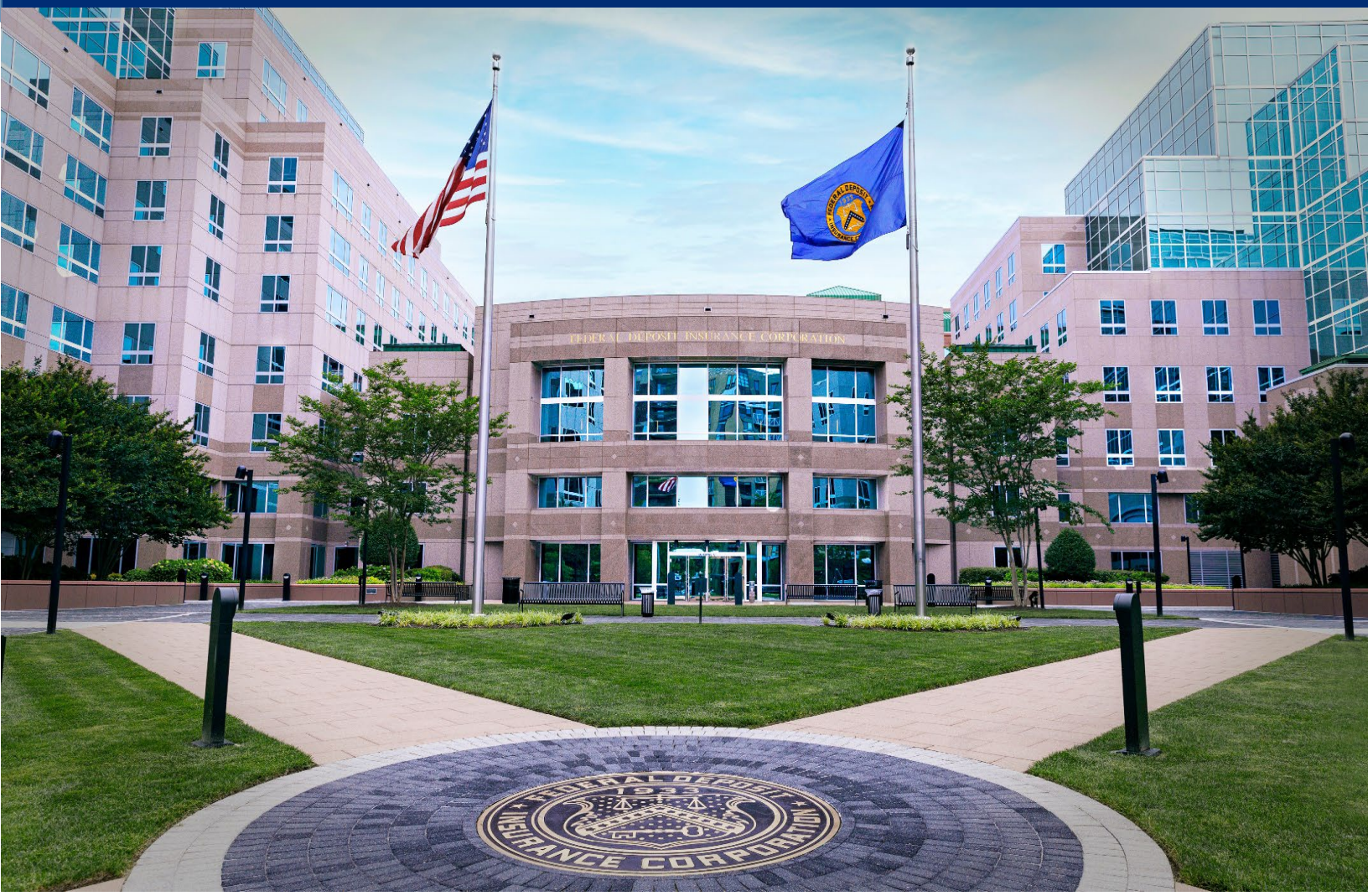
FDIC Office of Inspector General

The FDIC's Information Security Program – 2025

Office of Audits

September 2025 | **EVAL-25-03**



Office of Inspector General

REDACTED VERSION PUBLICLY AVAILABLE

The redactions in this report are based on legal provisions protecting sensitive information.

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.

Executive Summary

The FDIC's Information Security Program – 2025 (EVAL-25-03) **September 26, 2025**

What We Did

We contracted with KPMG LLP to assess the effectiveness of the FDIC's information security program and practices. To plan and perform the work and conclude on the objective, KPMG considered:

- FISMA requirements,
- NIST standards and guidelines,
- NIST Cybersecurity Framework,
- OMB policy and guidance,
- FDIC policies and procedures, and
- DHS Guidance and reporting requirements.

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 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 2025 FISMA Metrics. As shown in the table below, KPMG assigned an Effective Rating for all six FISMA functions for FY 2025.

2025 Core and Supplemental Scores by Function

Function	Weighted Average	Maturity Level	Effectiveness
Govern	3.57	4	Effective
Identify	4.40	4	Effective
Protect	3.63	4	Effective
Detect	4.00	4	Effective
Respond	3.50	4	Effective
Recover	5.00	5	Effective
Overall	**4.02**	**4**	**Effective**

KPMG found that the FDIC established several information security program controls and practices that were consistent with FISMA requirements. However, the report describes security control weaknesses that diminished the effectiveness of certain aspects of the FDIC's information security program and practices. Newly identified security control weaknesses include:

- The FDIC did not implement privileged access review frequency requirements for both of the systems we tested.
- The FDIC utilized an incomplete and inaccurate listing for user recertification for one of the systems we tested.

Recommendations

KPMG made four new recommendations related to weaknesses identified during this year's evaluation. In addition, there are two outstanding recommendations from prior FISMA reports still warranting the FDIC's continued attention. The FDIC concurred with all four recommendations and plans to complete corrective actions by May 29, 2026.

The FDIC's Information Security Program – 2025

Date: September 26, 2025

Memorandum To: Sylvia W. Burns
Chief Information Officer

From: (b) (6)
Matthew Simber
Acting Assistant Inspector General for Audits

Subject *The FDIC's Information Security Program – 2025* | EVAL-25-03

Enclosed is the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) report on *The FDIC's Information Security Program – 2025*.

The FDIC OIG contracted with KPMG LLP (KPMG) to conduct an evaluation of the FDIC's information security program. The contract required KPMG's work to be conducted in accordance with the *Quality Standards for Inspection and Evaluation* (Blue Book) 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 standards outlined in CIGIE's Blue Book.

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 (b) (6).

The FDIC's Information Security Program – 2025

Part I

Part II

Part I

****

Report by KPMG LLP

THE FEDERAL DEPOSIT INSURANCE CORPORATION'S INFORMATION SECURITY PROGRAM – 2025

EVALUATION REPORT

SEPTEMBER 18, 2025

KPMG LLP
1801 K Street NW
Washington DC 20006

TABLE OF CONTENTS

Matthew Simber
Acting Assistant Inspector General for Audits
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 – 2025

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). 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 2025 through July 2025, and our results are as of July 10, 2025.

We conducted this evaluation in accordance with the 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 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).[1] 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.

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

[1] 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.

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)[2] 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. This effort yielded two distinct groups of metrics: **Core and Supplemental**.[5] The goal of this new framework was to maintain a consistent focus on annual assessments while allowing for greater flexibility for the federal community.

The "Core" metrics are associated with high value controls, whereas the "Supplemental" metrics provide additional insights to support and enhance the understanding of 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. Specifically, OMB provided the following guidance:

---

[2] The FY 2025 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).
[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 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, issued April 3, 2025.

- 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]
- 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 require 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-25-04[9] provides agencies with FY 2025 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]

During FY 2025, OMB and CIGIE introduced a weighted average approach to the scoring methodology. The new scoring is designed to account for select metrics that have a greater importance or provide interdependent relationships to other metrics. This calculation was utilized for the scoring results presented below in Table 3. Additionally, the Govern function was added to the IG metrics to align the FISMA function areas to the six NIST Cybersecurity Framework 2.0 function areas. This function also includes a new domain, Cybersecurity Governance.

---

[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.
[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 2025 Guidance on Federal Information Security and Privacy Management Requirements*, M-25-04 (January 15, 2025), available at: M-25-04 (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.

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.

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 2.0 (CSF 2.0), OMB policy and guidance, FDIC policies and procedures, and DHS guidance and reporting requirements to plan and perform our work and to make a conclusion to satisfy our evaluation objective. KPMG performed testing on two FDIC-maintained systems that formed our non-statistical sample: (b) (7)(E) (b) (7)(E) **Appendix I** contains more information about our scope and methodology.

DHS FISMA REPORTING METRICS AND THE NIST CYBERSECURITY FRAMEWORK 2.0

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 2025 IG FISMA Reporting Metrics, which are aligned to the NIST CSF 2.0.[12] NIST CSF 2.0 is a set of guidelines and leading practices designed to help organizations manage and reduce cybersecurity risks. The following table shows the alignment of the FY 2025 IG FISMA Reporting Metric domain areas with the NIST CSF 2.0 Function areas (Table 1).

[11] NIST Special Publication 800-53 Revision 5, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.
[12] NIST Cybersecurity Framework 2.0, available at: The NIST Cybersecurity Framework (CSF) 2.0.

Table 1: NIST CSF 2.0 Function and Domain Area Alignment

Function Area	Function Area Objective	Domain Area(s)
Govern	Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Cybersecurity Governance**
		Cybersecurity Supply Chain Risk Management (C-SCRM)
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 and Asset Management (RAM)**
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 (IDAM)
		Data Protection and Privacy (DPP)
		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 2025 IG FISMA Reporting Metrics.

Zero Trust Architecture

OMB Memorandum M-22-05[13] 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." The implementation of Zero Trust principles within an agency is an ongoing effort rather than a one-time implementation. To fully implement a mature Zero Trust environment, agencies must commit significant resources to implement and sustain the efforts.

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:

[13] 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.

- **Identity**: Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant Multifactor Authentication (MFA) protects those personnel from sophisticated online attacks.
- **Devices**: The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices.
- **Networks**: Agencies encrypt all Domain Name System (DNS) requests and Hypertext Transfer Protocol (HTTP) traffic within their environment and begin executing a plan to break down their perimeters into isolated environments.
- **Applications and Workloads**: Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.
- **Data**: Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data and have implemented enterprise-wide logging and information sharing.

OMB Memorandum M-22-09 directed 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 2025 FISMA guidance listed in M-25-04 states OMB will continue to mature current and future metrics utilized to measure implementation of Zero Trust Principles.

In FY 2022, the FDIC developed and submitted a Zero Trust Implementation Plan 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. During FY 2024, progress was made to align with the Zero Trust Implementation Plan, including the completion of six out of thirteen tasks identified at that time. In FY 2025, the FDIC updated the Zero Trust Implementation Plan in May 2025 to further refine and enhance milestones in alignment with changes made to the CIOO Roadmap. This roadmap focuses on modernizing IT systems, improving service delivery, and enhancing cybersecurity by aligning IT investments with business strategy.

While the FDIC continued to make progress towards meeting M-22-09 objectives, based on the Implementation Plan Status, actions required by M-22-09 have not been fully implemented. Specifically, progress was made across the five pillars to implement the OMB requirements; however, dates of implementation span the timeframe from 2023 through 2029. Although the FDIC was behind in its implementation efforts to meet the requirements of M-22-09, KPMG determined that management implemented measures to perform a robust analysis on current state, future state, and actions required to meet future state goals.

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.*[14] 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 establishing centralized access and visibility for the enterprise security operations center 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), agencies should achieve 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), agencies should 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), agencies should achieve EL3 maturity.

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

As of July 10, 2025, 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 achieved the logging requirements at EL1, established a project plan to meet EL2 and EL3, and awaited CISA guidance during our evaluation scope period, KPMG did not issue a recommendation with respect to the FDIC's progress satisfying the M-21-31 requirements.

[14]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 Inventory

M-25-04 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. M-25-04 directed each agency to inventory its Internet of Things (IoT) devices by the end of FY 2024.

In FY 2025, the FDIC made progress towards meeting the intent of M-25-04. Specifically, the FDIC completed the creation of an inventory structure and continued to refine the attributes and elements contained within the inventory. KPMG noted the FDIC was also establishing a process to consistently maintain the inventory, to include performing a gap analysis over asset management. However, KPMG determined that the FDIC did not currently have an IoT inventory in place in accordance with M-25-04 Section II. 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 was 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, the function areas, and the overall program. The OMB considers a security program effective if the calculated average of the FY 2025 Core and Supplemental IG FISMA Metrics is 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. Table 3 provides 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 2025, the DHS FISMA Reporting Metrics used a calculated, weighted average rating methodology, wherein certain metrics that have a greater importance or provide an interdependent relationship to other metrics are scored more heavily. 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 information security program. Because of this 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 as 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: Metric Ratings by Function Area and the Overall Information Security Program

Function Area	Domain	Domain Core Metric Average	Domain Supplemental Metric Average	Domain Overall Average	Function Overall Average	Overall Average
Govern	Cybersecurity Governance	**N/A**	**3.33**	**3.33**	**3.57**	**4.02**
	C-SCRM	**5**	**N/A**	**5**		
Identify	RAM	**4.60**	**4**	**4.40**	**4.40**	
Protect	Configuration Management	**4.50**	**N/A**	**4.5**	**3.63**	
	IDAM	**3**	**N/A**	**3**		
	DPP	**4**	**N/A**	**4**		
	Security Training	**3**	**N/A**	**3**		
Detect	ISCM	**4**	**4**	**4**	**4**	
Respond	Incident Response	**3.50**	**N/A**	**3.50**	**3.50**	
Recover	Contingency Planning	**5**	**N/A**	**5**	**5**	

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

Based on the ratings of the core and supplemental metrics, KPMG determined that the FDIC information security program was rated a Level 4 maturity, effective. A Level 4 maturity is typically categorized as having quantitative and qualitative measures of the effectiveness of policies, procedures, and strategies that have been defined and consistently implemented across the organization that are used to assess and make necessary changes.[15]

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. However, KPMG noted the following in respect to the evaluated domains for FY 2025:

- Cybersecurity Governance was identified as a Level 3 maturity due to a lack of policy and procedures to maintain current and target cybersecurity profiles.
- Identity and Access Management (IDAM) was identified as a level 3 maturity with two, prior-year open recommendations and four new open recommendations.
- Security Training was also rated as a Level 3 maturity. Although the FDIC has performed a workforce assessment to identify gaps in skills and resources, the gaps identified as a result of this assessment had not yet been addressed during our evaluation scope period.

All other Domains evaluated had no open recommendations reported during the FY 2025 FISMA evaluation and obtained an effective, Level 4 or higher maturity rating.

[15] Stated from the FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0.

In response to the recommendations that remained open as of the report in September 2024, the FDIC also took action to strengthen related security controls. For example, the FDIC:

- Completed corrective actions to improve flaw remediation to include closing related Plans of Action and Milestones (POA&M) and updating policies and procedures to clarify the requirement to open and maintain POA&Ms from identified vulnerabilities.
- Implemented corrective actions to resolve a technical issue related to Role-Based training requirements.[16]

However, this and prior FISMA reports describe security control weaknesses that diminished the effectiveness of the FDIC's information security program and practices. The FDIC can counteract risks associated with these weaknesses by improving controls over the confidentiality, integrity, and availability[17] 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. Prior year security control weaknesses identified include:

- The FDIC Did Not Timely Notify or Remove Network Accounts (identified in report AUD-23-004).[18]
- The FDIC Did Not Fully Implement Audit Logging Requirements on Assessed Information Systems (identified in report EVAL-24-07).[19]

Appendix II notes two outstanding recommendations warranting the FDIC's continued attention to address these weaknesses identified in prior FISMA reports remain open as of July 10, 2025.

Security control weaknesses identified in this year's evaluation include:

- The FDIC Did Not Implement Privileged Access Review Frequency Requirements for (b) (7)(E).
- The FDIC Did Not Implement Privileged Access Review Frequency Requirements for (b) (7)(E).
- The User Listing Utilized for the (b) (7)(E) User Recertification Was Not Complete and Accurate.

[16] This corrective action was assessed and closed by the OIG prior to KPMG performing the FY 2025 FISMA evaluation.
[17] 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.
[18] AUD-23-004, *The Federal Deposit Insurance Corporation's Information Security Program – 2023*, AUD-23-004-Redacted.pdf.
[19] EVAL-24-07, *The FDIC's Information Security Program–2024*, FISMA 2024-EVAL-24-07 - Final Report - Redacted.pdf.

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.

GOVERN

The *Govern* Function area includes the evaluation of the agency's Cybersecurity Governance and C-SCRM.

Cybersecurity Governance

The *Cybersecurity Governance* Domain emphasizes the need for agencies to establish a robust framework for managing cybersecurity risks. It focuses on aligning cybersecurity strategies with organizational goals, ensuring compliance with federal policies, and integrating cybersecurity into enterprise risk management processes. As noted above, KPMG assessed the Cybersecurity Governance Domain as Level 3, *Consistently Implemented* (Not effective).

In order to reach an effective maturity rating, the FDIC must establish formal policies and procedures for developing and maintaining current and target cybersecurity profiles in alignment with NIST CSF 2.0. The FDIC should consider seeking guidance from external authorities to understand the requirements and expectations surrounding the use and maintenance of cybersecurity profiles. Due to the lack of federal guidance and criteria, KPMG did not issue a recommendation to the FDIC.

Cybersecurity Supply Chain Risk Management

The *Cybersecurity Supply Chain Risk Management* Domain emphasizes the integration of supply chain security into the broader cybersecurity governance framework. It focuses on assessing agencies' performance and maturity in managing risks associated with external providers, ensuring that products, systems, and services align with cybersecurity standards. As noted above, KPMG assessed the Cybersecurity Supply Chain Risk Management Domain as Level 5, *Optimized* (Effective).

IDENTIFY

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

Risk and Asset Management

The *Risk and Asset 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, software licenses, and data; 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 and Asset Management Domain as Level 4, *Managed and Measurable* (Effective).

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 configuration management roles and responsibilities; installing software patches to address security vulnerabilities; applying software updates, including 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 Configuration Management Domain as Level 5, *Optimized* (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, 2025, the FDIC successfully implemented the recommendation by closing the 31 identified POA&Ms.

Additionally, in the FISMA report for FY 2024, a recommendation was issued to update and implement the POA&M Management and Acceptance of Risk Process document to clearly define requirements as to when vulnerabilities must be documented within a POA&M, and what the remediation timeline for POA&Ms must be. As of July 10, 2025, the FDIC successfully implemented the recommendation.

Identity and Access Management

The *Identity and Access Management* 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 3, *Consistently Implemented* (Not 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. Although the FDIC initially provided an estimated completion date of June 28, 2024; KPMG noted as of July 10, 2025, the recommendation remained open.

In the FY 2024 FISMA report, a recommendation was issued to enforce existing policies and procedures to consistently perform reviews of and analyze system audit records, and document and maintain those reviews and analysis for privileged users and actions taken on (b) (7)(E) [redacted] devices in accordance with FDIC policy. As of July 10, 2025 the

recommendation remained open with a planned estimated completion date of September 30, 2025.

Additionally, during FY 2025, the FDIC's management of privileged user accounts still needed improvement based on issues identified in its implementation of Identity and Access Management security controls, as noted below.

The FDIC Did Not Implement Privileged Access Review Frequency Requirements for (b) (7)(E)

(b) (7)(E) consists of Microsoft server operating systems, software, and services on both virtual and physical servers residing in FDIC facilities. (b) (7)(E) hosts major and minor applications, services, and software that support the FDIC business mission. It also interconnects with other FDIC systems through the (b) (7)(E) Local Area Network and Wide Area Network (LAN/WAN) infrastructure and provides centralized authentication services to FDIC infrastructure resources.

User access review is a process that involves periodically evaluating user access rights within an organization to assess whether users have appropriate access to systems and data based on their roles, reducing the risk of unauthorized access and data breaches. By removing unnecessary or outdated permissions, the process enhances the overall security of the system or network environment, thus ensuring that only authorized personnel have access to sensitive information and resources. It is crucial that the FDIC implement proper user access review in accordance with security policies and procedures since privileged users can perform functions such as system configuration and management, data manipulation, and security administration.

While KPMG noted that FDIC management did perform a user access review for all administrator accounts within (b) (7)(E) it was not performed and documented every 90 days as required by FDIC policy.

KPMG noted a lack of dissemination of the FDIC access review requirements and operational challenges; as a result, system management did not perform the review every 90 days. KPMG noted that a subset of administrator accounts within (b) (7)(E) were performed on a quarterly basis as of January 1, 2025.

KPMG recommends the **Chief Information Officer**:

1. Ensure privileged user access reviews for the (b) (7)(E) system are performed in accordance with FDIC policy.

The FDIC Did Not Implement Privileged Access Review Frequency Requirements for (b) (7)(E)

(b) (7)(E) is the FDIC's implementation of the Oracle PeopleSoft Human Capital Management (HCM) system that maintains organizational and position information for the FDIC, which is transmitted to U.S. Department of Agriculture National Finance Center. (b) (7)(E) hosts the Division of Finance's Supplemental Payment System within the (b) (7)(E) database

As noted above, it is crucial that the FDIC implements proper user access review in accordance with security policies and procedures.

While KPMG noted that FDIC management did perform a user access review for privileged accounts within (b) (7)(E) all privileged accounts were not reviewed every 90 days as required by FDIC policy. This included, but was not limited to, roles such as System Administrator – (b) (7)(E) and Security Administrator – (b) (7)(E).

KPMG noted that FDIC management did not document which roles, privileges, and accounts were considered privileged within (b) (7)(E) As such, management did not enforce the requirement to ensure that all accounts that can perform privileged functions, such as user access modifications, are reviewed every 90 days.

KPMG recommends the **Division of Finance (DOF) in coordination with CIOO**:

2. Define the accounts, permissions, and roles that are considered privileged within (b) (7)(E)
3. Ensure privileged user access reviews for (b) (7)(E) are performed in accordance with FDIC policy.

The User Listing Utilized for the (b) (7)(E) User Recertification Was Not Complete and Accurate

To perform an effective user access review, it is imperative that the information used to perform the review is complete and accurate. Without a complete and accurate listing, users with access to systems and data could be unaccounted for during management's review of the access, which could result in users maintaining inappropriate access to sensitive information and resources. Further, a thorough user listing supports the detection of redundant or outdated accounts, which can be a security risk if not properly managed.

KPMG noted that the FDIC utilized a user listing maintained in the (b) (7)(E) , the FDIC's Identity and Access Management System, to perform the (b) (7)(E) Business Owner Certification. When users from the (b) (7)(E) user listing were selected for testing, 2 users out of 25 sampled users with roles in (b) (7)(E) were not included within the (b) (7)(E) user listing; however, these roles were active within (b) (7)(E) As such, we determined that the (b) (7)(E) user listing used in the performance of the user access review was not complete and accurate.

KPMG recommends the **DOF in coordination with CIOO**:

4. Ensure a complete and accurate user listing is utilized for the (b) (7)(E) user access review as required by 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).

At the time of our assessment of the FY 2025 IG Metrics, FDIC management had performed a workforce assessment to identify gaps in skills and resources. However, the gaps identified as a result of this assessment have not been completed. KPMG determined that to obtain a Level 4, Effective rating, the FDIC should continue to address the gaps identified within the completed workforce assessment.

The FDIC also completed corrective actions for a recommendation issued in the FY 2024 FISMA report related to addressing technical issues preventing enforcement of Role-Based training requirements. This recommendation was closed by the OIG after the FY 2024 FISMA report was issued.

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, 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, 2025, 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 required for the FDIC to fully comply with EL2 requirements. Therefore, KPMG did not issue a recommendation addressing this issue. The FDIC 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 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 5, *Optimized* (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 four 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.

Testing of internal controls was designed to assess the maturity levels for the associated metrics as defined in the FY25 IG FISMA Metric guidance. The scope of our assessment of internal controls was limited to those that were responsive to OMB Office of the Federal Chief Information Officer *FY 2025 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, 2025 (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 M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* (December 2023), when planning and conducting our work. KPMG also consulted the FY 2025 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, 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.[20] 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 this evaluation remotely at its off-site locations within the United States from January through July 2025.

[20] 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 an 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 2022, 2023, and 2024. Recommendations marked 'Closed' denote status updates that followed the publication of the FISMA report in 2024.

Recommendation	Status
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).	Closed
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 2024, Recommendation 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.	Closed
Report Issued in 2024, Recommendation 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.	Unimplemented
Report Issued in 2024, Recommendation 3 Remediate the technical issues within the 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.	Closed

APPENDIX III – LIST OF ACRONYMS

Acronym	Description
AICPA	American Institute of Certified Public Accountants
(b) (7)(E)	(b) (7)(E)
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
(b) (7)(E)	(b) (7)(E)
CM	Configuration Management
C-SCRM	Cybersecurity Supply Chain Risk Management
CSF 2.0	Cybersecurity Framework 2.0
(b) (7)(E)	(b) (7)(E)
DHS	Department of Homeland Security
DNS	Domain Name System
DOF	Division of Finance
DPP	Data Protection and Privacy
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
GSS	General Support System
HTTP	Hypertext Transfer Protocol
IDAM	Identity and Access Management
IG	Inspector General
IoT	Internet of Things
ISCM	Information Security Continuous Monitoring
ITRAC	IT Risk Advisory Council
KPMG	KPMG LLP
LAN	Local Area Network
MEF	Mission Essential Function
MFA	Multifactor Authentication
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
RAM	Risk and Asset Management
SCRM	Supply Chain Risk Management
SP	Special Publication
WAN	Wide Area Network

The FDIC's Information Security Program – 2025

Part II

****

FDIC Comments and OIG Evaluation

FDIC COMMENTS AND OIG EVALUATION

On September 15, 2025, the Chief Information Officer, Chief Privacy Officer, and Director of Information Technology; the Chief Information Security Officer; and the Director, Division of Finance provided a written response to a draft of this report, which is presented in its entirety starting on page II-3.

In its response, the FDIC concurred with all four new recommendations and plans to complete corrective actions by May 29, 2026. The OIG assessed the FDIC's proposed corrective actions and determined they were sufficient to address the intent of the recommendations. 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-6.

APPENDIX 1: FDIC COMMENTS

Federal Deposit Insurance Corporation

MEMO

TO: Matthew W. Simber
Acting Assistant Inspector General for Audits
Office of Inspector General

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

SYLVIA BURNS Digitally signed by SYLVIA BURNS Date: 2025.09.15 15:37:36 -04'00'

Zachary N. Brown
Chief Information Security Officer

ZACHARY BROWN Digitally signed by ZACHARY BROWN Date: 2025.09.15 15:09:36 -04'00'

Donna Saulnier
Director, Division of Finance

DONNA SAULNIER Digitally signed by DONNA SAULNIER Date: 2025.09.15 12:25:29 -04'00'

CC: Mark F. Mulholland, Deputy Chief Information Officer for Management
Sheena N. Burrell, Deputy Chief Information Officer for Technology and Chief Technology Officer

DATE: September 15, 2025

RE: Draft Office of Inspector General Evaluation Report, Entitled *The FDIC's Information Security Program–2025* (No. 2025-008)

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 28, 2025. The objective of the evaluation was to assess the effectiveness of the FDIC's information security program 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 that 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 National Institute of Standards and Technology standards and guidelines. The report also noted actions taken by the FDIC following the OIG's 2024 FISMA evaluation to strengthen security controls in the areas of flaw remediation, Plan of Actions and Milestones, and role-based training.

Notwithstanding these results, the OIG's evaluation identified weaknesses in the FDIC's security controls and practices. Such weaknesses include the need to: implement access reviews for privileged accounts consistent with established frequency requirements; use a complete and accurate user listing to support account recertifications, ensure prompt notification and removal of network accounts when users separate from the FDIC; and fully implement audit logging requirements for certain systems.

1

Federal Deposit Insurance Corporation

The draft report contains four recommendations addressed to the CIO and the Division of Finance (DOF).[1] FDIC management concurs with all four recommendations. A summary of management's planned and completed corrective actions and associated milestones follows.

Recommendation 1

We recommend that the CIO:

1. Ensure privileged user access reviews for the (b) (7)(E) system are performed in accordance with FDIC policy.

Management Decision: Concur

Corrective Action: The FDIC will review the (b) (7)(E) privileged user recertification process and policy, make appropriate updates, and ensure privileged user recertifications are conducted in accordance with the policy.

Estimated Completion Date: May 29, 2026

Recommendation 2

We recommend that DOF in coordination with the CIOO:

2. Define the accounts, permissions, and roles that are considered privileged within (b) (7)(E)

Management Decision: Concur

Corrective Action: The FDIC will review (b) (7)(E) user accounts, permissions, and roles and define which ones are considered privileged.

Estimated Completion Date: December 31, 2025

Recommendation 3

We recommend that DOF in coordination with the CIOO:

3. Ensure privileged user access reviews for (b) (7)(E) are performed in accordance with FDIC policy.

Management Decision: Concur

Corrective Action: The FDIC will review the (b) (7)(E) privileged user recertification process, make appropriate updates, and ensure privileged user recertifications are conducted in accordance with FDIC policy.

Completion Date: December 31, 2025

[1] (b) (7)(E) is a DOA-owned application; however, DOF manages security for (b) (7)(E) and will implement the corrective actions for recommendations 2-4.

2

Federal Deposit Insurance Corporation

Recommendation 4

We recommend that DOF in coordination with the CIOO:

4. Ensure a complete and accurate user listing is utilized for the (b) (7)(E) user access review as required by FDIC policy.

Management Decision: Concur

Corrective Action: The FDIC will perform reconciliations between profiles in the (b) (7)(E) (b) (7)(E) and roles in (b) (7)(E) to ensure the user listings in (b) (7)(E) and (b) (7)(E) are complete and accurate prior to performing recertifications. Any inconsistencies identified in these reviews will be resolved prior to conducting (b) (7)(E) user recertifications.

Completion Date: December 31, 2025

3

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 review the (b) (7)(E) privileged user recertification process and ensure privileged user recertifications are conducted in accordance with the updated policy.	May 29, 2026	$0	Yes	Open
2	The FDIC will review (b) (7)(E) user accounts, permissions, and roles and define which ones are considered privileged.	December 31, 2025	$0	Yes	Open
3	The FDIC will review the (b) (7)(E) privileged user recertification process and ensure privileged user recertifications are conducted in accordance with the updated policy.	December 31, 2025	$0	Yes	Open
4	The FDIC will perform reconciliations to ensure user listings are complete and accurate prior to performing user recertifications.	December 31, 2025	$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| @FDIC_OIG
Oversight.gov | www.oversight.gov