The FDIC's Adoption of Cloud Computing Services

July 2023 **No. AUD-23-003**

Audit Report

Audits, Evaluations, and Cyber

☆☆☆☆☆☆☆☆

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

Executive Summary

The FDIC's Adoption of Cloud Computing Services

The Federal Deposit Insurance Corporation (FDIC), like other Federal agencies, is modernizing its information technology (IT) infrastructure. In 2021, the FDIC began to accelerate its cloud migration to reduce its on-premises infrastructure and modernize its IT portfolio. The FDIC invested significant resources and made IT modernization the main priority of its IT strategy to improve internal operations. The FDIC plans to have most of its mission essential and mission critical[1] systems operating in the cloud by 2024.

Migration to the cloud introduces different security risks and privacy concerns as cloud environments differ from traditional on-premises IT architectures. In addition, organizations need to align cloud adoption with organizational performance goals by taking into consideration business goals and operational efficiencies when developing and implementing cloud systems. Therefore, it is imperative that organizations have an effective IT modernization strategy to ensure an effective transition occurs and that governance processes are in place to manage different risks.

The objective of our audit was to determine whether the FDIC has an effective strategy and governance processes to manage its cloud computing services.

Results

Overall, we found the FDIC had effective strategy and governance processes to manage its cloud computing services. However, the FDIC did not adhere to several cloud-related practices recommended by the Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and FDIC guidance in the following areas:

1. **Data Inventory for Cloud-Based Systems:** The FDIC did not have an inventory of all data assets residing in its cloud environments or a fully developed data catalog (i.e., organized inventory of its cloud data assets).

2. **Cloud Exit Strategy:** The FDIC did not establish an exit strategy as part of its cloud strategy planning to address issues (e.g., triggering events, roles

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

and responsibilities, and portability and transitioning of data) if the FDIC needed to terminate a contract with a cloud service provider.

3. **Contract Management Plans:** The FDIC did not develop Contract Management Plans (CMP) for all 17 contract actions for cloud services valued at over $546 million.

4. **Decommissioning Plans for Legacy Systems:** The FDIC did not develop disposal strategies and/or decommission plans for legacy systems.

As a result, these ineffective governance and strategy controls over cloud computing pose increased risks to the FDIC, including (1) security and privacy concerns due to the lack of visibility into cloud data, (2) inability to effectively move from an existing cloud service provider to another, (3) not identifying and mitigating performance risks and vulnerabilities in cloud contracts, and (4) increased potential for cyber attacks and costs from the lack of disposal strategies for legacy systems.

We determined that the FDIC had effective controls in seven other control areas related to application rationalization, IT governance bodies' alignment with cloud risks, cloud expenditures, cloud workforce transformation, assessment and authorization, continuous monitoring, and business continuity.

Recommendations

We are making nine recommendations to strengthen the strategy and governance over the FDIC's adoption of cloud computing services. Specifically, we recommend that the FDIC develop, maintain, and use an inventory and catalog of its cloud data throughout the cloud data lifecycle. In addition, we recommend that the FDIC establish and implement data governance requirements for managing data residing in the cloud. We also recommend that the FDIC establish an exit strategy for its cloud-based systems. Further, we recommend that the FDIC develop and implement CMPs for all active contract actions, to include contracts, basic ordering agreements, and related task orders, as required by FDIC policy; provide training to relevant staff on the requirement; and implement a review process. Finally, we recommend that the FDIC update the Project Management Lifecycle and/or System Development Life Cycle frameworks to include a Disposal phase and process; develop and implement policies and procedures for overseeing the decommissioning of legacy systems; and review current and planned system replacements to ensure legacy system decommissioning plans are created in accordance with FDIC policies and procedures.

The FDIC concurred with all nine recommendations in this report and plans to complete all corrective actions by September 30, 2024.

Contents

July 25, 2023

Subject | ***The FDIC's Adoption of Cloud Computing Services***

The FDIC, like other Federal agencies, is increasing its use and accelerating its adoption of cloud computing services. 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.[2]

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,[3] cloud computing also brings potential areas for concern, including system complexity, shared multi-tenancy environments,[4] internet facing services,[5] and loss of control over resources in the cloud service provider environment.

As the FDIC is migrating its mission essential and mission critical systems and applications into the cloud, an effective strategy must be in place to ensure there is alignment between cloud adoption and the FDIC's performance goals for increasing operational efficiencies and optimizing costs. In addition, with migrating systems and applications to the cloud, different security risks and vulnerabilities are introduced, and control over cloud systems and applications will vary by cloud provider and delivery service type. While cloud computing provides many benefits, it does not alleviate the need for governance but rather amplifies the need.[6] Effective cloud governance processes must be in place to manage security risks appropriately, enable visibility and control of IT infrastructure and data, and have contracting safeguards in place.

[2] NIST SP 800-145, *The NIST Definition of Cloud Computing* (September 2011).
[3] NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing* (December 2011).
[4] In cloud computing, multi-tenancy is when multiple customers of a cloud vendor are using the same computing resources. The primary concern with multi-tenancy environments is how to ensure security and isolation of environments.
[5] All programs and services that are accessed externally from the internet.
[6] According to NIST SP 800-144, governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it does not alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

The objective of this audit was to determine if the FDIC has an effective strategy and governance processes to manage its cloud computing services. Appendix 1 contains information about the objective, scope, methodology, and control areas tested.

BACKGROUND

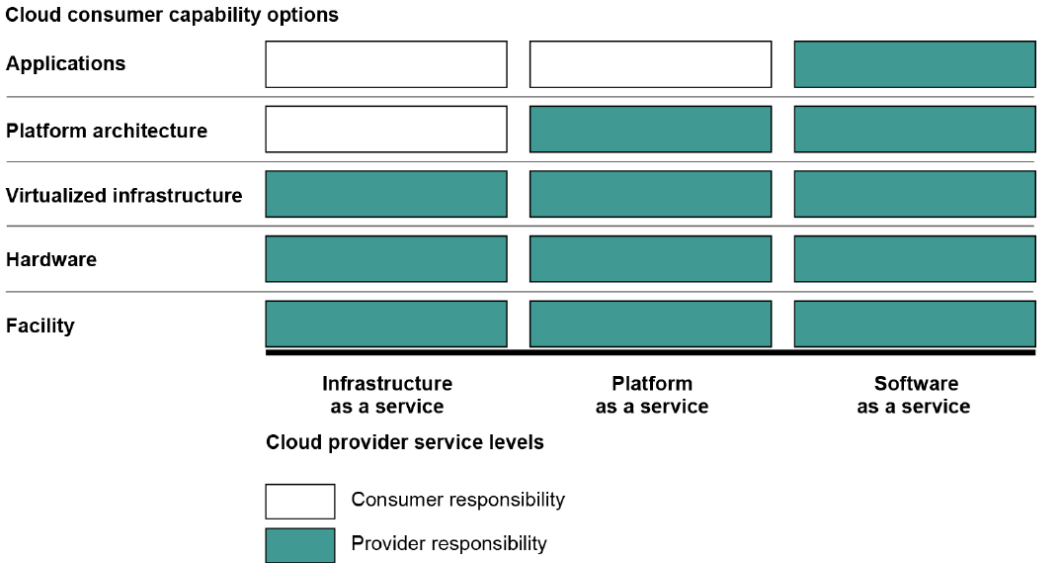
The FDIC's Current Cloud Environment

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 that the head of each agency 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 IT portfolio by migrating to the cloud.

As of March 2023, the FDIC had 252 systems in operation with 95 being cloud-based (38 percent) and had 7 major cloud platforms in use. The FDIC operates in a multi-cloud environment, procuring services from various cloud service providers who provide Infrastructure as a Service (IaaS),[7] Platform as a Service (PaaS),[8] and Software as a Service (SaaS).[9] As shown in **Figure 1**, the FDIC's responsibilities vary under the three cloud delivery service models and increase from the SaaS to the PaaS and IaaS service models. For example, the FDIC is responsible for developing, securing, and managing platform architecture and applications in an IaaS service model. In contrast, a third-party provider performs these responsibilities in the SaaS service model.

[7] IaaS is a model in which a third-party provider hosts servers, storage, and other computing resources and makes them available to customers so they can deploy and run operating systems, software, and applications.
[8] PaaS is a model in which a third-party provider hosts application development platforms and tools on its own infrastructure and makes them available to customers.
[9] SaaS is a software distribution model in which a third-party provider hosts applications and makes them available to customers.

Figure 1: Cloud Service Provider and Consumer Responsibilities for the Three Service Models



Source: GAO Report, *Agencies Need to Incorporate Key Practices to Ensure Effective Performance* (GAO-16-325) (April 2016).

As the FDIC continues to expand its cloud presence, costs for cloud initiatives are expected to increase.[10] In 2021, the budget for cloud initiatives was $53,391,238. Then, in 2022, the budget for cloud initiatives grew to $55,381,947 and accounted for about 18 percent of the Division of Information Technology (DIT) budget of $306,370,273. The FDIC plans to have most of its mission essential and mission critical systems in the cloud by 2024. Cloud IT investments are expected to grow in the subsequent years as the FDIC continues to migrate more legacy systems into the cloud environment.

The FDIC's Cloud Strategy

2025 FDIC Target State Architecture Plan

In response to Executive Order 14028, the FDIC published its 2025 Target State Architecture Plan in December 2021, which outlined the next phase of the FDIC's IT modernization efforts. The 2025 FDIC Target State Architecture Plan incorporates OMB *Federal Computing Strategy* (Cloud Smart)[11] implementation guidance and emphasizes a foundational transformation in the FDIC's IT portfolio management to

[10] Cloud initiatives include the costs associated with procuring new cloud services, including licenses, subscriptions, and platforms, and the associated operations and maintenance costs.
[11] According to OMB, *Federal Cloud Computing Strategy* (Cloud Smart) (June 2019), the Cloud Smart strategy offers practice implementation guidance for Government missions to fully actualize the promise and potential of cloud-based technologies while ensuring thoughtful execution that incorporates practical realities.

increase operational efficiencies, improve cost transparency, and optimize costs to obtain the best business value.

To achieve its target state architecture, the FDIC laid out four overarching themes: (1) accelerating cloud adoption, (2) revamping IT delivery, (3) empowering the customer, and (4) establishing cross-cutting enablers.[12] For accelerated cloud adoption, the FDIC intends to embrace commercial Federal Risk and Authorization Management Program-authorized cloud services to securely increase the visibility, scalability, and flexibility of IT capabilities.

The FDIC's Quantum Leap Program

As part of the Target Architecture State 2025 plan to accelerate cloud adoption, the FDIC initiated its *Quantum Leap* program in March 2022. The program is intended to establish Microsoft Azure, an IaaS, as the FDIC's primary platform for its mission essential and mission critical applications and accelerate the FDIC's phase-out of its on-premises Backup Data Center and Primary Data Center. The FDIC plans to complete the migration of 20 mission essential and mission critical applications to Microsoft Azure in 2024.

The FDIC's Cloud Governance Processes

Information Technology Asset Management

IT asset management is ensuring an organization's assets are accounted for, deployed, maintained, upgraded, and disposed of when an asset is to be retired. As organizations consider acquiring new IT assets, they must consider a strategy to both transition into and exit the application or system. An exit strategy ensures the cloud services used by an organization can be replaced with minimal interruption and in an efficient manner. Where an active cloud service provider cannot meet its contractual obligations, an exit strategy can help relay key information on migrating to a new cloud service provider, retrieving the organization's data, and efficiently moving to a new provider with minimal disruptions to services.

As organizations accelerate their movement into the cloud environment, cloud-based systems replace on-premises legacy systems. Organizations require a strategy to dispose of legacy systems to avoid redundancy and incurring excessive costs. More importantly, organizations must secure their sensitive data to properly dispose of legacy systems. Outdated systems are more prone to security attacks, and vital

[12] Cross-cutting enablers refer to the implementation of foundational capabilities (e.g., Cybersecurity and Privacy, Zero Trust Architecture, Identity and Access Management, and Data Management) across every platform, application, and system.

data, including Personal Identifiable Information, can be leaked through legacy systems if the system is not disposed of properly. Organizations must also consider rendering all storage devices and media inoperable and/or incapable of leaking data to third parties.

Contract Risk Management

Contract risk management is the process that allows businesses to realize the maximum value of their contracts while continuously identifying, tracking, and minimizing risk throughout the contract lifecycle. Contract risk management is critical for the overall success of contractual relationships and arrangements because it provides a more efficient way to spot potential challenges early on and avoid them. Cloud contract awards will increase as the FDIC continues to modernize its IT architecture by reducing its on-premises infrastructure and moving towards cloud-based solutions.

To manage inherent risks related to contracts, the FDIC implemented CMPs to describe the oversight necessary to ensure the contractor makes satisfactory progress toward the successful completion of the contract. The objective of the CMP is to ensure that the Contracting Officer (CO), Oversight Manager (OM), and Technical Monitor have a common understanding of both contractor and FDIC obligations under the contract. Additionally, a CMP reflects a strategy for managing key contract vulnerabilities or performance areas inherent in the contract, and any unique contract terms and conditions.

Data Governance

Data governance defines roles, responsibilities, policies, and processes for ensuring accountability for, and stewardship of, data assets across the enterprise. Data governance is a function of an organization's overarching enterprise data strategy. This strategy or framework provides the organization with a holistic approach to collecting, managing, securing, and storing data. With cloud computing, cloud-based architectures challenge organizations to evolve the traditional methods of securing data due to cloud service providers and customers sharing control of computing resources.

Therefore, it is imperative that organizations ensure cloud service providers have robust data governance practices in place. Multi-tenancy and shared security responsibilities within cloud computing require an organization to give more consideration to cloud data governance.

Roles and Responsibilities

The FDIC's Chief Information Officer Organization (CIOO) has responsibility for IT governance, investments, program management, information security, and privacy. Within the CIOO, the Office of the Chief Information Security Officer (OCISO) is responsible for the agency-wide information security program and privacy support for the information and information systems that support the operations and assets of the FDIC. The CIOO also maintains a Chief Data Officer Staff, which is responsible for leading the design, integration, and institutionalization of the FDIC's Enterprise Data Strategy.

The FDIC's Division of Administration (DOA) is responsible for acquisition, corporate, and human resource services. Within DOA, the Acquisition Services Branch (ASB) is responsible for all procurement actions awarded in the corporate, receivership, or conservatorship capacity.

AUDIT RESULTS

Overall, we found the FDIC had effective strategy and governance processes to manage its cloud computing services. However, the FDIC did not adhere to several cloud-related practices recommended by OMB, NIST, and FDIC guidance in 4 of the 11 areas we assessed (See Appendix 1). Specifically, we found that the FDIC should improve controls for data governance, cloud exit strategy, contract management plans, and decommissioning plans for legacy systems. We also found that the FDIC had effective controls in the remaining seven control areas we assessed related to application rationalization, IT governance bodies' alignment, cloud expenditures, cloud workforce transformation, assessment and authorization, continuous monitoring, and business continuity.

Finding #1: The FDIC Did Not Inventory Data Stored in the Cloud Environment

The FDIC did not have an inventory of all data assets residing in its cloud environments or fully develop a data catalog (i.e., organized inventory of its cloud data assets). OMB Circular A-130, *Managing Information as a Strategic Resource* (July 2016), requires that agencies maintain an inventory of major information systems, information holdings, and dissemination products at a level of detail that is

most appropriate for overseeing and managing the information resources.[13] OMB Circular A-130 requires that the inventory of agency information resources include an enterprise-wide data inventory that accounts for data used in the agency's information systems.

In addition, the OPEN Government Data Act requires agencies to develop and maintain a comprehensive data inventory that accounts for all data assets created by, collected by, under the control or direction of, or maintained by the agency.[14] The OPEN Government Data Act requires that an agency's data inventory "provides a clear and comprehensive understanding of the data assets in the possession of the agency." The OPEN Government Data Act tasked OMB with issuing guidance to agencies on how to construct its comprehensive data inventory, among other requirements in the statute.

In December 2021, the GAO acknowledged in a report on the OPEN Government Data Act that implementation of this statutory requirement is critical to agencies' full implementation and compliance with the OPEN Government Data Act. The GAO also stated that absent formal OMB guidance, OMB has pointed agencies to existing policies and resources.[15] For example, OMB collaborates with the General Services Administration (GSA) and the National Archives and Records Administration (NARA) to provide agencies with a repository of open data tools, best practices, and schema standards on the Federal Enterprise Data Resources website.[16] OMB also participates in the Chief Data Officer Council and CIO Council to assist agencies with challenges and questions as they implement the OPEN Government Data Act requirements.

Furthermore, NIST SP 800-53, Revision 5, PM-23, *Data Governance Body,* requires Federal agencies to establish a Data Governance Body with specific roles and responsibilities. PM-23 also requires establishing policies, procedures, and standards that facilitate data governance so that data is effectively managed and maintained.

---

[13] The FDIC has determined that OMB Circular A-130 is "generally applicable" to the FDIC, to the extent that the Circular aligns with OMB's statutory authorities; does not impose obligations on the FDIC based on statutes that are legally inapplicable to the FDIC; and does not conflict with the FDIC's independence, statutory obligations, or regulatory authority.

[14] Pub. L. No. 115–435, 132 Stat. 5529 (2019). Requirements for Federal agencies to improve Federal data management are codified at 44 U.S.C §§ 3501, 3502, 3504, 3506, 3511, and 3520. The FDIC has determined that the OPEN Government Data Act is legally binding on the FDIC.

[15] GAO, *Open Data: Additional Action Required for Full Public Access* (GAO-22-104574) (December 2021) examines (1) the extent to which OMB met its statutory requirements; (2) selected agencies' progress developing comprehensive data inventories; (3) the extent to which selected agencies engage with the public; and (4) how data users value and use information made publicly available.

[16] OMB, GSA, and NARA established and maintain this repository of resources intended to facilitate the adoption of open data practices across the Federal government.

The FDIC has established a data governance framework and body for all FDIC data and is maturing the governance processes supporting the framework.[17] However, the FDIC has not yet established data governance requirements (i.e., policies, processes, roles, and responsibilities) for managing FDIC data stored in the cloud, a component of the FDIC's data governance framework. In response to our concern, FDIC officials stated that the lack of guidance from OMB on cataloging and inventorying of agency data was a contributing cause for the lack of a data inventory and fully developed data catalog.

Further, FDIC officials stated that in the absence of OMB guidance, they have taken steps to address the intent of the OPEN Government Data Act, to include publishing an inventory of priority data assets and beginning to develop a data catalog. However, despite the lack of OMB guidance pertaining to the OPEN Government Data Act, the FDIC is still required to comply with OMB Circular A-130, which requires an enterprise-wide data inventory that accounts for data used in the agency's information systems (including cloud-based systems).

Having complete visibility into what cloud data exists and where it resides (including throughout the data life cycle) is vital for the FDIC to address privacy and security concerns.[18] For example, it is imperative that the FDIC understands what Personally Identifiable Information exists in the cloud environment to ensure it is properly managed. In addition, visibility into all existing cloud data helps to promote efficiency and effectiveness of FDIC operations, including the incorporation of data analytics to support business objectives. Not having complete visibility into what cloud data exists poses increased risks to security and privacy and overall effectiveness of operations at the FDIC.

Recommendations

We recommend that the CIOO:

1. Develop and maintain an inventory and catalog of all FDIC data used throughout the cloud data lifecycle.

[17] In April 2020, the Chief Data Officer Staff released the FDIC's *Enterprise Data Governance: Framework and Enterprise Data Council Charter*. The goal of the framework is to effectively govern and manage the FDIC's data. To achieve that goal, the FDIC is leveraging data stewards to represent families of data and advocate for the data strategy to be adopted by the organization. In addition, the framework establishes responsibilities of the Chief Data Officer and the Council Chair.

[18] According to NIST SP 800-37, Revision 2, information life cycle (or data life cycle) is defined as "the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion."

2. Establish and implement data governance requirements (e.g., policies, processes, roles, and responsibilities) for managing data residing in the cloud.

Finding #2: The FDIC Did Not Establish a Cloud Exit Strategy

The FDIC did not establish an exit strategy as part of its overall cloud strategy planning to address issues (e.g., triggering events, roles and responsibilities, and portability and transitioning of data) if the FDIC needed to terminate a contract with a cloud service provider. A triggering event can occur when a cloud service provider cannot execute the services it is contractually required to perform. This is important given that the FDIC operates in a cloud environment and has started moving its mission essential and mission critical applications to the cloud and continues to do so. A disruption in these applications and related services could affect the FDIC's ability to perform its roles and responsibilities.

In fulfilling its mission, the FDIC is becoming more dependent on cloud service providers. The FDIC has phase-in/phase-out clauses in its cloud contracts with cloud service providers to address situations where the FDIC needs to terminate a contract on an ad-hoc basis. These clauses require a cloud service provider to fully cooperate with a smooth migration out of the cloud service provider's cloud environment to another environment and provide requirements for handling FDIC data. However, an exit strategy is a component of an organization's broader cloud strategy and provides a standardized approach for identifying and handling situations where the FDIC needs to terminate a relationship with a cloud service provider. For example, this includes determining which events would trigger the FDIC's termination of a relationship with a cloud service provider and the process for identifying a replacement cloud service provider.

Gartner conducts and shares research on topics related to information technology.[19] The Gartner *Cloud Strategy Cookbook* provides best practices for developing a cloud strategy as part of cloud-based implementations.[20] In developing a cloud strategy, Gartner recommends adding an exit strategy that addresses topics such as data ownership, data backups, reclaiming an organization's data from a cloud service provider, and portability of data within IT environments.

CIOO officials stated that the FDIC does not have an exit strategy for its cloud-based systems. They further stated that they could not have an exit strategy with the Microsoft Azure environment before determining where on-premises systems are going in the cloud environment, what services the FDIC is using, and what the

[19] Gartner is the registered trademark and service mark of Gartner Inc. and has been used herein with permission. All rights reserved.
[20] Gartner, *The Cloud Strategy Cookbook,* April 2021.

dependencies and interdependencies are for systems. However, this does not minimize the need for the FDIC to develop a cloud exit strategy that provides an overall approach for exiting a relationship with any of its cloud service providers.

When planning a cloud implementation, it is necessary to have an exit strategy that describes when and how to exit a cloud service provider relationship with minimal disruption to the FDIC's operations. For example, the FDIC could lose its data and experience prolonged downtime when obtaining and transitioning to a new cloud service provider. Further, a cloud service provider may not meet agreed-upon performance metrics such as consistently providing an acceptable level of service, and the FDIC may not properly or efficiently transition to a new cloud service provider.

Recommendation
We recommend that the CIOO:

3. Establish an exit strategy for all cloud-based systems.

Finding #3: The FDIC Did Not Develop Contract Management Plans

The FDIC did not develop CMPs for all 17 contract actions that included BOAs,[21] contracts for goods and services, and software licenses and renewals for the five cloud-based platforms sampled. See **Table 1** for the names and a brief description of each platform, the number of contract actions supporting each platform, and total value of contract actions for each platform.

[21] A BOA is a written instrument of understanding negotiated between the FDIC and a contractor for future delivery of as yet unspecified quantities of goods or services. A BOA becomes a binding contract when a task order is issued.

Table 1: Summary of Sampled Contract Actions and Contract Values for Each Cloud-Based Platform

Cloud-Based Platform	Number of Contract Actions*	Total Value of Contract Actions for Each Platform
Appian: Low-code automation platform for end-to-end processes.	6	$113,485,263
Azure and Microsoft 365 (M365): Azure is Microsoft's public cloud platform. M365 is a cloud-based suite of productivity applications.	2	$192,920,000
Salesforce: Customer relationship management platform.	6	$115,800,000
ServiceNow: IT service management and automation platform.	2	$30,616,153
Azure, M365, and ServiceNow Platform Support	1	$93,750,000
Total	**17**	**$546,571,416**

Source: FDIC contracts obtained from the Contract Electronic File (CEFile) system.[22]

* Each BOA, Contract, and Software License and Renewal has a contract value of at least $1 million.

The Acquisition Policy Manual requires the CO and the OM to develop a CMP for the acquisition of services having a total estimated value of $1 million and greater. For task orders, the $1 million threshold applies at either the Basic Ordering Agreement (BOA)/RBOA (Receivership BOA)/BPA (Blanket Purchase Agreement) level or at the task order level, depending on the nature of the task order.[23] If the combined value of the task orders is expected to be $1 million or greater and the task orders will involve the same contract oversight approach, a single CMP may be processed at the BOA, RBOA, or BPA level.

According to the Acquisition Policy Manual, the objective of the CMP is to ensure the CO, OM, and Technical Monitor have a common understanding of both contractor and FDIC obligations under the contract. The CO is responsible for initiating the CMP and ensuring a signed copy is in the CEFile system. Also, the FDIC's *Acquisition Procedures, Guidance and Information (PGI)* (November 2021) requires, at a minimum, that a CMP be developed before the post-award conference (generally held no later than one week after award), if one is held, and updated as

[22] The CEFile system is the official contract file of record and contains pre-award, post-award, and contract file documentation.
[23] RBOA, a unique type of contract which is similar to a BOA, may only be used for contracts in support of the Division of Resolutions and Receiverships' (DRR) efforts related to failing or failed financial institutions. A BPA is an agreement establishing FDIC rights to place orders for specific goods or services but is not a contract because it does not obligate funds, nor does it obligate the FDIC to place any call orders under it.

appropriate during performance to reflect any major changes to the contract or oversight plan.

Acquisition Services Branch Oversight

After we notified ASB of this issue, the ASB Deputy Director instructed the appropriate COs to complete the CMPs for the 17 contract actions we identified as missing. In addition, the ASB Deputy Director instructed ASB Assistant Directors to review all active contracts and complete a CMP if one is required and missing. However, ASB could not provide the results of these reviews showing which CMPs were initially missing.

To understand the extent to which active contract actions lacked CMPs by the post-award conference date, we selected an additional sample of 93 active contract actions assigned to the DIT/CIOO and valued at $1 million or greater as of February 2023. We searched the CEFile system and found CMPs for 91 of 93 contract actions selected; however, we determined the FDIC did not have any of the 91 CMPs in place by the post-award conference date.

Therefore, the CMPs were not in place to help ensure inherent performance risks and contract vulnerabilities were managed appropriately for extended periods of time for most contracts selected. We determined that 18 of 93 contract actions selected did not have a completed CMP for more than 5 years after the award date and 50 of 93 contract actions selected did not have a completed CMP between 1 and 4 years after the award date.[24]

In response to our concerns, the ASB Deputy Director stated that, prior to their tenure, the top priority for ASB was awarding contracts quickly, and on-boarding contractors was essential to the FDIC's mission.[25] This led to the assigned COs prioritizing other time-sensitive procurement actions and not adhering to ASB controls for developing CMPs.

Therefore, ASB did not enforce or monitor the COs' compliance with CMP requirements for the 17 cloud contract actions, valued at over $546 million, to ensure proper contract oversight and appropriate use of resources. The FDIC operates in a multi-cloud environment with cloud-based contracts that inherently have performance risks and contract vulnerabilities that must be managed and monitored to be mitigated effectively. Without CMPs, the FDIC may not monitor performance

[24] While the requirement is to complete the CMP before the post-award conference, to facilitate testing, we used the award date as an approximation of the trigger date for when the CMPs should have been completed. The post-award conference should generally be held no later than one week after the award date.
[25] The previous ASB Deputy Director retired in January 2022.

measures, respond to missed metrics, and enforce penalties in a consistent manner, all of which could lead to inefficient use of resources and disruption to FDIC operations.

While we could not determine whether the lack of CMPs directly contributed to performance issues in the contract actions we reviewed, the FDIC documented significant performance issues with cloud-based contracts through contract performance evaluations. For example, the FDIC's performance evaluation for one sampled cloud contract reported that the contractor missed requirements, did not identify defects, had difficulty finding and retaining skilled staff, and other performance issues that caused a schedule delay of 6 months. CMPs are designed to serve as an oversight mechanism to ensure COs and OMs are aware of inherent performance risks and vulnerabilities and can better respond to any potential issues that may arise.

History of Deficient Contract Management at the FDIC

Over the past several years, the OIG has identified similar contract management deficiencies at the FDIC related to inadequate resources and lack of compliance with established management controls. Since 2017, the OIG has identified Contract Management as a Top Management and Performance Challenge facing the FDIC, with inadequate staffing resources being the main concern.[26] Additionally, our OIG report, *Contract Oversight Management* (EVAL-20-001) (October 2019), found the FDIC needed to improve its contracting management information system, contract documentation, OM workload, and OM training and certification.

Further, our OIG report, *Critical Functions in FDIC Contracts* (EVAL-21-002) (March 2021), found that the FDIC did not have policies and procedures for identifying Critical Functions in its contracts, and did not implement heightened contract monitoring activities for procured Critical Functions.[27] Finally, in both 2021 and 2022, the GAO found that the FDIC had a significant internal control deficiency within its contract oversight and invoice review and payment processes.[28]

[26] We previously identified contract management as a Top Management and Performance Challenge at the FDIC (2018, 2019, 2020, 2021, 2022, and 2023).
[27] OMB, Publication of the Office of Federal Procurement Policy, Policy Letter 11-01, Performance of Inherently Governmental and Critical Functions (September 2011) (OMB Policy Letter 11-01), defines critical function as "a function that is necessary to the agency being able to effectively perform and maintain control of its mission and operations."
[28] GAO Management Report: *Improvements Needed in FDIC's Internal Control over Contract-Payment Review Processes* (GAO-21-420R) (May 2021) and GAO Management Report: *Improvements Needed in FDIC's Internal Control over Contract Documentation and Payment-Review Processes* (GAO-22-105824) (May 2022).

Recommendations
We recommend that the Director, DOA:

4. Develop and implement Contract Management Plans for all contract actions, including contracts, basic ordering agreements, and related task orders, as required by FDIC policy.

5. Provide additional training to Contracting Officers and Oversight Managers to emphasize the requirement to develop Contract Management Plans for contract actions, when appropriate.

6. Develop and implement policies and procedures to regularly review contract actions to confirm Contract Management Plans are put in place.

Finding #4: The FDIC Did Not Establish a Process to Decommission Legacy Systems

The FDIC did not establish a standardized process to develop disposal strategies and/or decommission plans for legacy systems. Of the 26 cloud initiatives with related legacy systems operating for over one year, we judgmentally selected five initiatives and their related legacy systems (see **Table 2**). Only one initiative (FOCUS – Framework for Oversight of Compliance and CRA (Community Reinvestment Act) Activities User Suite)[29] included a plan outlining decommissioning activities for its related legacy system (SOURCE – System of Uniform Reporting of Compliance and CRA Exams) with estimated milestone dates documented in ServiceNow.[30]

In contrast, management did not follow a similar process for documenting decommissioning activities for the remaining four initiatives and their associated legacy systems. As a result, the FDIC was unable to provide documentation supporting its decommissioning activities for the four initiatives that demonstrated the FDIC considered and consistently managed all aspects of the decommissioning process such as record retention, contract considerations, and hardware component identification, as applicable.

[29] FOCUS provides enhanced supervisory capabilities to schedule, plan, document, and report on Division of Depositor and Consumer Protection (DCP) supervisory activities for Compliance and CRA.
[30] We are leveraging FOCUS as an internal FDIC best practice and the decommissioning plans or strategy of SOURCE to compare to other decommissioning efforts of FDIC systems.

Table 2: Sample Selection of Cloud Initiatives and Related Legacy Systems*

Division	Sampled Cloud Initiative/System	Legacy System Replaced
DCP	FOCUS	SOURCE
DRR	RRMP	FACTS
DRR	PASS	STRS and STRS Field
DRR	RITA	BOLD, RPT, and FMS
DCP	CRAPES Cloud	CRAPES On-premises

Source: CIOO-provided information obtained from FDIC information systems and program officials.

* The following are the acronyms defined: RRMP (Resolution and Receivership Management Portal; FACTS (FDIC Automated Corporate Tracking System); PASS (Purchase and Assumption Settlement System); STRS Field (Settlements Tracking and Reconciliation System-Field Version); RITA (Resolution Information Tracking Application); BOLD (BIS Operational Database); RPT (Resolution Planning Tool); FMS (Franchise Marketing System); and CRAPES (Community Reinvestment Act Performance Ratings).

To ensure the FDIC decommissions legacy systems effectively and in a timely manner, project managers need to develop a disposal strategy and/or decommission plan with timelines for key activities, such as identifying application components, working with key stakeholders to archive data, identifying records to be disposed of, and coordinating with IT security for managing and cleansing data.

NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (December 2018), Task M-7, states, "[i]mplement a system disposal strategy and execute required actions when a system is removed from operation." This NIST guidance identifies this step as part of the Disposal phase of the System Development Life Cycle. Further, NIST SP 800-160, Vol. 1, *Systems Security Engineering – Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (November 2016), lists key security activities and tasks for the Disposal process.

Also, the GSA Office of Shared Solutions and Performance Improvement (OSSPI), developed the *Modernization and Migration Management (M3) Playbook* to help customer and provider organizations apply the M3 Framework by providing guidance, tools, and templates, based on best practices, to improve the likelihood of successful outcomes of their modernization and migration projects.[31] The M3 Framework is a six-phased approach to system and service modernizations and migrations. As part of the Selection phase, one of the key objectives is to develop a

[31] OSSPI coordinates government-wide shared services governance, executes program management, and develops processes to support development and implementation of OMB policy as it relates to mission support services.

plan to retire the legacy system(s). This objective includes task activities and best practices for decommissioning legacy systems, such as: reviewing contract language; identifying application and hardware components; coordinating with key stakeholders; and drafting a decommission plan.[32]

Lastly, GAO, *Standards for Internal Control in the Federal Government* (September 2014), states, "[m]anagement should design control activities to achieve objectives and respond to risks. Management designs control activities in response to the entity's objectives and risks to achieve an effective internal control system. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks."

The FDIC did not have clearly documented decommissioning plans because the FDIC, *Project Management Lifecycle* (October 2022) and the FDIC, *System Development Life Cycle Framework* (December 2021), did not include a Disposal phase as recommended by NIST. Additionally, we found that the FDIC did not develop policies and procedures to require and guide project teams through developing decommissioning plans for legacy systems. This resulted in the FDIC not having a standardized process in place to oversee the decommissioning of legacy systems in an effective and efficient manner.

Without a standardized process, the FDIC may not decommission legacy systems promptly, which increases the attack surface for a potential attacker. In addition, the FDIC may not be destroying data from the legacy systems in a timely and secure manner. As legacy systems remain operational, they can also become expensive to maintain. Lastly, legacy systems not decommissioned in accordance with best practices may be exposed to additional cybersecurity risks.

Recommendations

We recommend that the CIOO:

7. Update the Project Management Lifecycle and/or System Development Life Cycle frameworks to include a Disposal phase and process.

8. Develop and implement policies and procedures for overseeing the decommissioning of legacy systems.

9. Review all current and planned system replacements and ensure legacy system decommissioning plans are created in accordance with FDIC policies and procedures.

[32] GSA, *Modernization and Migration Management (M3) Playbook* (2022).

FDIC COMMENTS AND OIG EVALUATION

The FDIC's Chief Information Officer (CIO) and Deputy to the Chairman and Chief Operating Officer (COO) provided a written response, dated July 18, 2023, to a draft of the report. The response is presented in its entirety beginning on page 24. In the response, the CIO and Deputy to the Chairman and COO concurred with the report's recommendations. The recommendations will remain open until we confirm that corrective actions have been completed and are responsive. A summary of the FDIC's corrective actions begins on page 28.

Objective

The objective of this audit was to determine if the FDIC has an effective strategy and governance processes to manage its cloud computing services.

We conducted this audit from June 2022 through June 2023. This audit was performed in accordance with *Generally Accepted Government Auditing Standards*. 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.

Scope and Methodology

We assessed the effectiveness of the FDIC's cloud strategy and governance processes in the following 11 control areas:

Table 3: Summary of Strategy and Governance Control Areas Assessed

		Control Area
Strategy	1	Federal Mandates/Requirements and Business Outcomes Alignment
	2	Application Rationalization/Critical Legacy Systems
	3	Decommissioning of Legacy Systems in a Timely Manner
Governance	4	Review of Existing IT Governance Bodies' Alignment With Cloud Related Risks
	5	Cloud Data Governance
	6	Cloud Expenditures
	7	Contract Language/Service Level Agreement Monitoring/Contract Performance
	8	Cloud Workforce Transformation
	9	Assessment & Authorization/Authority to Operate (ATO) Process
	10	Continuous Monitoring
	11	Business Continuity

Source: OIG analysis based on cloud strategy and governance-related Federal regulations, Executive Orders, standards, and best practices.

The scope of our audit focused on the effectiveness of the FDIC's strategy and governance processes to modernize and migrate on-premises systems and

applications into the cloud and determine if the strategy aligns with Federal mandates and requirements. Specifically, we assessed:

- The FDIC project planning and contracting efforts for achieving goals and objectives related to adopting cloud computing services and if the goals and objectives align with NIST and government-wide security policy and guidance;
- How the FDIC considers security and privacy risks and its related Federal mandates when acquiring cloud services and how cloud-related expenditures are managed at the FDIC;
- The effectiveness of on-going monitoring of Service Level Agreements with Cloud Service Providers according to Federal requirements and contractual obligations;
- Whether the FDIC has provided training and hired resources with skill sets to manage cloud-based systems; and
- The FDIC's Authority to Operate processes.

To achieve our objective, we conducted the following procedures:

- Interviewed FDIC senior executives (e.g., CIO) and Division-level personnel (e.g., DIT, DOA, Division of Finance, DRR, Legal) regarding FDIC cloud computing services.

- Reviewed applicable Federal regulations, Executive Orders, and standards related to cloud computing:
  - Executive Order 14028, *Improving the Nation's Cybersecurity* (May 2021);
  - OMB *Federal Cloud Computing Strategy "Cloud Smart"* (June 2019);
  - OMB Circular A-130, *Managing Information as a Strategic Resource* (July 2016);
  - NIST Special Publication 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations* (December 2018);
  - NIST Special Publication 800-145, *The NIST Definition of Cloud Computing* (September 2011);
  - NIST Special Publication 800-160 Volume 1, *Systems Security Engineering-Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (November 2016);
  - Foundations for Evidence-Based Policymaking Act of 2018;
  - GAO Report, *OPEN Government Data Act* (GAO-22-104574) (December 2021); and
  - Federal Chief Data Officer Council Report, *Enterprise Data Inventories* (April 2022).

- Reviewed FDIC policies and procedures related to acquisition and IT system authorization:
  - FDIC *Acquisition Policy Manual* (January 24, 2020);
  - FDIC *Acquisition Procedures, Guidance, and Information* (November 2021); and
  - FDIC *Assessment and Authorization Process Guide* (February 2022).

- Reviewed applicable best practices (Gartner, Cloud Security Alliance, and other) related to cloud migration including:
  - Gartner *Cloud Strategy Cookbook* (February 2021);
  - Microsoft's *Exit Planning for Microsoft Cloud Services* (August 2020);
  - Cloud Security Alliance: *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* (2021); and
  - GSA OSSPI: *Modernization and Migration Management Playbook.*

- Reviewed reports from other OIGs that have performed similar audit work related to the adoption of cloud computing services, including:
  - Department of Energy OIG Report, *Management of Legacy Information Technology Infrastructure* (DOE-OIG-19-22) (March 2019);
  - General Services Administration OIG Report, *Audit of the Federal Risk and Authorization Management Program, Program Management Office's Goals and Objectives* (A170023/Q/T/P19002) (March 2019);
  - National Archives and Records Administration OIG Report, *Audit of NARA's Adoption and Management of Cloud Computing* (17-AUD-08) (March 2017);
  - Nuclear Regulatory Commission OIG Report, *Audit of NRC's Adoption of Cloud Computing* (OIG-17-A-16) (June 2017);
  - Securities and Exchange Commission OIG Report, *SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services* (Report No. 556) (November 2019);
  - Department of Homeland Security OIG Report, *Progress and Challenges in Modernizing DHS' IT Systems and Infrastructure* (OIG-20-61) (August 2020); and
  - Department of Commerce OIG Report, *The Census Bureau Must Correct Fundamental Cloud Security Deficiencies in Order to Better Safeguard the 2020 Decennial Census* (OIG-19-015-A) (June 2019).

- Selected a judgmental sample of seven cloud-based systems to determine if the FDIC:
  - performed an application rationalization process;
  - monitored costs to migrate and operate in the cloud environment;
  - included Service Level Agreements in its contracts with cloud service providers;

  - authorized these systems to operate; and
  - performed continuous monitoring.

- Selected a judgmental sample of five cloud-based systems to determine if the FDIC had developed decommissioning plans for these systems' associated legacy systems.

- Selected a judgmental sample of 17 contract actions to determine if the FDIC had completed CMPs within the required timeframe.

- Selected all 93 active DIT/CIOO contract actions with a value of $1,000,000 or greater to determine if the FDIC had completed Contract Management Plans within the required timeframe.

We relied on computer-processed information used to generate total contract awards. We corroborated the data from the automated system used to support our audit conclusions with the contract documents we obtained. As a result, we determined that the information was sufficiently reliable for our analysis. In addition, we addressed the risk of fraud and abuse related to our objective in the course of evaluating audit evidence.

Appendix 2 Acronyms and Abbreviations

ASB	Acquisition Services Branch
BOA	Basic Ordering Agreement
BOLD	BIS Operational Database
BPA	Blanket Purchase Agreement
CDO	Chief Data Officer
CEFile	Contract Electronic File
CIOO	Chief Information Officer Organization
CMP	Contract Management Plan
CO	Contracting Officer
CRAPES	Community Reinvestment Act Performance Rating
DCP	Division of Depositor and Consumer Protection
DIT	Division of Information Technology
DOA	Division of Administration
DRR	Division of Resolutions and Receiverships
FACTS	FDIC Automated Corporate Tracking System
FDIC	Federal Deposit Insurance Corporation
FMS	Franchise Marketing System
FOCUS	Framework for Oversight of Compliance and CRA Activities User Suites
GAO	Government Accountability Office
GSA	General Services Administration
IaaS	Infrastructure as a Service
IT	Information Technology
M3	Modernization and Migration Management
NIST	National Institute of Standards and Technology
OCISO	Office of Chief Information Security Officer
OIG	Office of Inspector General
OM	Oversight Manager
OMB	Office of Management and Budget

Appendix 2 Acronyms and Abbreviations

OSSPI	Office of Shared Solutions and Performance Improvement
PaaS	Platform as a Service
PASS	Purchase and Assumption Settlement System
PGI	Procedure, Guidance, and Information
RBOA	Receivership Basic Ordering Agreement
RITA	Resolution Information Tracking Application
RPT	Resolution Planning Tool
RRMP	Resolution and Receivership Management Portal
SaaS	Software as a Service
SLA	Service-Level Agreement
SOURCE	System of Uniform Reporting of Compliance and CRA Examinations
STRS	Settlements Tracking and Reconciliation System

Federal Deposit Insurance Corporation

MEMO

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

FROM: Sylvia W. Burns For MARK MULHOLLAND Digitally signed by MARK MULHOLLAND Date: 2023.07.18 10:51:46 -04'00'
Chief Information Officer, Chief Privacy Officer, and Director, Division of Information Technology

Daniel H. Bendler DANIEL BENDLER Digitally signed by DANIEL BENDLER Date: 2023.07.18 14:02:29 -04'00'
Deputy to the Chairman and Chief Operating Officer

CC: Sanjeev Purohit, Acting Deputy Chief Information Officer for Technology/Chief Technology Officer
Mark F. Mulholland, Deputy Chief Information Officer for Management
E. Marshall Gentry, Chief Risk Officer
Shanna R. Webbers, Deputy Director, Acquisition Services Branch, Division of Administration

DATE: July 18, 2023

RE: Draft Audit Report, entitled *The FDIC's Adoption of Cloud Computing Services*

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft audit report, entitled *The FDIC's Adoption of Cloud Computing Services (No. 2022-003)*. The OIG issued the draft report on June 23, 2023. The objective of the audit was to determine whether the FDIC has an effective strategy and governance processes to manage its cloud computing services.

We are pleased that, overall, the OIG found the FDIC had an effective strategy and governance processes to manage its cloud computing services. As detailed in the draft report, the OIG determined that the FDIC had effective controls in place for a majority of the areas assessed pertaining to application rationalization, information technology (IT) governance bodies' alignment with cloud risks, cloud expenditures, cloud workforce transformation, assessment and authorization, continuous monitoring, and business continuity. However, the report also noted that the FDIC did not adhere to several cloud-related practices recommended by the Office of Management and Budget, National Institute of Standards and Technology, and FDIC guidance in the areas of data governance, cloud exit strategy, contract management plans, and decommissioning plans for legacy systems.

The draft report contains nine recommendations, six of which are addressed to the Chief Information Officer and the remaining three to the Director of the Division of Administration (DOA). FDIC management concurs with the recommendations. Notably, the Chief Information Officer Organization (CIOO) and DOA have already initiated action to address many of the report's recommendations, and in one case has completed corrective actions. A summary of management's planned and completed corrective actions and associated milestones follows.

Recommendation 1

We recommend that the CIOO:

1. Develop and maintain an inventory and catalog of all FDIC data used throughout the cloud data lifecycle.

1

FDIC Federal Deposit Insurance Corporation

Management Decision: Concur

Corrective Action: The CIOO continues to make strategic improvements in data management, including the recent procurement of a software tool to establish an enterprise-wide inventory and catalog of FDIC data. Once the CIOO operationalizes the tool this year, the CIOO will begin loading metadata into it. The CIOO will also document a process for populating and maintaining data (including data in the cloud) in the inventory and catalog.

Estimated Completion Date: February 15, 2024

Recommendation 2

We recommend that the CIOO:

2. Establish and implement data governance requirements (e.g., policies, processes, roles and responsibilities) for managing data residing in the cloud.

Management Decision: Concur

Corrective Action: The CIOO will review its existing data policies, processes, and other governance controls and expand upon them by establishing and implementing appropriate enterprise governance requirements for managing data in the cloud.

Estimated Completion Date: September 27, 2024

Recommendation 3

We recommend that the CIOO:

3. Establish an exit strategy for all cloud-based systems.

Management Decision: Concur

Corrective Action: The CIOO will document the FDIC's cloud exit strategy as part of the 2027 Target State Architecture.

Estimated Completion Date: September 15, 2023

Recommendation 4

We recommend that the Director, DOA:

4. Develop and implement Contract Management Plans for contract actions, including contracts, basic ordering agreements, and related task orders as required by FDIC policy.

Management Decision: Concur

Corrective Action: ASB will identify contract actions that require a Contract Management Plan (CMP) in accordance with FDIC policy and will ensure CMPs have been created and uploaded into the CeFile.

Estimated Completion Date: December 31, 2023

Recommendation 5

We recommend that the Director, DOA:

5. Provide additional training to Contracting Officers and Oversight Managers to emphasize the requirement to develop Contract Management Plans for contract actions, when appropriate.

Management Decision: Concur

Corrective Action: DOA's Acquisition Services Branch (ASB) conducted training on the requirement to develop CMPs during an all-hands meeting for Contracting Officers on June 29, 2023. The training materials will also be provided to all Oversight Managers via email.

Estimated Completion Date: August 30, 2023

Recommendation 6

We recommend that the Director, DOA:

6. Develop and implement policies and procedures to regularly review contract actions to confirm Contract Management Plans are put in place.

Management Decision: Concur

Corrective Action: In March 2023, ASB created a Quality Assurance and Internal Controls Program. The program includes a documented plan that requires quarterly reviews of various procedural, documentation and contract clause requirements, including CMPs. Quarterly reviews were conducted in the 1st and 2nd quarter of 2023 and final reports were distributed to ASB leadership.

Estimated Completion Date: Completed on June 26, 2023

Recommendation 7

We recommend that the CIOO:

7. Update the Project Management Lifecycle and/or System Development Life Cycle frameworks to include a Disposal phase and process.

Management Decision: Concur

Corrective Action: The CIOO will update the System Development Life Cycle (SDLC) and the Project Management Lifecycle (PMLC) frameworks to address the disposal and decommissioning of legacy systems.

Estimated Completion Date: June 28, 2024

Recommendation 8

We recommend that the CIOO:

8. Develop and implement policies and procedures for overseeing the decommissioning of legacy systems.

   Management Decision: Concur

   Corrective Action: FDIC Policy Directive 1300.07, *Governance of Information Technology Resources* (dated June 29, 2020), states that the FDIC will acquire and manage IT in compliance with the FDIC's published SDLC and IT Project Management (Life Cycle) Framework as they evolve and mature. Further, CIOO Policy 09-004, *CIOO Policy on Information Technology Project Management* (dated August 3, 2022), requires CIOO portfolios, programs, and projects to adhere to the principals in the SDLC and PMLC. When the CIOO modifies the SDLC and PMLC to address the disposal and decommissioning of legacy systems as described in our response to Recommendation 7, the two referenced policies will ensure the modifications are implemented. The CIOO will supplement the revisions to the SDLC and PMLC with procedures to guide the decommissioning and disposal of legacy systems.

   Estimated Completion Date: June 28, 2024

Recommendation 9

We recommend that the CIOO:

9. Review all current and planned system replacements and ensure legacy system decommissioning plans are created in accordance with FDIC policies and procedures.

   Management Decision: Concur

   Corrective Action: The CIOO will review current and planned legacy system replacements to ensure decommissioning plans exist in accordance with the updated SDLC, PMLC, and related procedures.

   Estimated Completion Date: September 30, 2024

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 CIOO continues to make strategic improvements in data management, including the recent procurement of a software tool to establish an enterprise-wide inventory and catalog of FDIC data. Once the CIOO operationalizes the tool this year, the CIOO will begin loading metadata. The CIOO will also document a process for populating and maintaining data (including data in the cloud) in the inventory and catalog.	February 15, 2024	$0	Yes	Open
2	The CIOO will review its existing data policies, processes, and other governance controls and expand upon them by establishing and implementing appropriate enterprise governance requirements for managing data in the cloud.	September 27, 2024	$0	Yes	Open
3	The CIOO will document the FDIC's cloud exit strategy as part of the 2027 Target State Architecture.	September 15, 2023	$0	Yes	Open
4	ASB will identify contract actions that require a CMP in accordance with FDIC policy and will ensure CMPs have been created and uploaded into the CEFile.	December 31, 2023	$0	Yes	Open
5	ASB conducted training on the requirement to develop CMPs during an all-hands meeting for Contracting Officers on June 29, 2023. The training materials will also be provided to all Oversight Managers via email.	August 30, 2023	$0	Yes	Open
6	In March 2023, ASB created a Quality Assurance and Internal Controls Program. The program includes a documented plan that requires quarterly reviews of various procedural, documentation and contract clause requirements, including CMPs. Quarterly reviews were conducted in the 1st and 2nd quarter of 2023 and final reports were distributed to ASB leadership.	June 26, 2023	$0	Yes	Open
7	The CIOO will update the System Development Life Cycle (SDLC) and the Project Management Lifecycle	June 28, 2024	$0	Yes	Open

	(PMLC) frameworks to address the disposal and decommissioning of legacy systems.				
8	FDIC Policy Directive 1300.07, *Governance of Information Technology Resources* (dated June 29, 2020), states that the FDIC will acquire and manage IT in compliance with the FDIC's published SDLC and IT Project Management [Life Cycle] Framework as they evolve and mature. Further, CIOO Policy 09-004, *CIOO Policy on Information Technology Project Management* (dated August 3, 2022), requires CIOO portfolios, programs, and projects to adhere to the principles in the SDLC and PMLC. When the CIOO modifies the SDLC and PMLC to address the disposal and decommissioning of legacy systems as described in our response to Recommendation 7, the two referenced policies will ensure the modifications are implemented. The CIOO will supplement the revisions to the SDLC and PMLC with procedures to guide the decommissioning and disposal of legacy systems.	June 28, 2024	$0	Yes	Open
9	The CIOO will review current and planned legacy system replacements to ensure decommissioning plans exist in accordance with the updated SDLC, PMLC, and related procedures.	September 30, 2024	$0	Yes	Open

[a] Recommendations are resolved when —

1. Management concurs with the recommendation, and the OIG agrees the planned corrective action is consistent with the recommendation.
2. Management does not concur or partially concurs with the recommendation, but the OIG agrees that the proposed corrective action meets the intent of the recommendation.
3. For recommendations that include monetary benefits, management agrees to the full amount of OIG monetary benefits or provides an alternative amount and the OIG agrees with that amount.

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

Federal Deposit Insurance Corporation
Office of Inspector General

3501 Fairfax Drive
Room VS-E-9068
Arlington, VA 22226

(703) 562-2035

★★★★★★

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

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