FDIC Office of Inspector General

The FDIC's Information Security Program - 2026

Office of Audits

September 2026 | EVAL-26-02

Office of Inspector General

REDACTED VERSION
PUBLICLY AVAILABLE

The redactions 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.

Executive Summary

The FDIC's Information Security Program - 2026 (EVAL-26-02) September 25, 2026

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 2026 FISMA Metrics. As shown in the table below, KPMG assigned an Effective Rating for all six FISMA functions for FY 2026.

2026 Core and Supplemental Scores by Function

Function	Weighted Average	Maturity	Effectiveness
Govern	4.33	4	Effective
Identify	4.40	4	Effective
Protect	3.88	4	Effective
Detect	4.00	4	Effective
Respond	4.00	4	Effective
Recover	4.67	4	Effective
Overall	**4.23**	**4**	**Effective**

KPMG found that the FDIC established several information security program controls and practices that were consistent with FISMA requirements. However, the report references previously identified security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices. KPMG did not identify any new areas specific to this year's metrics that the FDIC should continue to improve in order enhance the agency's security program.

Further, since the 2025 FISMA evaluation, the FDIC has addressed and implemented four prior FISMA recommendations.

Status of Prior Year Recommendations

Year	Total	Closed (Implemented)	Open (Unimplemented)
2023	2	1	1*
2024	1	1	0
2025	4	3	1

* Open pending the results of another ongoing OIG audit.

Recommendations

KPMG made no new recommendations during this year's FISMA evaluation. In response, the FDIC committed to completing corrective actions on two prior unimplemented recommendations.

Date: September 25, 2026

Memorandum To: Zachary N. Brown
Chief Information Officer

From: Jason M. Yovich
Acting Assistant Inspector General for Audits

Subject The FDIC's Information Security Program - 2026 | EVAL-26-02

Enclosed is the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) report on The FDIC's Information Security Program - 2026.

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 (703) 562-6165.

The FDIC's Information Security Program - 2026

Part I

****

Report by KPMG LLP

THE FEDERAL DEPOSIT INSURANCE CORPORATION'S INFORMATION SECURITY PROGRAM – 2026

EVALUATION REPORT

SEPTEMBER 18, 2026

KPMG LLP
1801 K Street NW
Washington DC 20006

TABLE OF CONTENTS

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

Jason Yovich
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 – 2026

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 2026 through July 2026, and our results are as of July 28, 2026.

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.

[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.

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)[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**. 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 and issued by the OMB, the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) on April 3, 2025. OMB did not release new reporting metrics for FY 2026 and directed agencies to use the FY 2025 IG FISMA Metrics for the required annual Inspector General FISMA evaluation.

[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.

- Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (M-22-09)[5]
- Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (M-22-01)[6]
- Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31)[7]

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[8] 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.[9]

During FY 2025, OMB and CIGIE introduced a weighted average approach to the scoring methodology. As of the issuance of this report, OMB did not release new reporting guidance for FY 2026. As such, the scoring methodology remained the same for the FY 2026 evaluation. The new scoring is designed to account for select metrics that have a greater importance or provide interdependent relationships with 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.

---

[5] OMB, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, M-22-09 (January 26, 2022), available at: M-22-09 (whitehouse.gov).
[6] 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: M-22-01(whitehouse.gov).
[7] OMB, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, M-21-31 (August 27, 2021), available at: M-21-31(whitehouse.gov).
[8] 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). OMB did not release new reporting metrics for FY 2026 and directed agencies to use the FY 2025 IG FISMA Metrics for the required annual Inspector General FISMA evaluation.
[9] 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).

Effective May 17, 2026, the FDIC appointed a new CIO, following the announced retirement of the former CIO, effective July 31, 2026. The FDIC additionally appointed leadership to serve as both the acting FDIC CISO and Deputy Director of the OCISO.

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. In addition, the FDIC has established an Artificial Intelligence (AI) program with an established governance structure with the AI Coordination Committee (AICC) to promote AI use cases and solutions across the agency. Specifically, in June 2025 the Acting Chairman established the AI governance structure for the agency to align with Executive Order 14179, *Removing Barriers to American Leadership in Artificial Intelligence*. These information 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) .
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,[10] and the FY 2026 IG FISMA Reporting Metrics, which are aligned to the NIST CSF 2.0.[11] NIST CSF 2.0 is a set of guidelines and leading practices designed to help organizations manage and reduce cybersecurity risks. Table 1 shows the alignment of the FY 2026 IG FISMA Reporting Metric domain areas with the NIST CSF 2.0 Function areas.[12]

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: IG FISMA Reporting Metrics.

[10] NIST Special Publication 800-53 Revision 5, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.
[11] NIST Cybersecurity Framework 2.0, available at: The NIST Cybersecurity Framework (CSF) 2.0.
[12] OMB did not release new reporting metrics for FY 2026 and directed agencies to use the FY 2025 IG FISMA Metrics for the required annual Inspector General FISMA evaluation.

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:

- **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 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

[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.

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. In FY 2026, the FDIC updated the Zero Trust Implementation Plan in December 2025 and February 2026 to ensure the implementation plan is up to date and current.

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 2030. Although the FDIC had not fully met requirements to meet 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 (EL)

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.

On May 22, 2026, OMB released Memorandum M-26-14, *Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats*.[15] Upon issuance, the Memo rescinded M-21-31 and focused agencies on "an adaptive framework that enables them to effectively and efficiently monitor their networks while minimizing red tape and containing costs." While the primary focus remains on the effective and mature logging capabilities, the Memo provides a revised maturity model: Initial (Level 1), Intermediate (Level 2), Advanced (Level 3), and Optimal (Level 4). Further, it establishes new requirements to be guided by CISA and a new schedule for agency implementation. See **Table 2** below for a summary of the Action Items and timeline requirement for agency implementation.

Table 2: Summary of Agency Implementation Requirements and Timeline

Requirement	Timeline
Complete the first version of the Agency Logging Plan, providing for fulfillment of this memorandum's minimum requirements and using the guidance and resources within the Logging Reference Architecture (LRA).	Within 90 days of the release of the LRA
Achieve a minimum of Basic (Level 1) across all elements of the maturity model.	Within 120 days of the release of the LRA
Achieve a minimum of Intermediate (Level 2) across all elements of the maturity model	Within 180 days of the release of the LRA

[14]OMB, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, M-21-31, available at: M-21-31(whitehouse.gov).
[15] OMB, *Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats*, M-26-14, available at: M-26-14 (whitehouse.gov)

Achieve a minimum of Advanced (Level 3) across all elements of the maturity model.	Within 360 days of the release of the LRA
• Within 30 calendar days, update the Agency Logging Plan. • Within 60 calendar days, achieve a minimum of "Intermediate" across all elements of the maturity model. • Within 120 calendar days, achieve a minimum of "Advanced" across all elements of the maturity models.	Ongoing Actions: After CISA notifies agencies that there is an updated version of the logging reference architecture

As of May 22, 2026, the FDIC had reached level Event Logging (EL)1 in alignment with M-21-31 requirements, 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 issuance of OMB M-26-14, the FDIC has established a project plan to meet the requirements for M-26-14, which originally was established to meet EL2 and EL3. As such, KPMG did not issue a recommendation with respect to the FDIC's progress satisfying the M-21-31 requirements or newly issued M-26-14 requirements, as the timeframes for meeting M-26-14 were not due as of the issuance of this report.

Internet of Things (IoT) Inventory

M-25-04 identified "Fiscal Year 2025 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.

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. In FY 2026, the FDIC continued to mature its enterprise IT inventory management capabilities, including the identification and management of applicable IoT devices. Specifically, it continues to utilize (b) (7)(E) and its automated discovery capabilities to identify technology detectable within the managed network environment and maintain associated inventory and configuration records. The IoT inventory is maintained to include the name, asset, asset tag, updated date, manufacturer, location, install status and first discovered date.

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 2026 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 IG 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. As of the issuance of this report, OMB did not release new reporting guidance. As such, the scoring methodology remained the same for the FY 2026 evaluation. 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 Weighted Average	Function Overall Weighted Average	Overall Weighted Average
Govern	Cybersecurity Governance	N/A	4.33	4.33	4.43	4.23
	C-SCRM	5	N/A	5		
Identify	RAM	4.60	4	4.40	4.40	
Protect	Configuration Management	4.50	N/A	4.50	3.88	
	IDAM	3.67	N/A	3.67		
	DPP	4	N/A	4		
	Security Training	3	N/A	3		
Detect	ISCM	4	4	4	4	
Respond	Incident Response	4	N/A	4	4	
Recover	Contingency Planning	4.5	N/A	4.5	4.67	

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.[16]

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 2026:

- Identity and Access Management (IDAM) was identified with two prior-year open recommendations.
- Security Training was also rated as a Level 3 maturity. The FDIC is in the process of finalizing the workforce assessment for FY 2026 and has begun addressing immediate workforce gaps. However, the FDIC has not yet addressed specific knowledge, skills, and abilities gaps that would be identified as a result of the in-depth workforce assessment.

All other Domains evaluated had no open recommendations reported during the FY 2026 FISMA evaluation and obtained an effective, Level 4 or higher maturity rating.

In response to the recommendations that remained open as of the report in September 2025, the FDIC also took action to strengthen related security controls. For example, the FDIC:

- Implemented corrective actions to perform and document periodic reviews of audit logs for the (b) (7)(E) devices.
- Implemented corrective actions to define the accounts, permissions, and roles that are considered privileged for the (b) (7)(E) system.
- Implemented corrective actions to perform and document review of all (b) (7)(E) privileged accounts according to FDIC policy.
- Implemented corrective actions to resolve an issue related to the completeness and accuracy of the user listing used to recertify (b) (7)(E) business owners.

However, these and prior FISMA reports describe security control weaknesses that diminished the effectiveness of the FDIC's information security program and practices. 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).[17]
- The FDIC Did Not Implement Privileged Access Review Frequency Requirements for (b) (7)(E) (identified in report EVAL-25-03).[18]

---

[16] Stated from the FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0.
[17] AUD-23-004, *The Federal Deposit Insurance Corporation's Information Security Program – 2023*, AUD-23-004-Redacted.pdf.
[18] EVAL-25-03, The FDIC's Information Security Program – 2025. EVAL-25-03-Redacted.pdf

KPMG did not identify any new security control weaknesses during the current year's evaluation.

Appendix II notes the two outstanding recommendations warranting the FDIC's continued attention.

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.

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 4, *Managed and Measurable* (Effective).

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 (RAM)* 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 4, *Managed and Measurable* (Effective).

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 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. Although the FDIC submitted a recommendation closure package to the OIG for review in January 2026; KPMG noted as of July 28, 2026, the recommendation overlapped with the scope of another on-going OIG audit and the recommendation will remain open pending the results of that audit.

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) (b) (7)(E) devices in accordance with FDIC policy. As of July 28, 2026, KPMG noted the FDIC successfully implemented the recommendation by developing and implementing procedures to review (b) (7)(E) audit logs.

In the FY 2025 FISMA report, recommendations were issued to address weaknesses in the user account review process. These specifically focused on ensuring all privileged user access reviews were performed in accordance with policy for the (b) (7)(E) and (b) (7)(E) systems; defining privileged accounts, permissions, and roles, within (b) (7)(E); and ensuring a complete and accurate user listing is utilized for user account reviews for (b) (7)(E). As of July 28, 2026, KPMG noted the FDIC successfully addressed and closed the three (b) (7)(E) recommendations by updating and implementing its privileged user account review process. The recommendation regarding the (b) (7)(E) user account review remains open.

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 2026 IG FISMA Metrics, FDIC management was in the process of finalizing a workforce assessment to identify gaps in skills and resources. KPMG determined that to obtain a Level 4, Effective rating, the FDIC should finalize the workforce assessment and address the gaps identified within the completed workforce assessment.

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 directed agencies to improve their event logging and log management capabilities along three maturity levels (EL1, EL2, and EL3). As of May 22, 2026, the FDIC

reached level EL1 in alignment with M-21-31 requirements, as it was able to demonstrate that it could log the required events as well as collect, maintain, and protect event logs.

Since the issuance of OMB M-26-14, the FDIC has established a project plan to meet the requirements for M-26-14, which originally was established to meet EL2 and EL3. As such, KPMG did not issue a recommendation with respect to the FDIC's progress satisfying the M-21-31 requirements or newly issued M-26-14 requirements.

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 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 does not contain any new recommendations but 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 FY 2026 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 2026 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, 2026 (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 2026 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 judgmentally selected these systems in coordination with the FDIC OIG. 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 2026.

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 2023, 2024, and 2025. Recommendations marked 'Closed' denote status updates that followed the publication of the FISMA report in 2024.

Recommendation	Status
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 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.	Closed
Report Issued in 2025, Recommendation 1 Ensure privileged user access reviews for the (b) (7)(E) system are performed in accordance with FDIC policy.	Unimplemented
Report Issued in 2025, Recommendation 2 Define the accounts, permissions, and roles that are considered privileged within (b) (7)(E)	Closed
Report Issued in 2025, Recommendation 3 Ensure privileged user access reviews for (b) (7)(E) are performed in accordance with FDIC policy.	Closed
Report Issued in 2025, Recommendation 4 Ensure a complete and accurate user listing is utilized for the (b) (7)(E) user access review as required by FDIC policy.	Closed

APPENDIX III – LIST OF ACRONYMS

Acronym	Description
AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants
(b) (7)(E)	[redacted]
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
CM	Configuration Management
C-SCRM	Cybersecurity Supply Chain Risk Management
CSF 2.0	Cybersecurity Framework 2.0
(b) (7)(E)	[redacted]
DHS	Department of Homeland Security
DPP	Data Protection and Privacy
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
(b) (7)(E)	[redacted]
HTTP	Hypertext Transfer Protocol
IDAM	Identity and Access Management
IG	Inspector General
IoT	Internet of Things
ISCM	Information Security Continuous Monitoring
KPMG	KPMG LLP
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
RAM	Risk and Asset Management
SP	Special Publication

The FDIC's Information Security Program - 2026

Part II

****

FDIC Comments and OIG Evaluation

September 2026 | EVAL-26-02

The FDIC's Information Security Program - 2026

FDIC COMMENTS AND OIG EVALUATION

On September 14, 2026, the Chief Information Officer, Chief Privacy Officer, and Director of Information Technology; and the Acting Chief Information Security Officer provided a written response to a draft of this report, which is presented in its entirety in Appendix 1.

In its response, the FDIC noted that no new security control weaknesses or recommendations were identified as part of the Fiscal Year (FY) 2026 FISMA evaluation. However, two recommendations from prior FISMA reports remain open and warrant continued attention. The response indicates that the FDIC is committed to completing corrective actions to address these outstanding recommendations and further strengthen its information security program.

APPENDIX 1: FDIC COMMENTS

FDIC Federal Deposit Insurance Corporation

MEMO

TO: Jason Yovich
Acting Assistant Inspector General
Office of Inspector General

FROM: Zachary N. Brown
Chief Information Officer, Chief Privacy Officer, and
Director, Division of Information Technology

ZACHARY BROWN Digitally signed by ZACHARY BROWN Date: 2026.09.14 11:05:38 -04'00'

Rami Dillon
Acting Chief Information Security Officer

RAMI DILLON Digitally signed by RAMI DILLON Date: 2026.09.14 10:07:40 -04'00'

CC: Nicholas Thottam, Acting Deputy CIO for Management
Jill Lennox, Chief Risk Officer

DATE: September 14, 2026

RE: Audit of the FDIC's Information Security Program - 2026 (No. 2026-002)

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, entitled *The FDIC's Information Security Program – 2026 (EVAL-2026-002)*. The objective of the evaluation was to assess the effectiveness of the FDIC's information security program and practices. The FDIC appreciates the OIG's assessment and remains fully committed to maintaining an effective information security program and continuously strengthening its cybersecurity posture.

We are pleased that the OIG's evaluation determined that the FDIC's information security program was operating at maturity level of 4 (Managed and Measurable) and was Effective for Fiscal Year (FY) 2026. The evaluation assigned an Effective rating to all six of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 function areas—Govern, Identify, Protect, Detect, Respond, and Recover—and an overall maturity level of 4, Managed and Measurable. These results demonstrate that the FDIC has established and consistently implemented information security policies, procedures, controls, and practices that support the FDIC's mission to maintain stability and public confidence in the nation's financial system.

During the evaluation period, the FDIC continued to strengthen and mature its information security program. The FDIC established formal policies and procedures for developing and maintaining current and target cybersecurity profiles in alignment with the NIST CSF 2.0. These profiles provide a structured approach for assessing the FDIC's current cybersecurity posture, defining its desired future state, and informing cybersecurity risk management and improvement activities. In addition, the FDIC made meaningful progress in addressing previously identified weaknesses. Since the FY 2025 FISMA evaluation, the FDIC implemented corrective actions to address four prior FISMA audit recommendations, including actions to strengthen periodic reviews of audit logs for certain devices and improving the management and review of privileged access accounts for its (b) (7)(E) (b) (7)(E)

The FDIC's Information Security Program - 2026

FDIC Federal Deposit Insurance Corporation

Notwithstanding these accomplishments, the FDIC recognizes that maintaining an effective information security program requires continuous improvement as technologies, threats, and Federal cybersecurity requirements evolve.

The OIG identified no new security control weaknesses and made no new recommendations as part of the FY 2026 FISMA evaluation. However, two recommendations from prior FISMA reports remain open and warrant continued attention. The FDIC remains committed to completing appropriate corrective actions to address these outstanding recommendations and further strengthen the effectiveness of its information security program.

The FDIC appreciates the OIG's recognition of the FDIC's progress in FY 2026 and will continue to mature its cybersecurity capabilities; address identified areas for improvement; and protect the confidentiality, integrity, and availability of FDIC information and systems.

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