorized users, processes, and devices have access to the organization's IT resources and facilities, and that their access is limited to the minimum necessary to perform their jobs. These capabilities involve the implementation of strong authentication mechanisms for privileged and non-privileged users (e.g., multi-factor), assigning and maintaining personnel risk designations, and effectively managing privileged users. Based on the results of our test procedures, KPMG assessed the Identity and Access Management Domain as Level 4, Managed and Measurable (Effective).

In the FY 2023 FISMA report, a recommendation was issued to address weaknesses within the user separation process, specifically with ensuring prompt notification and removal of user network accounts on or before the user's separation date. The FDIC had planned an estimated completion date of June 27, 2025; as of July 10, 2024, the recommendation remains open.

In FY 2024, in the OIG published report on *Audit of Security Controls for the FDIC's Cloud Computing Environment* in September 2024, it was noted that audit logs are not reviewed at sufficient frequency to timely detect and respond to suspicious events. As such, a recommendation was issued to update the audit log review frequency (b) (7)(E) to support the ability to detect and respond to suspicious activity shortly after the activity has occurred.

Additionally, during FY 2024, the FDIC's management of privileged user accounts still needed improvement based on issues identified in its implementation of IAM security controls, as noted below.

The FDIC Did Not Fully Implement Privileged User Audit Logging Requirements on Assessed Information Systems

Audit logging involves the systematic recording of events and activities within a computer system or network to ensure accountability, traceability, and security. It captures information such as user actions, system changes, and access attempts, providing a detailed record that can be used for monitoring, analysis, and investigation purposes. Failure to perform consistent

[18] BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*, requires agencies to remediate critical and high vulnerabilities on Internet-accessible systems within 15 and 30 days, respectively. It also requires specific actions to be taken to ensure these vulnerabilities are appropriately tracked within CISA. https://www.cisa.gov/news-events/directives/bod-19-02-vulnerability-remediation-requirements-internet-accessible-systems.

review and analysis of audit record logs, specifically over privileged accounts and actions, may lead to anomalous activities that are not investigated and increase the risk that unauthorized or inappropriate activities occurred. As privileged users have the ability to perform functions such as system configuration and management, data manipulation, and security administration, it is crucial that the FDIC implement proper monitoring mechanisms to help ensure that privileged accounts are used responsibly and in accordance with security policies and procedures.

KPMG noted the FDIC has enterprise audit logging capabilities. However, weaknesses specific to the (b) (7)(E) existed related to the audit logging process for privileged actions and accounts, the remediation of which is key to FDIC's goal to strengthen the security of the FDIC's information resources. KPMG tested audit logging and review of privileged actions and accounts on two information systems selected for testing at the FDIC. KPMG noted that management did not consistently perform and document a periodic review of audit logs within one of the two tested systems.

KPMG noted a lack of dissemination of the FDIC logging requirements; as a result, system management did not document and maintain evidence of review/follow-up actions of anomalous audit log activity. KPMG noted that some of the devices within the system boundary implemented audit logging requirements prior to the end of fieldwork.

KPMG recommends the CIO:

2. Enforce existing policies and procedures to consistently perform reviews and analyze system audit records, and document and maintain those reviews and analysis for privileged users and actions taken on (b) (7)(E) devices in accordance with FDIC policy.

Data Protection and Privacy

The *Data Protection and Privacy* Domain includes controls that address an agency's maturity in implementing a privacy program to properly collect, use, maintain, protect, share, and dispose of PII. Organizations must consider the protection of PII throughout its lifecycle (from initial, creation or acquisition through disposal), including the confidentiality, integrity, and availability of PII, using controls such as encryption, data loss prevention, labeling, and minimizing PII holdings. As noted above, KPMG assessed the Data Protection and Privacy Domain as Level 4, Managed and Measurable (Effective).

Security Training

The *Security Training* Domain includes controls that address an agency's maturity in providing appropriate security awareness training to its personnel, contractors, and other system users. Based on the results of our test procedures, KPMG assessed the Security Training Domain as Level 3, Consistently Implemented (Not Effective).

During our assessment of the IG Metrics during FY 2024, KPMG determined that the FDIC had not completed a workforce assessment as of July 10, 2024. A Workforce Planning Guide has been developed that documents the need to perform periodic workforce assessments. Doing so would allow CIOO senior management to determine personnel competencies and skill gaps within a continuously changing IT environment, and address the gaps as needed. The FDIC was actively performing such an assessment, with a planned completion date of September 30,

2024. As the FDIC was actively working toward conducting the assessment by a planned completion date, KPMG did not issue a recommendation. To help ensure effectiveness within this metric, the FDIC should continue to work towards completion of the workforce assessment, as well as addressing any gaps identified from the assessment.

The FDIC also completed corrective actions for a recommendation issued in the FISMA report for 2023 related to addressing the technical issues preventing enforcement of security and privacy training compliance. This recommendation was closed by the OIG after the FY 2023 FISMA report was issued.

However, the FDIC's security training program continues to need additional improvement, as noted below.

The FDIC Needs to Enforce Role-Based Training Requirements

A robust and enterprise-wide role-based training program is paramount to ensuring that privileged users understand their security responsibilities, organizational policies, and how to properly use and protect the information and systems entrusted to them. The FDIC relies on information systems to support its mission and thus provides system access to FDIC employees and contractors ("users") accordingly to perform their job functions.

FDIC management did not effectively implement the security training requirements for the organization in accordance with the FDIC Cybersecurity & Privacy Awareness Training (CPAT) Plan. Specifically, 7 out of 25 FDIC users, with elevated access rights and permissions selected for testing, were late to take their annual GSS Rules of Behavior Training by the required suspense date.

KPMG noted a technical issue within the training tool where privileged users were not properly tracked for annual completion of the GSS Rules of Behavior Training. Within the training tool, users were able to select the GSS Rules of Behavior training course instead of the Rules of Behavior training path. If a user did not select the training path, the system did not appropriately flag that user to take the training on an annual basis. Privileged users have access to sensitive systems and data, and without proper training, they may not be aware of the latest security threats, best practices, and protocols. This can lead to negatively impacting the ability to protect personal information and sensitive data impacting the overall stability, security, and reliability of the system that the privileged users maintain.

KPMG recommends the CIO:

3. Remediate the technical issues within the FDIC's Learning Management System that allow users to select the GSS Rules of Behavior training course in place of the required GSS Rules of Behavior training path to ensure users complete annual Rules of Behavior training.

DETECT

The *Detect* Function area includes the evaluation of the agency's Information Security Continuous Monitoring Program.

Information Security Continuous Monitoring

The *Information Security Continuous Monitoring* Domain includes controls that address an agency's maturity in implementing an ISCM strategy and governance structure, ISCM policies and processes, granting system authorizations, performing system assessments, and monitoring systems on an ongoing basis. As noted above, KPMG assessed the ISCM Domain as Level 4, Managed and Measurable (Effective).

RESPOND

The *Respond* Function area includes the evaluation of the agency's Incident Response Program.

Incident Response

The *Incident Response* Domain includes controls that address an agency's maturity in implementing technologies for detecting, analyzing, and handling security incidents. As noted above, KPMG assessed the Incident Response Domain as Level 4, Managed and Measurable (Effective).

OMB M-21-31 directs agencies to improve their event logging and log management capabilities along three maturity levels (EL1, EL2, and EL3). As of July 10, 2024, the FDIC demonstrated EL1 maturity. Although the FDIC did not achieve EL2 maturity by February 27, 2024 as required by M-21-31, KPMG acknowledges that this delay was partially due to a dependency on the release of CISA guidance, which is estimated to be released by early FY 2025. Without CISA guidance, the FDIC cannot fully comply with EL2 requirements. Therefore, KPMG is not issuing a recommendation addressing this issue. The FDIC has established a project plan to meet EL2 and EL3 maturity, to include establishing the means to help ensure that all required system logs are retained in acceptable formats for specified timeframes.

RECOVER

The *Recover* Function area includes the evaluation of the agency's Contingency Planning Program.

Contingency Planning

The *Contingency Planning* Domain includes controls that address an agency's maturity in implementing a governance structure over system contingency planning activities, performing business impact analyses, maintaining system contingency plans, testing those contingency plans through simulated exercises, and conducting information system backups. As noted above, KPMG assessed the Contingency Planning Domain as Level 4, Managed and Measurable (Effective).

CONCLUSION

In response to the objective identified within **Appendix I**, KPMG determined that the FDIC generally established controls and practices consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. Our report contains three new recommendations and cites two unimplemented recommendations from FISMA reports in prior years, as noted in **Appendix II**. These recommendations and initiatives aim to strengthen the effectiveness of the FDIC's information security program controls and practices.

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY

KPMG conducted this evaluation, with FDIC OIG oversight, in accordance with Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation (Blue Book). These standards require that KPMG plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objective. KPMG believes that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objective.

Tests of internal controls must be sufficiently extensive to provide reasonable assurance that the controls being tested operate effectively throughout the period under evaluation. The scope of our assessment of internal controls was limited to the OMB Office of the Federal Chief Information Officer *FY 2023-2024 IG FISMA Reporting Metrics*, which KPMG used to assess the effectiveness of the FDIC's information security program and practices. Accordingly, our work may not have identified all internal control deficiencies in the FDIC's information security program and practices that existed at the time of our evaluation.

To accomplish our objective, KPMG:

- Evaluated key components of the FDIC's information security program plans, policies, procedures, and practices that were in place as of July 10, 2024 (or as otherwise noted in our report) for consistency with FISMA, NIST security standards and guidelines, and OMB policies and guidance. KPMG considered guidance contained in OMB's Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements* (December 2023), when planning and conducting our work. KPMG also consulted the FY 2024 FISMA Metrics Evaluator's Guide to verify the reasonableness of our procedures.
- Assessed the maturity of the FDIC's information security program with respect to the metrics defined in the DHS FISMA Reporting Metrics. As discussed above, the DHS FISMA Reporting Metrics provide a framework for assessing the effectiveness of agency information security programs.
- Considered the results of recent and ongoing audit and evaluation work, conducted by the FDIC OIG and the Government Accountability Office (GAO), relating to the FDIC's information security program controls and practices.
- Selected and evaluated security controls related to a non-statistical sample of two FDIC-maintained information systems, (b) (7)(E) and (b) (7)(E. Our analysis of these systems included reviewing selected system documentation and other relevant information, as well as testing selected security controls. KPMG selected these systems because they support mission-essential functions.[19] A disruption of their operation could impair the FDIC's business transactions and services necessary for operations, ultimately hindering the FDIC's ability to achieve its mission.

KPMG conducted the evaluation remotely at its off-site locations across the United States from September 2023 through July 2024.

[19] According to FDIC Directive 1360.13, *IT Continuity Implementation Program*, a Mission Essential Function (MEF) is directly related to accomplishing an organization's mission as set forth in its statutory or executive charter. Any IT application, system, or service that supports a MEF is deemed "mission essential" and is designated a recovery time of 0-12 hours.

APPENDIX II – STATUS OF PRIOR-YEAR FISMA RECOMMENDATIONS

The following table summarizes the OIG's determinations regarding the status of previously unimplemented recommendations from FISMA reports issued in 2021, 2022, and 2023. Recommendations marked 'Closed' denote status updates that followed the publication of the FISMA report in 2023.

Recommendation	Status
Report Issued in 2021, Recommendation 1 Develop and implement SCRM processes and procedures in accordance with the Supply Chain Risk Management Program Directive and applicable government guidance.	Closed
Report Issued in 2022, Recommendation 1 Address the 31 POA&Ms identified as of June 21, 2022, associated with NIST SP 800-53 Rev. 5 control SI-2 (Flaw Remediation).	Unimplemented
Report Issued in 2023, Recommendation 1 Implement process improvements to ensure prompt notification and removal of user network accounts on or before the user's separation date.	Unimplemented
Report Issued in 2023, Recommendation 2 Address the technical issues preventing enforcement of security and privacy training compliance.	Closed

Appendix III – List of Acronyms

Acronym	Description
(b) (7)(E) [redacted]	(b) (7)(E) [redacted]
AAR	After Action Report
AICPA	American Institute of Certified Public Accountants
ATO	Authorization to Operate
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIOO	Chief Information Officer Organization
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CPAT	Cybersecurity and Privacy Awareness Training
CSIRT	Computer Security Incident Response Team
(b) (7)(E) [redacted]	(b) (7)(E) [redacted]
DHS	Department of Homeland Security
DLP	Data Loss Prevention
EDR	Endpoint Detection and Response
EL	Event Logging
EO	Executive Order
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
GSS	General Support System
IG	Inspector General
IoT	Internet of Things
ISCM	Information Security Continuous Monitoring
ITRAC	IT Risk Advisory Council
KPMG	KPMG, LLP
MEF	Mission Essential Function
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SCRM	Supply Chain Risk Management
SIEM	Security Incident and Event Management
SOC	Security Operations Center

SOP	Standard Operating Procedure
SP	Special Publication
SRT	Security Response Team

Part II

****

FDIC Comments and OIG Evaluation

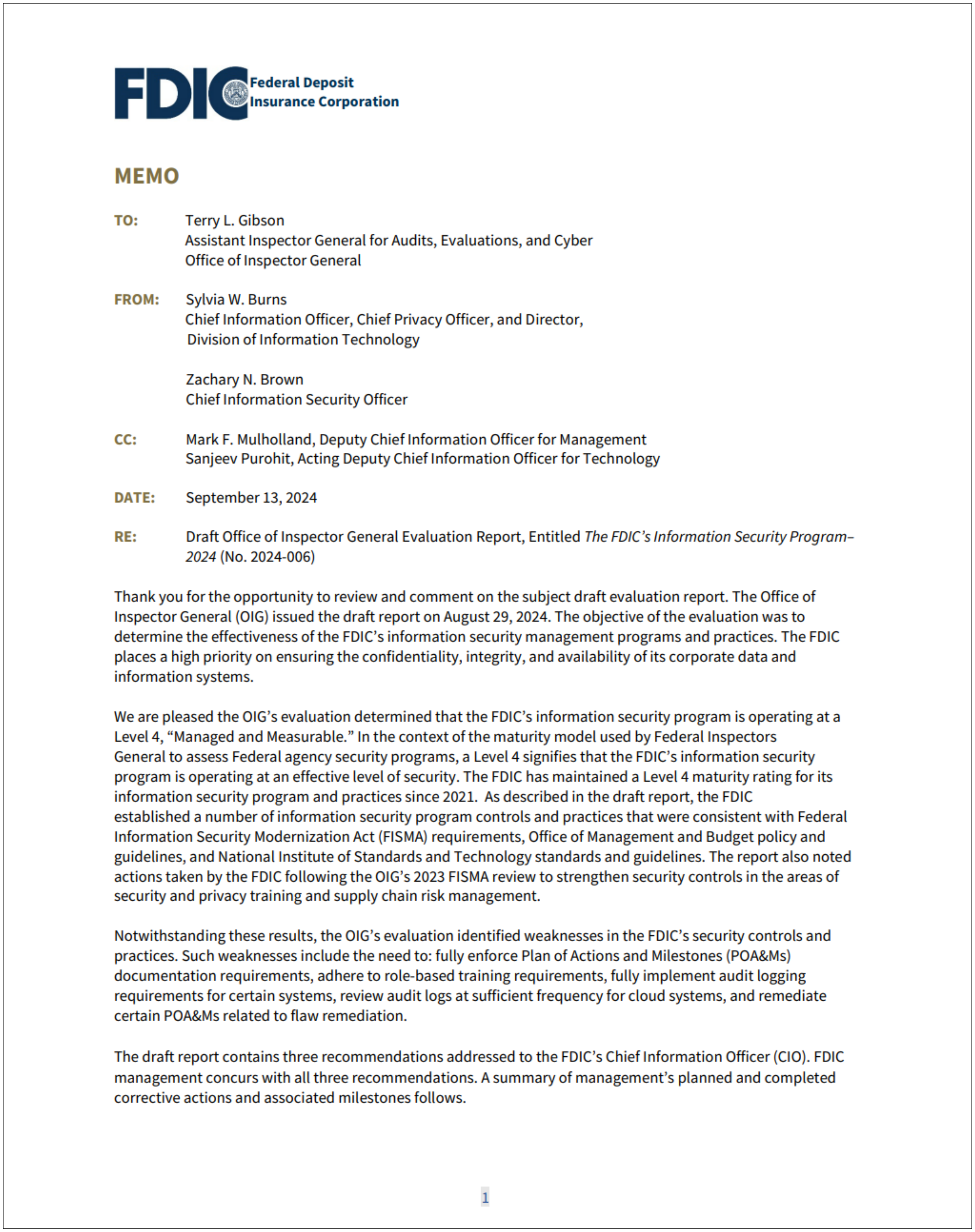
FDIC COMMENTS AND OIG EVALUATION

On September 13, 2024, the Chief Information Officer, Chief Privacy Officer, and Director, Division of Information Technology provided a written response to a draft of this report, which is presented in its entirety on page II-2.

In its response, the FDIC concurred with the three new recommendations, corrective actions were sufficient to address the intent of the recommendations, and we consider these recommendations to be resolved.

The recommendations in this report will remain open until we confirm that corrective actions have been completed and the actions are responsive. A summary of the FDIC's corrective actions is contained on page II-5.

APPENDIX 1: FDIC COMMENTS



FDIC Federal Deposit Insurance Corporation

MEMO

TO: Terry L. Gibson
Assistant Inspector General for Audits, Evaluations, and Cyber
Office of Inspector General

FROM: Sylvia W. Burns
Chief Information Officer, Chief Privacy Officer, and Director,
Division of Information Technology

Zachary N. Brown
Chief Information Security Officer

CC: Mark F. Mulholland, Deputy Chief Information Officer for Management
Sanjeev Purohit, Acting Deputy Chief Information Officer for Technology

DATE: September 13, 2024

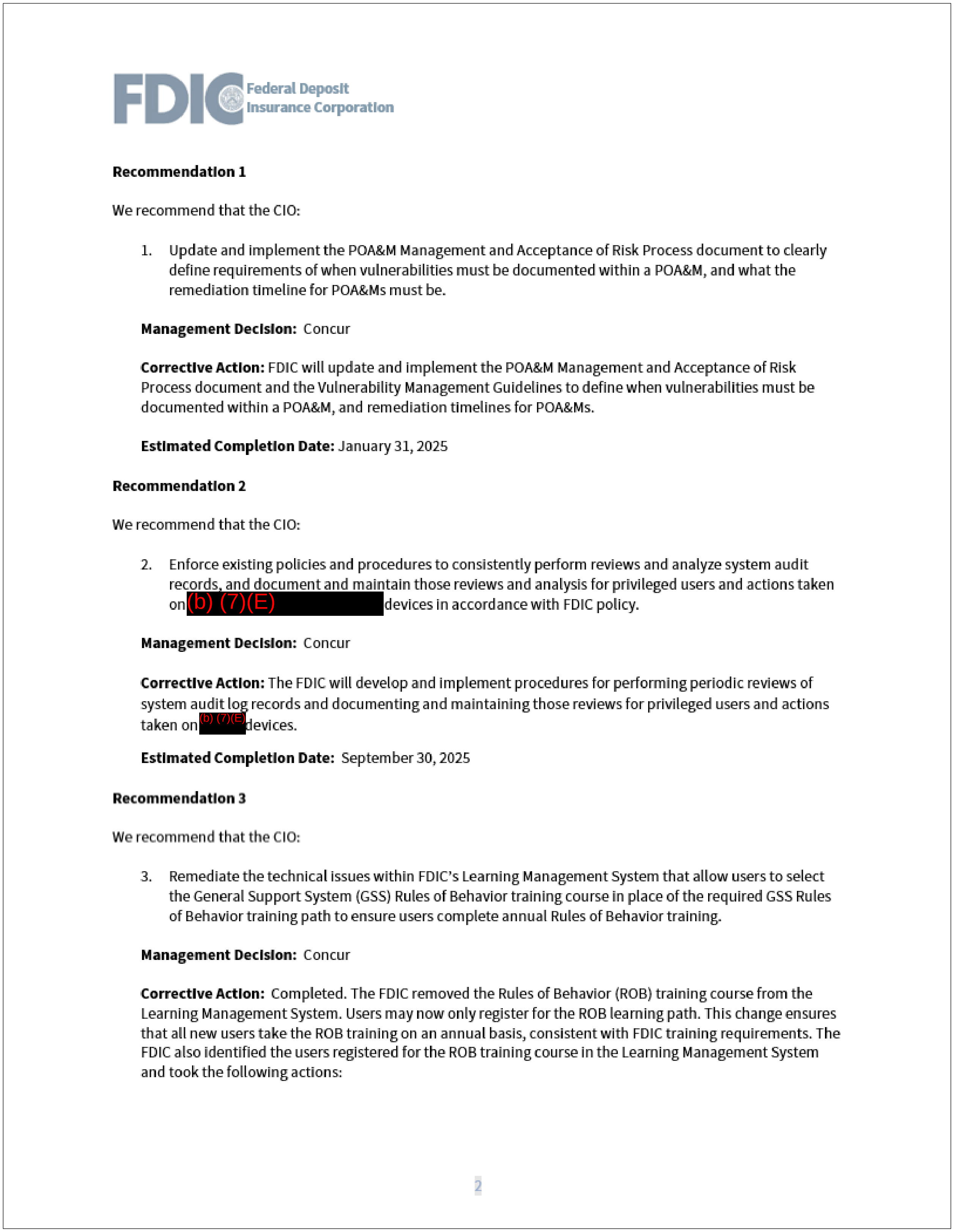
RE: Draft Office of Inspector General Evaluation Report, Entitled *The FDIC's Information Security Program–2024* (No. 2024-006)

Thank you for the opportunity to review and comment on the subject draft evaluation report. The Office of Inspector General (OIG) issued the draft report on August 29, 2024. The objective of the evaluation was to determine the effectiveness of the FDIC's information security management programs and practices. The FDIC places a high priority on ensuring the confidentiality, integrity, and availability of its corporate data and information systems.

We are pleased the OIG's evaluation determined that the FDIC's information security program is operating at a Level 4, "Managed and Measurable." In the context of the maturity model used by Federal Inspectors General to assess Federal agency security programs, a Level 4 signifies that the FDIC's information security program is operating at an effective level of security. The FDIC has maintained a Level 4 maturity rating for its information security program and practices since 2021. As described in the draft report, the FDIC established a number of information security program controls and practices that were consistent with Federal Information Security Modernization Act (FISMA) requirements, Office of Management and Budget policy and guidelines, and National Institute of Standards and Technology standards and guidelines. The report also noted actions taken by the FDIC following the OIG's 2023 FISMA review to strengthen security controls in the areas of security and privacy training and supply chain risk management.

Notwithstanding these results, the OIG's evaluation identified weaknesses in the FDIC's security controls and practices. Such weaknesses include the need to: fully enforce Plan of Actions and Milestones (POA&Ms) documentation requirements, adhere to role-based training requirements, fully implement audit logging requirements for certain systems, review audit logs at sufficient frequency for cloud systems, and remediate certain POA&Ms related to flaw remediation.

The draft report contains three recommendations addressed to the FDIC's Chief Information Officer (CIO). FDIC management concurs with all three recommendations. A summary of management's planned and completed corrective actions and associated milestones follows.



FDIC Federal Deposit Insurance Corporation

Recommendation 1

We recommend that the CIO:

1. Update and implement the POA&M Management and Acceptance of Risk Process document to clearly define requirements of when vulnerabilities must be documented within a POA&M, and what the remediation timeline for POA&Ms must be.

Management Decision: Concur

Corrective Action: FDIC will update and implement the POA&M Management and Acceptance of Risk Process document and the Vulnerability Management Guidelines to define when vulnerabilities must be documented within a POA&M, and remediation timelines for POA&Ms.

Estimated Completion Date: January 31, 2025

Recommendation 2

We recommend that the CIO:

2. Enforce existing policies and procedures to consistently perform reviews and analyze system audit records, and document and maintain those reviews and analysis for privileged users and actions taken on (b) (7)(E) devices in accordance with FDIC policy.

Management Decision: Concur

Corrective Action: The FDIC will develop and implement procedures for performing periodic reviews of system audit log records and documenting and maintaining those reviews for privileged users and actions taken on (b) (7)(E) devices.

Estimated Completion Date: September 30, 2025

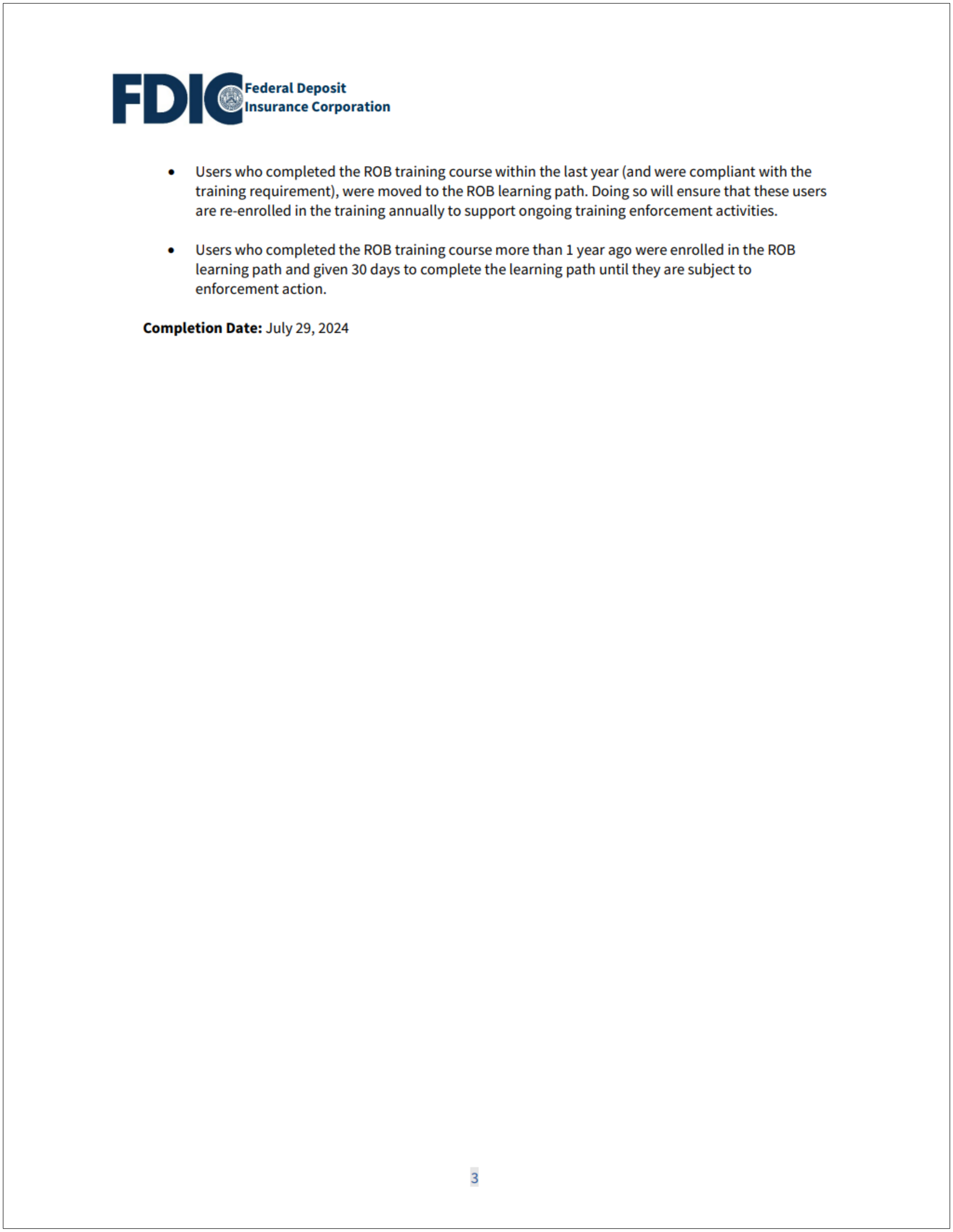
Recommendation 3

We recommend that the CIO:

3. Remediate the technical issues within FDIC's Learning Management System that allow users to select the General Support System (GSS) Rules of Behavior training course in place of the required GSS Rules of Behavior training path to ensure users complete annual Rules of Behavior training.

Management Decision: Concur

Corrective Action: Completed. The FDIC removed the Rules of Behavior (ROB) training course from the Learning Management System. Users may now only register for the ROB learning path. This change ensures that all new users take the ROB training on an annual basis, consistent with FDIC training requirements. The FDIC also identified the users registered for the ROB training course in the Learning Management System and took the following actions:



- Users who completed the ROB training course within the last year (and were compliant with the training requirement), were moved to the ROB learning path. Doing so will ensure that these users are re-enrolled in the training annually to support ongoing training enforcement activities.

- Users who completed the ROB training course more than 1 year ago were enrolled in the ROB learning path and given 30 days to complete the learning path until they are subject to enforcement action.

Completion Date: July 29, 2024

APPENDIX 2: SUMMARY OF THE FDIC'S CORRECTIVE ACTIONS

This table presents management's response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The FDIC will update and implement the POA&M Management and Acceptance of Risk Process document and the Vulnerability Management Guidelines to define when vulnerabilities must be documented within a POA&M, and remediation timelines for POA&Ms.	January 31, 2025	$0	Yes	Open
2	The FDIC will develop and implement procedures for performing periodic reviews of system audit log records and documenting and maintaining those reviews for privileged users and actions taken on (b) (7)(E) devices.	September 30, 2025	$0	Yes	Open
3	The FDIC removed the Rules of Behavior (ROB) training course from the Learning Management System. Users may now only register for the ROB learning path. This change ensures that all new users take the ROB training on an annual basis, consistent with FDIC training requirements. The FDIC also identified the users registered for the ROB training course and took action to ensure they are on the ROB learning path.	July 29, 2024	$0	Yes	Open

[a] Recommendations are resolved when —

1. Management concurs with the recommendation, and the OIG agrees the planned corrective action is consistent with the recommendation.

2. Management does not concur or partially concurs with the recommendation, but the OIG agrees that the proposed corrective action meets the intent of the recommendation.

3. For recommendations that include monetary benefits, management agrees to the full amount of OIG monetary benefits or provides an alternative amount and the OIG agrees with that amount.

[b] Recommendations will be closed when the OIG confirms that corrective actions have been completed and are responsive.

Federal Deposit Insurance Corporation
Office of Inspector General
3501 Fairfax Drive
Room VS-E-9068
Arlington, VA 22226
(703) 562-2035

☆ ☆ ☆ ☆ ☆ ☆

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding FDIC programs, employees, contractors, or contracts, please contact us via our Hotline or call 1-800-964-FDIC.

FDIC OIG website | www.fdicoig.gov
X, formerly known as Twitter | @FDIC OIG
Oversight.gov | www.oversight.gov