FDIC Office of Inspector General

Audit of Security Controls for the FDIC's Cloud Computing Environment

Audit Report - Final - Audits, Evaluations, and Cyber

September 2024 | No. **AUD-24-01**

Office of Inspector General

REDACTED VERSION
PUBLICLY AVAILABLE

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

Integrity • Independence • Accuracy • Objectivity • Accountability

NOTICE

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

Office of Inspector General

Federal Deposit Insurance Corporation
Office of Inspector General
Audits, Evaluations, and Cyber

Date: September 4, 2024

Memorandum To: Sylvia W. Burns
Chief Information Officer

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

Subject **Audit of Security Controls for the FDIC's Cloud Computing Environment** | No. AUD-24-01

Enclosed is the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) report on the *Audit of Security Controls for the FDIC's Cloud Computing Environment*.

The FDIC OIG contracted with the independent certified public accounting firm, Sikich CPA LLC (Sikich), to conduct a performance audit of the security controls for the FDIC's cloud computing environment. The contract required Sikich's audit work to be conducted in accordance with Generally Accepted Government Auditing Standards. The objective of this performance audit was to assess the effectiveness of security controls for the FDIC's cloud computing environment.

Sikich is responsible for the enclosed report. The OIG reviewed Sikich'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 Sikich did not comply with the Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States.

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

OIG
Office of Inspector General

Executive Summary

Audit of Security Controls for the FDIC's Cloud Computing Environment (AUD-24-01) ***September 4, 2024***

What We Did

We engaged with Sikich CPA LLC (Sikich) to conduct a performance audit of security controls for the FDIC's cloud computing environment. The objective of this performance audit was to assess the effectiveness of security controls for the FDIC's cloud computing environment. To address this objective, Sikich performed tests of nine IT security control areas for cloud platforms and applications in use at the FDIC. Sikich also assessed policies and procedures, conducted interviews of responsible officials, and conducted penetration testing procedures.

Impact on the FDIC

The benefits of cloud computing do not eliminate the customer's responsibility to effectively manage security risks. The FDIC continues to expand its cloud presence by migrating its mission essential and mission critical applications into the cloud. The FDIC must ensure that its systems and data within the cloud are secured and that control weaknesses are effectively addressed. Failure to do so could result in damage and harm to FDIC systems and data, hindering its ability to maintain stability and confidence in the nation's financial system.

Results

Sikich found that the FDIC had effective controls in four of nine security control areas assessed. However, Sikich determined that the FDIC had not effectively implemented security controls in its cloud computing environment in five areas, including Identity and Access Management, Protecting Cloud Secrets, Patch Management, Flaw Remediation, and Audit Logging. Specifically, the report includes 26 cloud security findings (b) (7)(E) (b) (7)(E) cloud computing platforms, applications, and the Application Programing Interface platform that Sikich assessed during this audit. Due to the number of findings and similarities among them, Sikich identified six common themes of security weaknesses listed below:

1. **Insecure Coding Practices:** The FDIC cloud platform teams did not consistently implement secure coding practices.
2. **Misconfigured Security Settings:** The FDIC cloud platform teams did not consistently configure cloud platform security settings in accordance with cloud service providers and industry best practices.
3. **Least Privilege:** The FDIC did not consistently provision access to its cloud-based systems in accordance with the principle of least privilege.
4. **Outdated Software:** (b) (7)(E) relied on outdated software components.
5. **Ineffective Monitoring:** The FDIC did not adequately monitor the activity on its cloud-based systems.
6. **Cloud Service Provider Vulnerabilities:** Cloud service providers were solely responsible for causing certain vulnerabilities and should be responsible for their remediation.

Recommendations

Sikich made 7 formal recommendations and 48 related technical recommendations to improve cloud security controls in the 6 common themes of security weaknesses listed above. Five of the formal recommendations are aligned by cloud platform with related technical recommendations to address the 26 findings. The remaining two formal recommendations were intended to help mitigate and address the security risks identified in this audit for all FDIC cloud-based systems. The FDIC concurred with all recommendations and plans to complete all corrective actions by December 30, 2026.

Audit of Security Controls for the FDIC's Cloud Computing Environment

Part I

****

Report by Sikich

Performance Audit of Security Controls for the Federal Deposit Insurance Corporation's Cloud Computing Environment

Submitted to the
Federal Deposit Insurance Corporation
Office of Inspector General

Audit Report

September 4, 2024

Final Report

Table of Contents

Figures

SIKICH®

Terry L. Gibson
Assistant Inspector General for Audits, Evaluations, and Cyber
Office of Inspector General
Federal Deposit Insurance Corporation

Subject: Audit of Security Controls for the Federal Deposit Insurance Corporation's Cloud Computing Environment

Sikich CPA LLC (Sikich) is pleased to submit the attached report detailing the results of our performance audit of the Federal Deposit Insurance Corporation's (FDIC) Security Controls Over its Cloud-Based Systems. The FDIC Office of Inspector General (OIG) engaged Sikich to conduct this performance audit. Sikich performed the work from September 2022 through April 2024.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Sincerely,

(b) (7)(E)

Simon Lee CISA, CISSP
Director

Introduction

The FDIC, like other Federal agencies, is increasing its use and accelerating its adoption of cloud computing services. The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[1]

Cloud computing offers many potential benefits, including optimizing costs, flexibility, scalability, and enhanced security. It enables organizations to do more with less by eliminating their on-premises infrastructure with the reduction of servers and staff to support that infrastructure. According to NIST, cloud computing introduces different risks than an on-premises infrastructure, including system complexity, shared multi-tenancy environments, internet facing services, and loss of control over resources in the cloud service provider (CSP) environment.

As the FDIC continues to expand its cloud presence by migrating its mission essential and mission critical applications[2] into the cloud by 2026, the FDIC must ensure that its systems and data that operate in the cloud are secured effectively. In addition, control over cloud-based systems and applications will vary by cloud provider and delivery service type. While cloud computing offers many benefits, it does not eliminate the customer's responsibility to manage security risks appropriately, especially for multi-cloud environments, such as the FDIC's, where numerous services, configurations and access to cloud resources must be managed.

This audit report is the second of two reports related to cloud adoption at the FDIC. The FDIC OIG report, *The FDIC's Adoption of Cloud Computing Services* (AUD-23-003) (July 2023), had an objective to determine whether the FDIC had an effective strategy and governance processes to manage its cloud computing services. That audit identified nine recommendations related to data governance, cloud exit strategy, contract management plans, and decommissioning plans for legacy systems. The objective of this audit was to assess the effectiveness of security controls for the FDIC's cloud computing environment. **Appendix II** contains information about the objective, scope, and methodology for this audit.

Background

The FDIC's Multi-Cloud Environment

The FDIC began limited operations in the cloud in September 2016. In 2021, the FDIC accelerated its movement into the cloud after the White House issued Executive Order 14028, *Improving the Nation's Cybersecurity* (2021), which required the head of each agency to update existing plans to prioritize the adoption and use of cloud technology, and provide a report to OMB detailing that plan. Since then, the FDIC has been reducing its on-premises infrastructure and modernizing its Information Technology (IT) portfolio by migrating to the cloud.

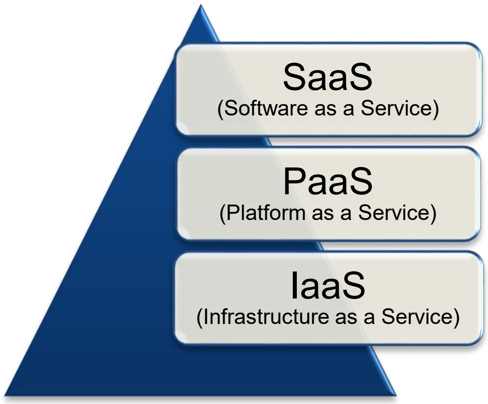
[1] NIST SP 800-145, *The NIST Definition of Cloud Computing* (September 2011).

[2] According to the FDIC Security Categorization Worksheet (March 2021), a mission essential application is defined as an application whose loss would cause a stoppage of the core operations supporting the FDIC's mission. It also defines a mission critical application as an application whose loss would produce a significant impact on the FDIC's operations, but not its core mission.

As of March 2024, the FDIC had 269 systems in operation with 115 being cloud-based (43 percent). The FDIC also had 7 major cloud platforms in use. The FDIC operates in a multi-cloud environment, procuring services from various cloud providers who provide Infrastructure as a Services (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

In a traditional on-premises implementation, web servers, application servers, and databases are physically hosted on servers directly controlled and configured by the organization. As shown in **Figure 1** below, depending on the cloud delivery model, organizations outsource different levels of responsibility to a CSP.

Figure 1: Cloud Delivery Models



Software as a Service: The CSP provides the application itself, which is used by the customer.

Platform as a Service: In addition to providing the IaaS capabilities, the CSP also builds the underlying virtual machines. The customer uses this environment to build the application logic.

Infrastructure as a Service: The CSP provides the physical infrastructure and computing resources. The customer controls the use of those resources, including deploying and configuring virtual web, application, and database servers and building applications on them.

As the FDIC continues to expand its cloud presence, costs for cloud initiatives are expected to increase. In 2023, the budget for cloud initiatives was $42.5 million. Then, in 2024, the budget for cloud initiatives grew to $47.2 million and accounted for about 9.9 percent of the Division of Information Technology (DIT) budget of $475.7 million. Most recently, in April 2024, the FDIC Board of Directors approved a multi-year investment project budget of $74.9 million to implement the Cloud Infrastructure Migration project. The FDIC's cloud-based systems are expected to grow in number and importance. By 2026, the FDIC plans to migrate all except one of its mission critical and mission essential applications to the cloud.

As shown in **Table 1**, we judgmentally selected (b) (7)(E) cloud platforms for testing based on significance and risk to the FDIC during our audit and assessed the platform-level controls that the FDIC was responsible for as a customer.[3] In addition to the (b) (7)(E) cloud platforms, we also assessed controls for the FDIC's API integration platform. We also performed penetration tests over at least one application hosted on each platform.

[3] We intended to test controls that the FDIC was responsible for as a customer. However, during our fieldwork, we identified (b) (7) findings where the controls are managed by the vendor. For those findings, (b) (7)(E) (b) (7)(E). Appendix I contains more details regarding these (b) (7) findings.

Table 1: Cloud Security Audit In-Scope Platforms: (As of March 2024)

(b) (7)(E)

* Due to the sensitive nature of the report, corresponding generic cloud platform names are shown for the cloud platform names contained in the Recommendations and related FDIC Comments, and Summary of the FDIC's Corrective Actions sections of the report.

For full details of each platform, see **Appendix III**.

Web Application Architecture

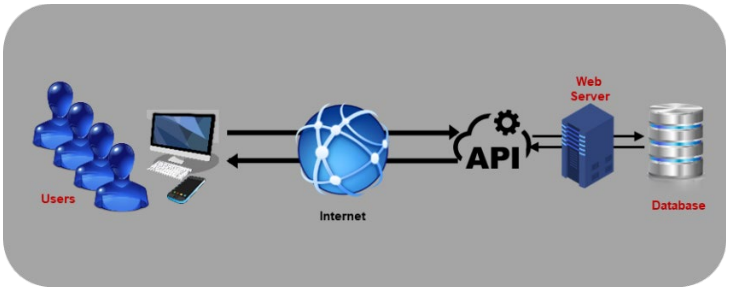
Cloud platforms constitute an alternate method to deliver system functions, most notably web applications. Web applications generally consist of these components:

1. Web servers – display application content on a user's browser.
2. Application servers – logically translate user requests into a system response.
3. Databases – hold the underlying data supporting the application.

As illustrated in **Figure 2** below, when a user accesses a web application (e.g., fdic.gov), their browser will send an Application Programming Interface (API)[4] request to the application's web server. It will then display content generated by the web server. This content may include both static content (e.g., text in the title "About the FDIC") and interactive dynamic content that responds to user actions (e.g., the search bar at the top of the site). When a user interacts with dynamic content (e.g., searches for content with the word "bank"), the browser will send additional API requests to the web server that forwards this request to the application server. The application server will perform actions based on this request, which often involves querying the database to obtain information. It retrieves this information and sends it back to the web server, which displays the response on the user's browser. In the example of searching for "bank" on fdic.gov, it would return the results from a scan of the web pages within fdic.gov.

[4] An API is a software intermediary that allows two software components to communicate with each other using a set of definitions and protocols.

Figure 2: Web Application Diagram



There are primarily two sections of this process that require code development:

1. The “front-end” controls for how the user views the application on their browser.
2. The “back-end” controls for the application logic. Specifically, it dictates how the application uses its resources (e.g., querying the database) to fulfill user requests.

The open-ended nature of application development can result in numerous vulnerabilities. A sufficiently knowledgeable and motivated attacker can use insecurely developed code to perform actions that were not intended by the developers. Therefore, organizations must securely develop code to mitigate the risk of such attacks. Organizations must also securely configure web servers, application servers, and databases in accordance with organizational policies and best practices. Further, the organization must implement administrative controls (e.g., access management and configuration management policies) to ensure secure usage.

DevSecOps (Development, Security, and Operations) and AppSec (Application Security)

To help facilitate faster code deployment, the FDIC is in the early stages of its multi-year adoption of DevSecOps (Development, Security, and Operations), a software development practice that, through automation, continuously integrates security practices throughout the entire lifecycle of software development, from design to deployment and maintenance. This integration includes the implementation of automated code scanning tools and the collaboration of developers with security teams to identify software vulnerabilities. These practices require the incorporation of security assessments throughout the continuous integration and continuous delivery (CI/CD) process.

AppSec is the process of finding, fixing, and preventing security vulnerabilities at the application level, as part of the software development processes. AppSec and DevSecOps complement each other and are not mutually exclusive. AppSec focuses on securing applications, while DevSecOps ensures that security is integrated across the development process. A dedicated AppSec team has a crucial role in ensuring the security of applications throughout their lifecycle. This team complements the role of existing security teams within DevSecOps. They are responsible for helping to define security requirements, integrating security requirements into software, monitoring checkpoints, promoting secure coding practices, and security testing and threat modeling for applications. The AppSec team helps to ensure that software vulnerabilities and security weaknesses are being identified and managed appropriately.

Roles and Responsibilities

Within the FDIC, the Chief Information Officer (CIO) has responsibility for IT governance, investments, program management, and information security. The Cloud, Infrastructure, & Platform Services Unit provides ongoing support to the FDIC's cloud services. The support for each platform is carried out by dedicated "platform teams" that are responsible for most or all of the FDIC's security settings at the cloud platform level. These platform teams are also responsible for communicating with their respective CSPs for security-related subjects.

The FDIC builds applications on these platforms, sometimes by writing code or by using the tools provided by the platform to generate code for applications. Therefore, each cloud application is generally supported by a separate application team consisting of functional personnel responsible for using the application to support FDIC business functions and technical personnel responsible for ensuring that the application operates as intended. Lastly, the FDIC maintains a security team/security operations center (SOC) that centralizes the real-time threat and incident monitoring capability across the organization, including on cloud-based systems. Each individual audit finding identified as an FDIC responsibility was primarily directed to one of three parties:

1. Platform team
2. Application team
3. Security team

Cloud Controls Assessed During the Audit

We assessed the effectiveness of the FDIC's controls to protect its cloud environments in 9 areas.[5] We identified these areas based on our analysis of relevant NIST security standards and guidance, FDIC policy and guidance, cloud CSP best practices, and government-wide security policy requirements. Note that while our intended scope was exclusive to the FDIC's responsibilities as a cloud customer, our penetration testing procedures also resulted in the identification of weaknesses where the CSP has responsibility for remediation. Additionally, due to the FDIC's varying responsibilities as a cloud customer for implementing each cloud service, our scope and procedures varied for each platform. **Table 8** in **Appendix II** contains additional information about the cloud security control areas we tested and the associated criteria.

As noted above Table 1, we performed penetration testing procedures over at least one application hosted on each in-scope cloud platform. We obtained approval from key CIOO stakeholders to conduct this testing, which was codified in a Rules of Engagement. Additionally, the CIOO created virtual desktops using Virtual Data Infrastructure (VDI) environments with a series of open-source and commercially available penetration testing tools and privileged accounts necessary to conduct testing.

We also inquired of application personnel regarding key technical and functional roles for their respective applications. Based on these discussions, we requested and were provided access to key roles within the testing environment for each application to validate effective security controls from

[5] See **Appendix II**. We also assessed the effectiveness of 13 internal control principles as described in **Table 7** in **Appendix II** and defined in GAO's *Standards for Internal Control in the Federal Government* (the Green Book) (September 2014) that we deemed significant to the audit objective and relevant to the 9 control areas we tested.

multiple user perspectives. Our findings reflect the observations we identified using this tailored and privileged access.

Audit Objective

The objective of this performance audit was to assess the effectiveness of security controls for the FDIC's cloud computing environment.

Audit Results

Although we found that the FDIC had effective controls in four of nine security control areas assessed, we determined that the FDIC had not effectively implemented security controls in its cloud computing environment in five areas, such as identity and access management and protecting cloud secrets. Specifically, we identified 26 cloud security findings (b) (7)(E) cloud computing platforms, applications, and API platform we assessed during this audit. We noted that a contributing cause for these security findings was that the FDIC does not have (b) (7)(E). These findings pose risks (b) (7)(E) We provide seven recommendations related to the identified control deficiencies and security weaknesses that, if effectively addressed by management, should strengthen the FDIC's security controls for its cloud computing services.

Cloud Security Findings – Implementation of Security Controls

We determined that the FDIC had not effectively implemented security controls in its cloud computing environment for five of the nine security control areas we assessed.[6] Specifically, we found that the FDIC should improve controls in the following areas:

1. Identity and Access Management
2. Protecting Cloud Secrets
3. Patch Management
4. Flaw Remediation
5. Audit Logging

We found that the FDIC had effective controls in the remaining four control areas we assessed in the following areas: change management, cloud-based system inventory management, cloud authorization, and minimizing shadow-IT.[7]

[6] See Table 8 of Appendix II for a detailed description of the nine security control areas assessed.

[7] Shadow IT is any software, hardware or information technology (IT) resource used on an enterprise network without the IT department's approval, knowledge or oversight.

Cloud Security Findings – All In-Scope Platforms and Applications

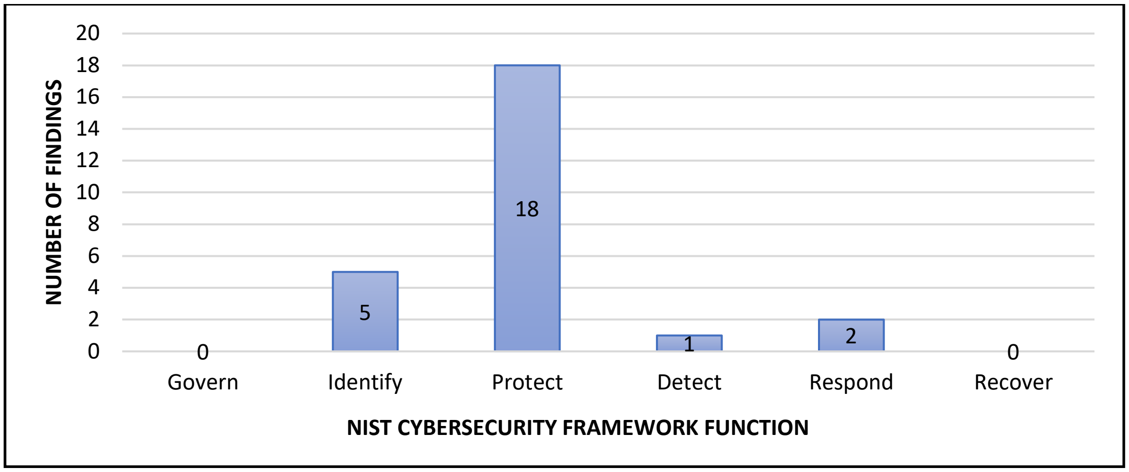
As noted above, we identified a total of 26 cloud security findings. The full details of each finding are in **Appendix I**. Due to the number of findings and commonalities among them, we identified six common themes of security weaknesses listed below and mapped them to the nine security control areas that were tested:

1. **Insecure Coding Practices**: The FDIC teams developing cloud platforms did not consistently implement secure coding practices. (b) (7)(E)
2. **Misconfigured Security Settings**: The FDIC platform teams did not consistently configure their cloud platform security settings in accordance with CSP and industry best practices. (b) (7)(E)
3. **Least Privilege**: The FDIC did not consistently provision access to its cloud-based systems in accordance with least privilege. (b) (7)(E)
4. **Outdated Software**: (b) (7)(E) cloud platforms rely on outdated software components. (b) (7)(E)
5. **Ineffective Monitoring:** The FDIC is not adequately monitoring the activity on its cloud-based systems. (b) (7)(E)
6. **Cloud Service Provider Vulnerabilities:** The CSPs were solely responsible for causing certain vulnerabilities (code injection, outdated libraries, and non-expiration of session cookies) and should be responsible for their remediation.

For many of the security weaknesses comprising all six themes above, we were able to develop a proof-of-concept demonstrating that a malicious user could leverage these weaknesses to cause harm to FDIC systems or data. These proof-of-concept exploits ranged in impact level from low to high. (b) (7)(E) However, the CIOO informed us that they did not identify any prior instances where any of the weaknesses identified within the themes above were exploited to compromise FDIC systems and data.

We also mapped the 26 cloud security findings identified to the NIST Cybersecurity Framework (CSF) 2.0 functions (Govern, Identify, Protect, Detect, Respond, and Recover) to understand how the findings impacted the FDIC. The NIST CSF was designed to help organizations of all sizes and sectors manage and reduce their cybersecurity risks. The Framework is used to provide a consistent approach for evaluating cybersecurity risks. The majority of the 26 findings were aligned to the Identify and Protect functions where weaknesses related to identity and access, vulnerability, and configuration management were identified. Please refer to **Figure 3** below for further details:

Figure 3: Cloud Security Findings Compared to NIST Cybersecurity Framework Functions



Note: The scope of this audit did not include testing related to the Govern and Recover functions.

The following describes each of the six common themes of security weaknesses that encompass the 26 cloud security findings.

Theme 1: Insecure Coding Practices

We found that the FDIC development teams did not consistently follow secure coding practices for (b) (7)(E) [redacted] cloud web applications that were tested where the FDIC had code development responsibilities. Specifically, we noted (b) (7)(E) [redacted].

The open-ended nature of web application development and the variety of application functions leave applications susceptible to a variety of vulnerabilities. Generally, the more complex an application, the more potential for unintended behavior that can be exploited by an attacker. Mitigating the risk requires the adoption of secure coding standards. According to NIST SP 800-218, *Secure Software Development Framework*, organizations should produce well-secured software with minimal security vulnerabilities in their releases.

We assessed the in-scope applications for susceptibility to the most common attacks, many of which are documented within the Top 10 Web Application Security Risks by the Open Worldwide Application Security Project (OWASP), which is a globally recognized standard for secure web development representing the most critical security risks for web applications. We identified vulnerabilities related to the following types of common attacks resulting from insecure coding practices:

(b) (7)(E) [redacted]

(b) (7)(E)

(b) (7)(E)

We identified (b) (7)(E) findings related to insecure coding practices. Full details are documented in Appendix I.

(b) (7)(E)

* We have provided reference numbers for each finding in Appendix I based on the platform or application that they are associated with. The reference schema is: (b) (7)(E)

These weaknesses resulted fro (b) (7)(E)

In addition, the FDIC does not have (b) (7)(E) appropriately. The overall cause identified for Theme 1 – Insecure Coding Practices is addressed by recommendation 6 below, and the detailed findings, causes, and related

[8] (b) (7)(E)

recommendations for this theme are outlined in **Appendix I** below and are addressed by recommendations 1-5 listed below.

A malicious actor could exploit the insecure coding practices identified (b) (7)(E) to compromise the application.

Theme 2: Misconfigured Security Settings

We found that the FDIC teams responsible for securing FDIC cloud platforms and applications did not consistently follow CSP and/or general best practices for configuring security settings. CSPs provide customers the ability to tailor security settings based on their risk appetite and business needs. However, CSPs and configuration baseline authorities, such as the Center for Internet Security (CIS), provide best practices for configurations of information systems that should be adopted by customers unless there are organization-specific justifications. NIST SP 800-128, *Guide for Security-Focused Configuration Management*, states that Common Secure Configurations identify commonly recognized and standardized secure configurations to be applied to configuration items. Agencies may have deviations from the baseline due to mission requirements or other constraints; however, they must be controlled through approvals, justifications, and compensating controls.

We identified (b) (7)(E) findings where FDIC personnel configured their cloud-based systems in an insecure manner with no business justification. Full details are documented in **Appendix I**.

(b) (7)(E)

These findings resulted from (b) (7)(E) Further, as discussed above, the FDIC does not have (b) (7)(E) The overall causes identified for Theme 2 – Misconfigured Security Settings are addressed by recommendation 6 below, and the detailed findings, causes, and related recommendations for this theme are outlined in **Appendix I** below and are addressed by recommendations 1-5 listed below.

A malicious actor could exploit the misconfigured security settings of FDIC cloud-based systems to (b) (7)(E)

Theme 3: Least Privilege Violations

We found that the FDIC did not consistently grant access to cloud-based systems in accordance with the least privilege principle. NIST defines least privilege as the principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. Although the customer is directly responsible for fewer security controls in a cloud environment, it still bears the responsibility for ensuring that its personnel only have the system access required for their job function (i.e., least privilege). NIST SP 800-53, Revision 5, AC-6, *Least Privilege*, requires organizations to provision access in accordance with this principle.

Within the context of a web application, system roles define the interactions that a user is allowed to make with the application resources. Users are intended to interact with the application via a browser user interface. Depending on the roles that users have, they will see different options on their browser.

We assessed the application of the least privilege principle by determining if:

1. System roles were appropriately designed and supported the job function they were meant for and did not include additional permissions, and
2. System roles, as implemented in the system, did not provide system access beyond their design.

We identified (b) (7)(E) findings related to least privilege. Full details are documented in **Appendix I**.

(b) (7)(E)

(b) (7)(E) the FDIC applied user roles by restricting the functions available to a user when interacting with the application through a web browser (b) (7)(E) In theory, a user could only interact with the application through the methods allowed through a browser (b) (7)(E) we were able to perform actions that exceeded role-based limitations. (b) (7)(E) was caused by the (b) (7)(E)

As previously indicated, the FDIC does not have (b) (7)(E) The overall causes identified for Theme 3 – Least Privilege Violations are addressed by recommendation 6 below, and the detailed findings, causes, and related recommendations for this theme are outlined in **Appendix I** below and are addressed by recommendations 1-5 listed below.

The existence of these excessive privileges results in users, in some cases (b) (7)(E) For example, we noted instances where (b) (7)(E)

Theme 4: Outdated Software Versions

We found that the FDIC is running outdated versions of software supporting cloud-based systems. Cloud applications require the integration of multiple software components, many developed by third-party CSPs. These CSPs release updated versions of these components to provide additional functionality, incorporate technological advances, and improve security. As a customer, the FDIC is required by NIST criteria to install security-relevant software updates in a timely manner. Specifically, NIST SP 800-53, Revision 5, SA-22, *Unsupported System Components* states that organizations should replace system components when support for the components is no longer available from the developer, vendor, or manufacturer. Additionally, NIST SP 800-53, Revision 5, SI-2, *Flaw Remediation* states that organizations should install security-relevant software and firmware updates within an organization-defined period of the release of the updates. The FDIC's organization-defined period is documented in the *CIOO Patch Management Policy,* which requires a patch to be applied or Plan of Actions and Milestones (POA&M)[9] to be created within (b) (7)(E) (critical/high/moderate) days.

We identified (b) (7)(E) findings related to the FDIC's use of outdated software versions. Full details are documented in **Appendix I**.

(b) (7)(E)

These findings were caused by (b) (7)(E)

[9] According to NIST SP 800-37 Revision 2, a POA&M describes the actions that are planned to correct deficiencies in the controls identified during the assessment of the controls and during continuous monitoring.

(b) (7)(E) Furthermore, the FDIC does not have (b) (7)(E) The overall causes identified for Theme 4 – Outdated Software Versions are addressed by recommendation 6 below, and the detailed findings, causes, and related recommendations for this theme are outlined in **Appendix I** below and are addressed by recommendations 1-5 listed below.

Using outdated software versions leaves the FDIC more susceptible to a large variety of security vulnerabilities and performance degradation, potentially culminating in the complete loss of application function. For example, we (b) (7)(E) For another example, (b) (7)(E)

Theme 5: Ineffective Monitoring

FDIC personnel, agents from external financial institutions and regulators, and the public interact with FDIC cloud-based systems as part of the FDIC's mission. Although almost all of this activity is legitimate, there is a risk of malicious actors performing unscrupulous actions. Therefore, relevant personnel within the FDIC, including the platform teams, are responsible for monitoring their environments for suspicious activity. NIST SP 800-53, *Control AU-6 Audit Record Review, Analysis, and Reporting* states that organizations should review and analyze system audit records at an organization-defined frequency for indications of inappropriate or unusual activity and their potential impact. Organizations should also report findings to relevant personnel.

We identified (b) (7)(E) findings related to ineffective monitoring. Full details are documented in **Appendix I**.

(b) (7)(E)

The insufficient frequency of (b) (7)(E) audit log reviews (b) (7)(E) resulted from (b) (7)(E)

(b) (7)(E) As mentioned above, the FDIC does not have (b) (7)(E) The overall causes identified for Theme 5 – Ineffective Monitoring are addressed by recommendation 6 below, and the detailed findings, causes, and related recommendations for this theme are outlined in **Appendix I** below and are addressed by recommendations 1-5 listed below.

(b) (7)(E)

(b) (7)(E)

The security of the FDIC's data relies on identifying malicious activity in a timely manner and responding accordingly. (b) (7)(E)

The (b) (7)(E) finding related to vulnerability scans that detected (b) (7)(E) vulnerabilities (b) (7)(E) Many of these vulnerabilities resulted from (b) (7)(E) FDIC policy states that critical vulnerabilities with exploits must be remediated within (b) (7)(E) days of identification. Similar to the findings above, these exploits can pose significant risk to the FDIC's data.

Theme 6: Cloud Service Provider Vulnerabilities

Our testing identified (b) (7)(E) findings that affected the security of the FDIC's cloud implementations where the CSP has a responsibility for remediation. The CSPs have a responsibility to remediate the vulnerabilities in these identified instances because they have ownership and access to the underlying code supporting these platforms and applications. Full details are documented in **Appendix I**.

(b) (7)(E)

The findings listed above are the responsibility of the CSP to remediate (except for (b) (7)(E) 02 and (b) (7)(E) 03[10] where there is a shared responsibility between the FDIC and (b) (7)(E) for full remediation), and the FDIC does not have access to the underlying source code or associated vendor processes. Therefore, we were not able to determine the cause of these findings.

The impact of these CSP findings could result in harm to FDIC systems and data. (b) (7)(E)

[10] In January 2024, subsequent to our testing conducted in September 2023, the FDIC (b) (7)(E)

While we were unable to exploit the (b) (7)(E) to obtain any information that we could not obtain legitimately, this observation represents unintended behavior that should be remediated.

We determined that the FDIC is unable to take any further mitigation actions as a customer for the (b) (7)(E) As a result of our observation, FDIC developers have implemented this corresponding validation. Additionally, we have reported this observation to the Cybersecurity & Infrastructure Security Agency (CISA) for the awareness of the Federal community. CISA stated that it will not take any further action on this issue as (b) (7)(E) believes this observation is a customer issue and, in accordance with CISA Common Vulnerabilities and Exposures (CVE) Program policy, did not pursue assigning a CVE Identifier (or CVE ID).

Recommendations

We recommend that the **CIOO**:[11]

1. Remediate the 7 findings and 19 associated recommendations identified in Cloud Platform #1 and the applications built on Cloud Platform #1.
2. Remediate the 8 findings and 11 associated recommendations identified in Cloud Platform #2 and the applications built on Cloud Platform #2.
3. Remediate the 4 findings and 5 associated recommendations identified in the applications built on Cloud Platform #3.
4. Remediate the 3 findings and 6 associated recommendations identified in Cloud Platform #4.
5. Remediate the 4 findings and 7 associated recommendations identified in Cloud Platform #5.

As noted in our audit results, the FDIC's cloud platform and application teams were susceptible to similar vulnerabilities resulting from (b) (7)(E) Although remediating the individual weaknesses is important, we tested a small subset of FDIC cloud-based systems representing the FDIC's cloud-based system population. Similar vulnerabilities may exist within the other FDIC cloud-based systems that were not within the scope of this audit that could result in (b) (7)(E)

In addition to the detailed recommendations for each cloud platform, we identified overarching recommendations to help mitigate and address the security risks identified in this audit for all FDIC cloud-based systems. Specifically, we recommend that the **CIOO**:

[11] Due to the sensitive nature of the report, generic names are shown in place of the cloud platform names contained in the Recommendations and the related FDIC Comments and Summary of Corrective Actions sections of the report. (b) (7)(E)

6. (b) (7)(E)

7. Design and implement a plan to prevent, detect, and remediate security weaknesses on FDIC cloud platforms and applications related to insecure coding practices, misconfigured security settings, least privilege violations, outdated software versions, and ineffective monitoring.

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

[redacted]

(b) (7)(E)

(b) (7)(E)

[redacted]

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

Appendix II – Objective, Scope, and Methodology

The objective of this performance audit was to assess the effectiveness of security controls for the FDIC's cloud computing environment. Sikich conducted the audit in accordance with *Generally Accepted Government Auditing Standards* (GAGAS) (2018 revision).[12] These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We assessed the effectiveness of internal controls that we deemed significant to the audit objective. Specifically, we assessed 13 of the 17 internal control principles defined in GAO's *Standards for Internal Control in the Federal Government* (the Green Book) (September 2014).[13] **Table 7** summarizes the principles we assessed.

Table 7: Internal Control Principles Assessed

Control Environment
Principle 2 – Exercise Oversight Responsibility
Principle 3 – Establish Structure, Responsibility, and Authority
Principle 4 – Demonstrate Commitment to Competence
Risk Assessment
Principle 6 – Define Objectives and Risk Tolerances
Principle 7 – Identify, Analyze, and Respond to Risks
Principle 8 – Assess Fraud Risk
Principle 9 – Identify, Analyze, and Respond to Change
Control Activities
Principle 10 – Design Control Activities
Principle 11 – Design of Activities for the Information System
Principle 12 – Implement Control Activities
Information and Communication
Principle 14 – Communicate Internally
Principle 15 – Communicate Externally
Monitoring
Principle 16 – Perform Monitoring

Source: Sikich analysis of the Green Book and work performed on this audit.

The report presents the internal control deficiencies we identified. Because our audit was limited to the 13 principles presented above, it may not have disclosed certain internal control deficiencies that may have existed at the time of the audit.

[12] Sikich began this performance audit in September 2022. The 2018 revision of GAGAS became effective for performance audits beginning on or after July 1, 2019.

[13] The Green Book organizes internal control through a hierarchical structure of 5 components and 17 principles. The five components, which represent the highest level of the hierarchy, consist of the Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. The 17 principles support the effective design, implementation, and operation of the components, and represent the requirements for establishing an effective internal control system.

We assessed the effectiveness of nine security control areas for the FDIC's cloud computing environment covered by NIST Special Publications and industry best practices. See **Table 8** for the control areas.

Table 8: Description of Assessed Security Control Areas

Selected Control Areas	Definition
1. **Identity and Access Management**: The FDIC has appropriately defined and assigned roles for cloud platforms and applications. Additionally, the FDIC has defined user account identities necessary to access cloud platforms and applications.	NIST SP 800-53 Rev. 5 Control AC-1, *Policy and Procedures*, requires agencies to develop and document access control policies and procedures to address purpose, scope, roles, and responsibilities. Additionally, the policies and procedures should be updated at a defined frequency and after key events. NIST SP 800-53 Rev. 4 Control AC-6, *Least Privilege*, requires agencies to employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks. NIST 800-63-3 *Digital Identity Guidelines*, states that digital authentication is the process of determining the validity of one or more authenticators used to claim a digital identity. Additionally, it states that the use of digital identity presents a technical challenge because this process often involves proofing individuals over an open network, and typically involves the authentication of individual subjects over an open network to access digital government services. There are multiple opportunities for impersonation and other attacks that fraudulently claim another subject's digital identity.
2. **Cloud Inventory Management**: The FDIC maintains an accurate inventory of its cloud assets and applications.	NIST SP 800-53 Rev. 5 Control CM-8, *System Component Inventory*, requires agencies to develop and document an inventory of system components that accurately reflects the system, includes all components within the system, does not include duplicate accounting of components or components assigned to any other system, and is at the level of granularity deemed necessary for tracking and reporting.
3. **Cloud Authorization**: The FDIC appropriately authorized its cloud implementation based on the cloud CSP's product.	NIST SP 800-53 Rev. 5 Control CA-3 *Information Exchange* requires agencies to approve and manage the exchange of information between the system and other systems. Additionally, NIST SP 800-53 Rev. 5 Control CA-3 *Authorization* requires the organization to authorize the system to operate prior to commencing operations.
4. **Protecting Cloud Secrets**: The FDIC is able to configure its cloud platforms and applications to protect cloud secrets. This includes encrypting its sensitive data on cloud platforms in transit and at rest.	NIST SP 800-128, *Guide for Security-Focused Configuration Management*, states that Common Secure Configurations identify commonly recognized and standardized secure configurations to be applied to configuration items. Agencies may have deviations from the baseline due to mission requirements or other constraints. However, they must be controlled through approvals, justifications, and compensating controls. NIST SP 800-218, *Secure Software Development Framework (SSDF)*, states that organizations should produce well-secured software with minimal security vulnerabilities in its releases. Additionally, OWASP defines common vulnerabilities endemic to web development, including injection attacks, cross-site scripting, and cross-site request forgery. NIST SP 800-53 Rev. 5 Control SC-28, *Protection of Information at Rest*, requires agencies to protect the confidentiality and integrity of information at rest. Additionally, Control SC-8 *Transmission Confidentiality and Integrity* requires organizations to protect the confidentiality and integrity of transmitted information.

5. **Change Management**: The FDIC ensures that changes in cloud environments are approved prior to implementation.	NIST SP 800-53 Rev. 5 Control CM-3, *Configuration Change Control*, states that organizations need to define the types of changes to the system that should be subject to configuration control and document, test, and approve those changes with explicit consideration for security and privacy impact.
6. **Patch Management**: The FDIC is patching its cloud platforms in a timely manner.	NIST SP 800-40, *Guide to Enterprise Patch Management Technologies*, defines Patch Management as the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they are mitigating software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation.
7. **Flaw Remediation**: The FDIC, as applicable, performs vulnerability scans on its cloud platforms and applications and remediates them in a timely manner.	NIST SP 800-53 Rev. 5 Control RA-5, *Vulnerability Monitoring and Scanning*, states that agencies should scan for vulnerabilities at a defined frequency, analyze scan reports, and remediate vulnerabilities within a defined timeframe.
8. **Audit Logging**: The FDIC has identified suspicious events relevant to its cloud platforms and applications. Additionally, the FDIC appropriately reviews and follows up on audit log reports.	NIST SP 800-53, Rev. 5 Controls AU-2 *Event Logging*, AU-3 Content of Audit Records, and AU-6 *Audit Record Review, Analysis, and Reporting* cumulatively state that organizations should define activity they deem to be of interest, develop capabilities that log such activity, and review, analyze, and respond to incidences of the activity.
9. **Shadow-IT**: The FDIC prevents the use of unsanctioned cloud services and is able to track its usage of cloud services.	NIST 800-124 Rev. 2 *Guidelines for Management the Security of Mobile Devices in the Enterprise*, denotes Shadow-IT as staff members' work-related use of IT-related hardware, software, or cloud services without the approval, oversight, or even knowledge of the organization's IT.

Source: Sikich scoping of the audit.

We selected these nine areas because a control failure in these areas could impair the FDIC's ability to ensure the confidentiality, integrity, and availability of sensitive FDIC data on cloud platforms. Such a failure could also impair the FDIC's ability to support its business operations and communications.

We assessed the design, implementation, and operating effectiveness of selected controls within each of the nine security control areas by:

- Assessing the extent to which FDIC policies, procedures, and guidance related to these controls aligned with NIST and government-wide security policy and guidance.
- Performing inquiries of CIOO personnel responsible for maintaining the cloud platforms at the FDIC.
- Performing inquiries of CIOO personnel responsible for maintaining a subset of applications hosted on the cloud platforms.
- Performing penetration testing procedures to identify common vulnerabilities on at least one application hosted on each platform. The procedures primarily consisted of manual analysis supported by open-source software and commercially available software such as Burp Suite Pro. We performed the following procedures:

    (b)(7)(E)

    [redacted]

    [redacted]

(b) (7)(E) [redacted]

- Assessing configuration settings on each cloud platform.
- Reviewing relevant controls and responsibilities within FedRAMP packages of each cloud platform.
- Reviewing FDIC authorization packages for relevant platforms and applications.
- Reviewing policies and procedures, including Role-Based Access Control documents, access control policies, configuration management plans, and system descriptions.
- Obtaining relevant system output for each platform/application, such as audit logs, patch notes, change tickets, and user listings.

We obtained approval from key CIOO stakeholders to conduct this testing, which was codified in a Rules of Engagement prior to performing penetration testing procedures over in-scope cloud platforms and applications. Additionally, the CIOO created virtual desktops using Virtual Data Infrastructure (VDI) environments with a series of open-source and commercially available penetration testing tools and privileged accounts necessary to conduct testing. We also inquired of application personnel regarding key technical and functional roles for their respective applications. Based on these discussions, we requested and were provided access to key roles within the testing environment for each application to validate effective security controls from multiple user perspectives.

We used NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations* (September 2020), as the primary criteria for determining whether the FDIC had established and implemented effective controls to secure and manage its cloud computing services. We also used NIST SP 800-53, Rev. 4 (April 2013) where applicable because the FedRAMP control baselines are still based on the older SP while transitioning to Rev. 5. We supplemented NIST SP 800-53 with other SPs including, NIST SP 800-63-3, *Digital Identity Guidelines* (June 2017); NIST SP 800-92, *Guide to Computer Security Log Management* (September 2006); NIST SP 800-128*, Guide for Security-Focused Configuration Management* (October 2019); NIST SP 800-123, *Guide to General Server Security* (July 2008); and NIST SP 800-218, *Secure Software Development Framework* (SSDF) (February 2022). We also reviewed best practices from Federal Information Processing Standards Publication 140-3, *Cryptographic Module Validation Program* (March 2019).

To support our knowledge of publicly available findings, we used the Common Vulnerabilities and Exposures (CVE) system, maintained by the US National Cybersecurity Federally Funded Research and Development Center (FFRDC). Additionally, we reviewed guidelines from non-profit organizations such as the Center for Internet Security (CIS), which develops security benchmarks for software platforms, and the Open Worldwide Application Security Project (OWASP), which publishes articles describing common web application vulnerabilities. Lastly, we reviewed best practices published online by the cloud CSPs – (b) (7)(E) [redacted]

We discussed our preliminary findings and conclusions with representatives of FDIC management throughout the audit.

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Office of Inspector General

Audit of Security Controls for the FDIC’s Cloud Computing Environment

Part II

****

FDIC Comments and OIG Evaluation

September 2024 | AUD-24-01

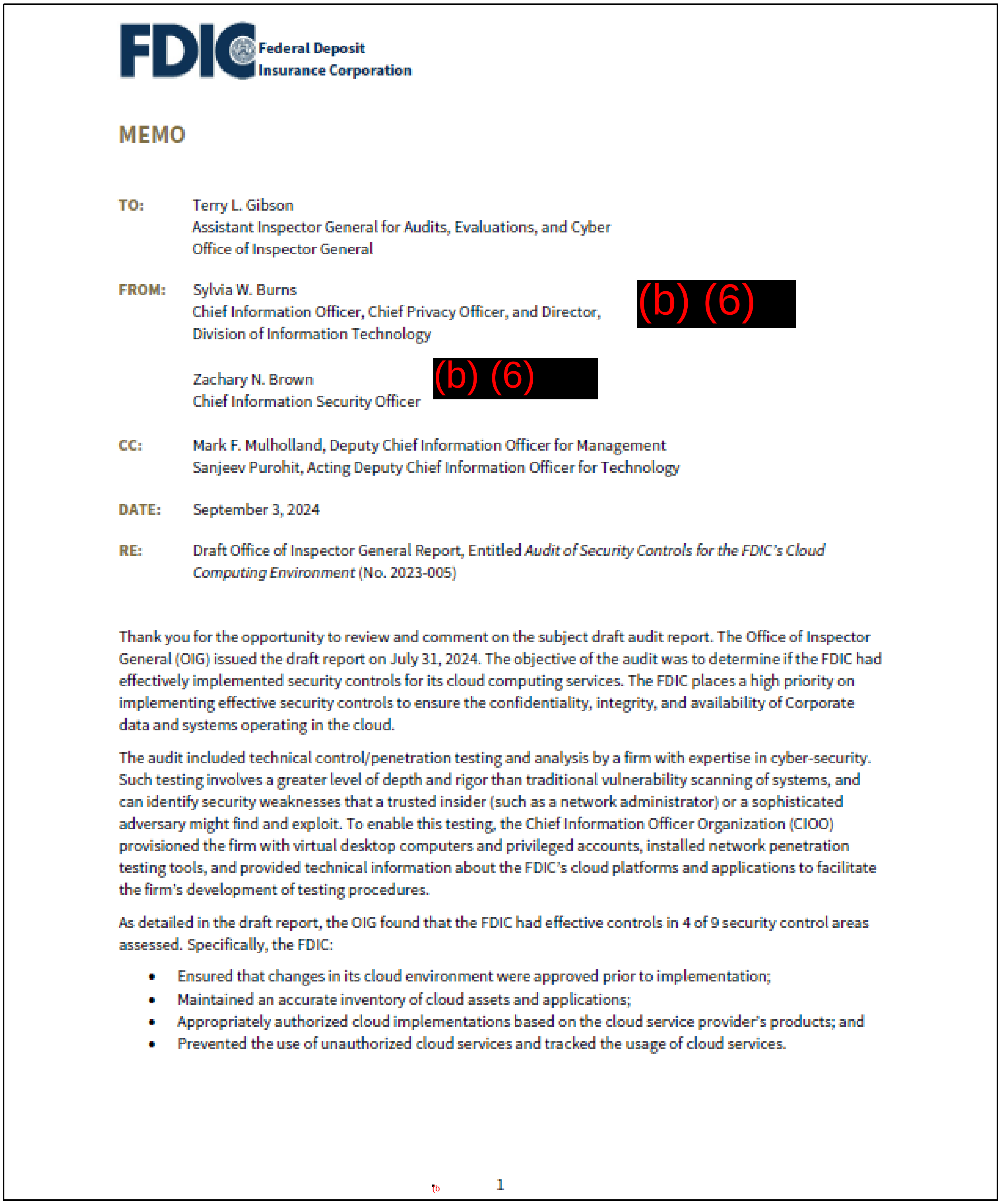
FDIC COMMENTS AND OIG EVALUATION

On September 3, 2024, the FDIC Chief Information Officer (CIO) and Chief Information Security Officer (CISO) provided a written response to a draft of this report, which is presented in its entirety on page II-2.

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

The recommendations in this report will remain open until we confirm that corrective actions have been completed and the actions are responsive. A summary of the FDIC's corrective actions is contained on page II-3.

APPENDIX 1: FDIC COMMENTS



FDIC Federal Deposit Insurance Corporation

MEMO

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

FROM: Sylvia W. Burns (b) (6)
Chief Information Officer, Chief Privacy Officer, and Director,
Division of Information Technology

Zachary N. Brown (b) (6)
Chief Information Security Officer

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

DATE: September 3, 2024

RE: Draft Office of Inspector General Report, Entitled *Audit of Security Controls for the FDIC's Cloud Computing Environment* (No. 2023-005)

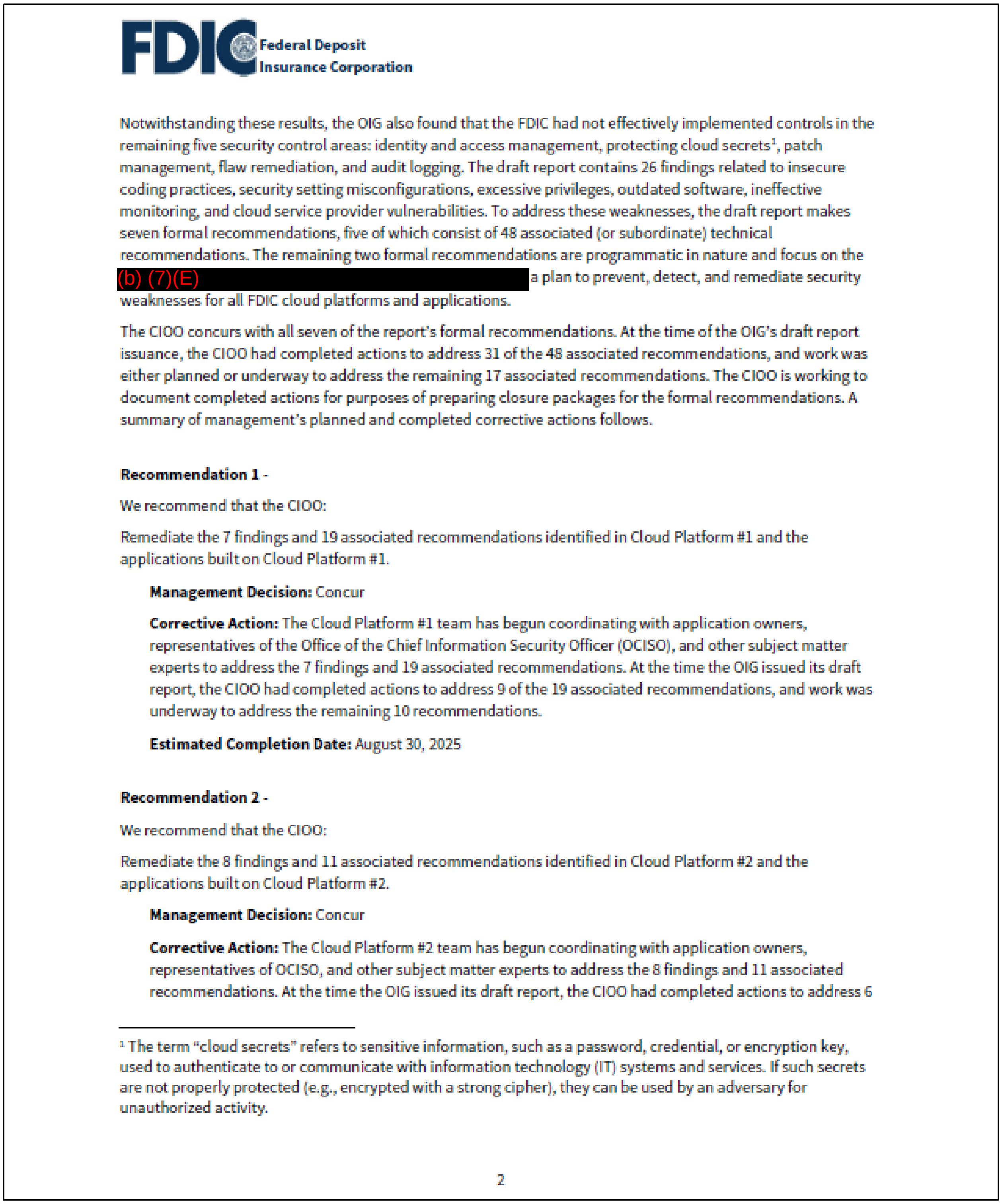
Thank you for the opportunity to review and comment on the subject draft audit report. The Office of Inspector General (OIG) issued the draft report on July 31, 2024. The objective of the audit was to determine if the FDIC had effectively implemented security controls for its cloud computing services. The FDIC places a high priority on implementing effective security controls to ensure the confidentiality, integrity, and availability of Corporate data and systems operating in the cloud.

The audit included technical control/penetration testing and analysis by a firm with expertise in cyber-security. Such testing involves a greater level of depth and rigor than traditional vulnerability scanning of systems, and can identify security weaknesses that a trusted insider (such as a network administrator) or a sophisticated adversary might find and exploit. To enable this testing, the Chief Information Officer Organization (CIOO) provisioned the firm with virtual desktop computers and privileged accounts, installed network penetration testing tools, and provided technical information about the FDIC's cloud platforms and applications to facilitate the firm's development of testing procedures.

As detailed in the draft report, the OIG found that the FDIC had effective controls in 4 of 9 security control areas assessed. Specifically, the FDIC:

- Ensured that changes in its cloud environment were approved prior to implementation;
- Maintained an accurate inventory of cloud assets and applications;
- Appropriately authorized cloud implementations based on the cloud service provider's products; and
- Prevented the use of unauthorized cloud services and tracked the usage of cloud services.

1



Notwithstanding these results, the OIG also found that the FDIC had not effectively implemented controls in the remaining five security control areas: identity and access management, protecting cloud secrets[1], patch management, flaw remediation, and audit logging. The draft report contains 26 findings related to insecure coding practices, security setting misconfigurations, excessive privileges, outdated software, ineffective monitoring, and cloud service provider vulnerabilities. To address these weaknesses, the draft report makes seven formal recommendations, five of which consist of 48 associated (or subordinate) technical recommendations. The remaining two formal recommendations are programmatic in nature and focus on the (b) (7)(E) a plan to prevent, detect, and remediate security weaknesses for all FDIC cloud platforms and applications.

The CIOO concurs with all seven of the report's formal recommendations. At the time of the OIG's draft report issuance, the CIOO had completed actions to address 31 of the 48 associated recommendations, and work was either planned or underway to address the remaining 17 associated recommendations. The CIOO is working to document completed actions for purposes of preparing closure packages for the formal recommendations. A summary of management's planned and completed corrective actions follows.

Recommendation 1 -

We recommend that the CIOO:

Remediate the 7 findings and 19 associated recommendations identified in Cloud Platform #1 and the applications built on Cloud Platform #1.

Management Decision: Concur

Corrective Action: The Cloud Platform #1 team has begun coordinating with application owners, representatives of the Office of the Chief Information Security Officer (OCISO), and other subject matter experts to address the 7 findings and 19 associated recommendations. At the time the OIG issued its draft report, the CIOO had completed actions to address 9 of the 19 associated recommendations, and work was underway to address the remaining 10 recommendations.

Estimated Completion Date: August 30, 2025

Recommendation 2 -

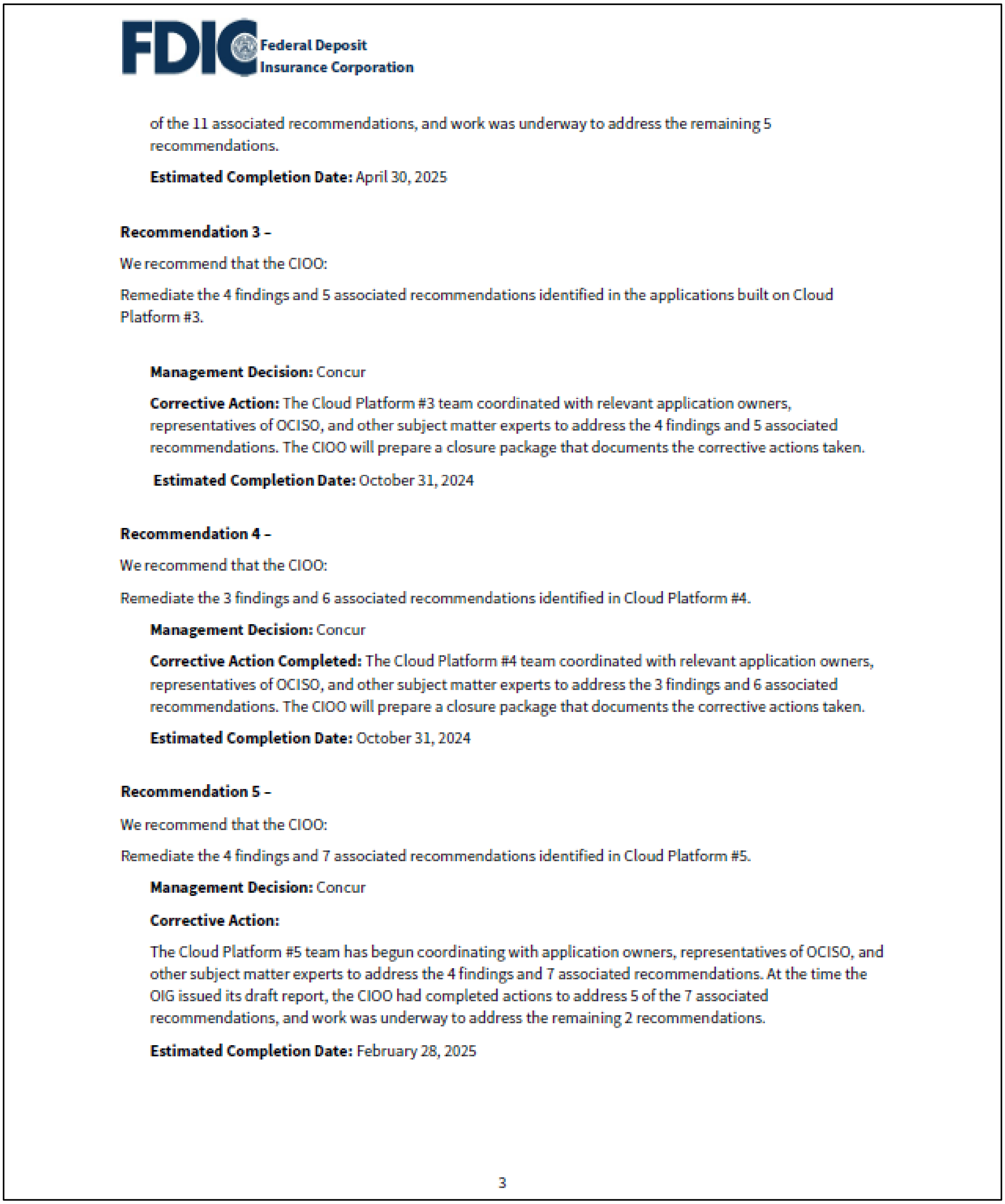
We recommend that the CIOO:

Remediate the 8 findings and 11 associated recommendations identified in Cloud Platform #2 and the applications built on Cloud Platform #2.

Management Decision: Concur

Corrective Action: The Cloud Platform #2 team has begun coordinating with application owners, representatives of OCISO, and other subject matter experts to address the 8 findings and 11 associated recommendations. At the time the OIG issued its draft report, the CIOO had completed actions to address 6

[1] The term "cloud secrets" refers to sensitive information, such as a password, credential, or encryption key, used to authenticate to or communicate with information technology (IT) systems and services. If such secrets are not properly protected (e.g., encrypted with a strong cipher), they can be used by an adversary for unauthorized activity.



of the 11 associated recommendations, and work was underway to address the remaining 5 recommendations.

Estimated Completion Date: April 30, 2025

Recommendation 3 –

We recommend that the CIOO:

Remediate the 4 findings and 5 associated recommendations identified in the applications built on Cloud Platform #3.

Management Decision: Concur

Corrective Action: The Cloud Platform #3 team coordinated with relevant application owners, representatives of OCISO, and other subject matter experts to address the 4 findings and 5 associated recommendations. The CIOO will prepare a closure package that documents the corrective actions taken.

Estimated Completion Date: October 31, 2024

Recommendation 4 –

We recommend that the CIOO:

Remediate the 3 findings and 6 associated recommendations identified in Cloud Platform #4.

Management Decision: Concur

Corrective Action Completed: The Cloud Platform #4 team coordinated with relevant application owners, representatives of OCISO, and other subject matter experts to address the 3 findings and 6 associated recommendations. The CIOO will prepare a closure package that documents the corrective actions taken.

Estimated Completion Date: October 31, 2024

Recommendation 5 –

We recommend that the CIOO:

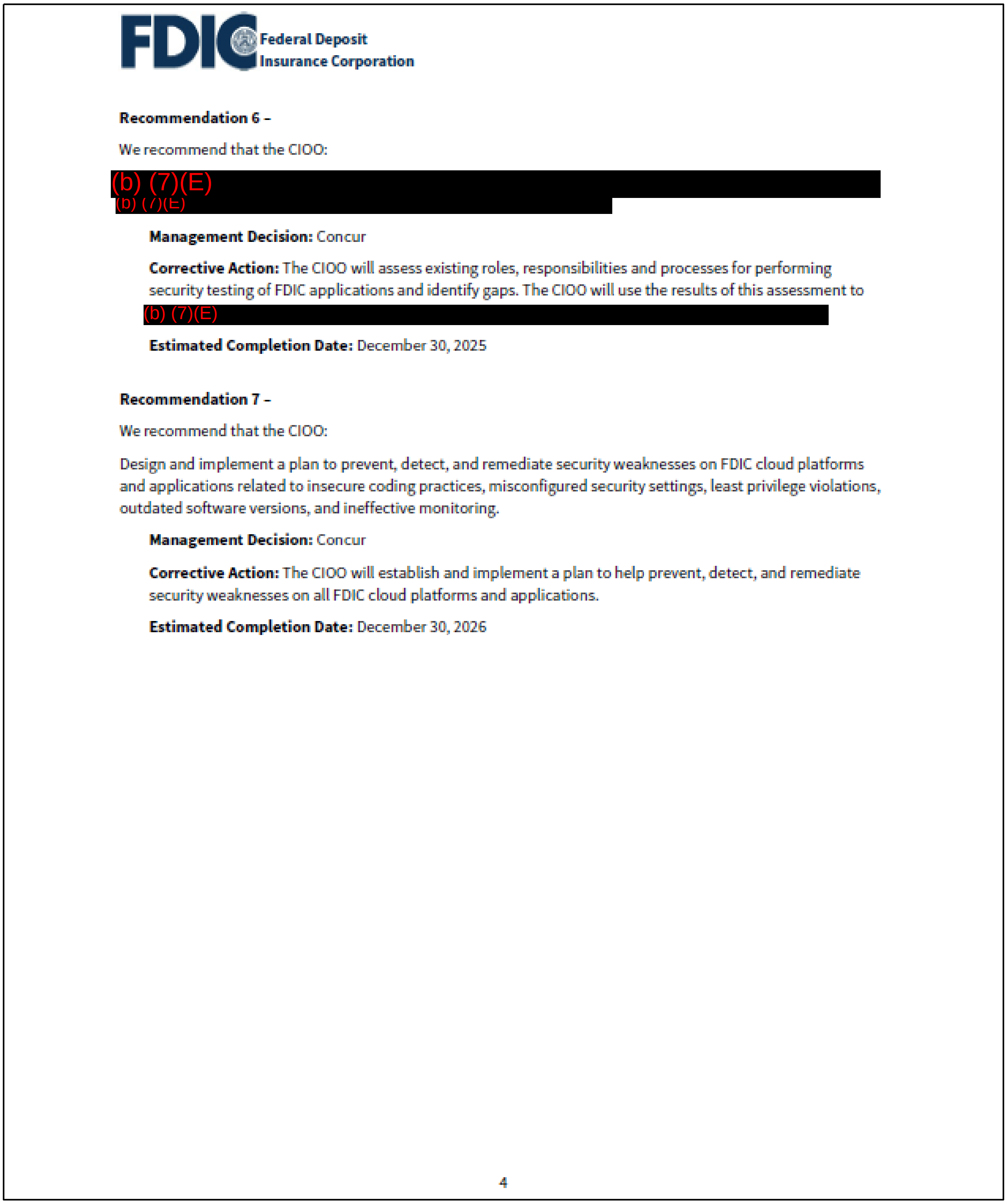
Remediate the 4 findings and 7 associated recommendations identified in Cloud Platform #5.

Management Decision: Concur

Corrective Action:

The Cloud Platform #5 team has begun coordinating with application owners, representatives of OCISO, and other subject matter experts to address the 4 findings and 7 associated recommendations. At the time the OIG issued its draft report, the CIOO had completed actions to address 5 of the 7 associated recommendations, and work was underway to address the remaining 2 recommendations.

Estimated Completion Date: February 28, 2025



FDIC Federal Deposit Insurance Corporation

Recommendation 6 –

We recommend that the CIOO:

(b) (7)(E)
(b) (7)(E)

Management Decision: Concur

Corrective Action: The CIOO will assess existing roles, responsibilities and processes for performing security testing of FDIC applications and identify gaps. The CIOO will use the results of this assessment to (b) (7)(E)

Estimated Completion Date: December 30, 2025

Recommendation 7 –

We recommend that the CIOO:

Design and implement a plan to prevent, detect, and remediate security weaknesses on FDIC cloud platforms and applications related to insecure coding practices, misconfigured security settings, least privilege violations, outdated software versions, and ineffective monitoring.

Management Decision: Concur

Corrective Action: The CIOO will establish and implement a plan to help prevent, detect, and remediate security weaknesses on all FDIC cloud platforms and applications.

Estimated Completion Date: December 30, 2026

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 Cloud Platform #1[15] team has begun coordinating with application owners, representatives of the Office of the Chief Information Security Officer (OCISO), and other subject matter experts to address the 7 findings and 19 associated recommendations. At the time the OIG issued its draft report, the CIOO had completed actions to address 9 of the 19 associated recommendations, and work was underway to address the remaining 10 recommendations.	August 30, 2025	$0	Yes	Open
2	The Cloud Platform #2 team has begun coordinating with application owners, representatives of OCISO, and other subject matter experts to address the 8 findings and 11 associated recommendations. At the time the OIG issued its draft report, the CIOO had completed actions to address 6 of the 11 associated recommendations, and work was underway to address the remaining 5 recommendations.	April 30, 2025	$0	Yes	Open
3	The Cloud Platform #3 team coordinated with relevant	October 31, 2024	$0	Yes	Open

[15] Due to the sensitive nature of the report, generic names are shown in place of the cloud platform names contained in the Recommendations and the related FDIC Comments and Summary of Corrective Actions sections of the report. (b) (7)(E) [redacted]

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
	application owners, representatives of OCISO, and other subject matter experts to address the 4 findings and 5 associated recommendations. The CIOO will prepare a closure package that documents the corrective actions taken.				
4	The Cloud Platform #4 team coordinated with relevant application owners, representatives of OCISO, and other subject matter experts to address the 3 findings and 6 associated recommendations. The CIOO will prepare a closure package that documents the corrective actions taken.	October 31, 2024	$0	Yes	Open
5	The Cloud Platform #5 team has begun coordinating with application owners, representatives of OCISO, and other subject matter experts to address the 4 findings and 7 associated recommendations. At the time the OIG issued its draft report, the CIOO had completed actions to address 5 of the 7 associated recommendations, and work was underway to address the remaining 2 recommendations.	February 28, 2025	$0	Yes	Open
6	The CIOO will assess existing roles, responsibilities and processes for performing security testing of FDIC applications and identify gaps. The CIOO will use the results of this assessment to (b) (7)(E)	December 30, 2025	$0	Yes	Open
7	The CIOO will establish and implement a plan to help prevent, detect, and remediate security weaknesses on all FDIC	December 30, 2026	$0	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
	cloud platforms and applications.				

[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
Twitter | @FDIC_OIG
Oversight.gov | www.oversight.gov