Governance of the FDIC's Mobile Device Management Solution

December 2020 **AUD-21-002**

Audit Report

Information Technology Audits and Cyber

☆☆☆☆☆☆☆☆

Integrity☆Independence☆Accuracy☆Objectivity☆Accountability

Office of Inspector General

Executive Summary

Governance of the FDIC's Mobile Device Management Solution

The Federal Deposit Insurance Corporation (FDIC) relies heavily on mobile devices to support its critical business operations and communications. For example, FDIC staff use mobile devices (smartphones and tablets) to access sensitive information, including personally identifiable information, on the internal network, and to exchange emails on bank examinations, bank closings, human resources issues, and other business activities.

The FDIC uses a cloud-based mobile device management (MDM) solution to secure and manage its smartphones and tablets. On October 4, 2019, the FDIC awarded a contract valued at $965,000 to replace its MDM solution with a new MDM solution (proposed MDM solution). However, in November 2019, the FDIC decided to terminate its contract for the proposed MDM solution because the FDIC could not validate whether the proposed MDM solution would satisfy the FDIC's security requirements.

The objective of the audit was to assess the adequacy of the FDIC's governance over the proposed MDM solution. The audit focused on the FDIC's actions to evaluate, authorize, procure, and subsequently terminate its contract for the proposed MDM solution.

Results

We found that the FDIC's Chief Information Officer Organization (CIOO) coordinated with the necessary IT governance bodies and the Office of the Chief Information Security Officer (OCISO) to evaluate the proposed MDM solution. However, the CIOO did not:

- Identify elevated and growing risks associated with the proposed MDM solution in reports describing the health and status of the project that were provided to CIOO Executives and other FDIC stakeholders;
- Resolve security concerns identified by the OCISO prior to procuring the proposed MDM solution; or
- Establish roles and responsibilities in its procedures for managing the use of Limited Authorizations to Operate (ATO).

In addition, the FDIC's Acquisition Services Branch did not engage the Legal Division to review the procurement of the proposed MDM solution consistent with FDIC guidance. The FDIC ultimately terminated the contract for the proposed MDM solution in response to security concerns and incurred unnecessary costs. In addition to internal and contractor resources expended on the project, the FDIC compensated the vendor $343,533 for the proposed MDM solution. The FDIC never used the solution for which it had signed a contract to purchase.

Recommendations

Our report contains five recommendations. We recommend that the FDIC reinforce guidance and provide training to staff on the effective identification, assessment, and prompt reporting of project risks. In addition, we recommend that the FDIC require the concurrence of security and privacy officials prior to submitting a procurement package for new technologies to the Acquisition Services Branch. By implementing this recommendation, the FDIC can achieve funds put to better use of $361,533. Further, we recommend that the FDIC clarify roles and responsibilities related to the review and assessment of security requirements for new technologies and guidance regarding the use of Limited ATOs. Finally, we recommend that the FDIC clarify expectations regarding the role of the Legal Division in reviewing procurements involving subscriptions. The FDIC concurred with all five recommendations and plans to complete corrective actions by August 31, 2021. Management also agreed that the FDIC could achieve funds put to better use in the future if it implements Recommendation 2.

Contents

Background **2**

Roles and Responsibilities 2

Timeline of Events 5

Audit Results **7**

Project Risks Not Reported to CIOO Management 7

Award of Contract Notwithstanding Significant Security Concerns 11

Guidance for Limited ATOs Warrants Clarification 13

Legal Review of Proposed MDM Procurement Not Performed 15

FDIC Comments and OIG Evaluation **16**

Appendices

1. Objective, Scope, and Methodology 18
2. Acronyms and Abbreviations 21
3. Quick Reference Guide for Project Health Ratings 22
4. FDIC Comments 23
5. Summary of the FDIC's Corrective Actions 27

Tables

1. Analysis of Changes in Project Milestones 9
2. Internal Controls and Principles Assessed 18

Figures

1. Timeline for the Proposed MDM Solution 6
2. Reported Project Status and Health for the Proposed MDM Solution (October 23, 2019) 8

December 21, 2020

Subject | ***Governance of the FDIC's Mobile Device Management Solution***

The Federal Deposit Insurance Corporation (FDIC) relies heavily on mobile devices to support critical business operations and communications. For example, FDIC executives, managers, and staff use mobile devices (smartphones and tablets) to access sensitive information (including personally identifiable information) on the internal network, as well as to exchange emails on bank examinations, bank closings, human resources issues, and other business activities. It is, therefore, vitally important that the FDIC properly secure and manage these mobile devices.

The FDIC uses a cloud-based mobile device management (MDM)[1] solution to secure and manage its smartphones and tablets. On October 4, 2019, the FDIC awarded a contract valued at $965,000 to replace its existing MDM solution with a new MDM solution (referred to herein as the proposed MDM solution). In November 2019, the FDIC decided to terminate its contract for the proposed MDM solution because the FDIC could not validate whether the proposed MDM solution would satisfy the FDIC's security requirements. In February 2020, the FDIC agreed to compensate the vendor $343,533 for terminating the contract.

The objective of the audit was to assess the adequacy of the FDIC's governance over the proposed MDM solution. The audit focused on the FDIC's actions to evaluate, procure, authorize, and subsequently terminate its contract for the proposed MDM solution. We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 of this report provides additional details about our objective, scope, and methodology; Appendix 2 contains a list of acronyms and abbreviations; Appendix 3 contains a Quick Reference Guide for rating the health of FDIC IT projects; and Appendix 4 and Appendix 5 contain the FDIC's comments on this report and a summary of the FDIC's corrective actions.

[1] An MDM solution is a software application used to remotely manage and secure mobile devices.

BACKGROUND

The FDIC's Chief Information Officer Organization (CIOO) uses the MDM solution to perform a number of important information technology (IT) functions for its smartphones and tablets. For example, the CIOO uses the MDM solution to connect these mobile devices to the FDIC's internal network, monitor the security and configuration settings on the devices, and wipe the devices when users report them as lost or stolen. The MDM solution also secures certain FDIC applications, such as Email, Calendar, Contacts, Documents, and Tasks, in an encrypted container on the mobile devices. A personal identification number, known only to the user, protects access to the container.

In August 2019, the CIOO designated a team of employees, herein referred to as the Project Team, to manage the selection of an alternative MDM solution to meet the FDIC's business needs. At that time, the CIOO had determined that the existing MDM solution could not provide important capabilities. For example, the MDM solution did not offer a single sign-on capability[2] that would facilitate user access to IT applications. According to the CIOO, the limitations with the MDM solution negatively affected the user experience when using the mobile devices.

The Project Team conducted market research and identified a proposed MDM solution that could provide greater functionality over the existing MDM solution and resolve the limitations described above. The Project Team established a schedule to install the proposed MDM solution on smartphones by December 31, 2019. This timeframe aligned with a separate CIOO initiative to distribute new smartphones to the FDIC's workforce by the end of 2019. By aligning the schedules for both initiatives, the CIOO intended to minimize inconvenience to employees by installing the proposed MDM solution on the smartphones before providing the smartphones to the employees.

Roles and Responsibilities

From August 2019 through October 2019, the Project Team took steps to secure internal FDIC approval for the proposed MDM solution and implement a procurement. Specifically, the Project Team coordinated with: (1) IT governance bodies for technical approvals, (2) the Office of the Chief Information Security Officer (OCISO)[3] for security approval, and (3) the Division of Administration's (DOA) Acquisition Services Branch (ASB) for the acquisition of the proposed MDM solution.

[2] According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations* (September 2020), single sign-on enables users to log in only once to gain access to multiple information system resources.
[3] OCISO is a group of information security and privacy professionals within the CIOO. OCISO's mission is to provide enterprise-wide information security and privacy programs that assure integrity, confidentiality, and availability of FDIC information by proactively protecting IT assets.

IT Governance Bodies

The CIOO created various IT governance bodies to review and approve new technologies and changes to existing technologies within the FDIC's environment. These governance bodies include the Security and Enterprise Architecture Technical Advisory Board (SEATAB), Engineering Review Board (ERB), Change Advisory Board (CAB), and Change Control Board (CCB). These governance bodies serve to ensure that new or changed technologies align with the FDIC's established technical guidance and standards. As described later, the Project Team coordinated with these IT governance bodies to obtain their approval to move forward with acquiring the proposed MDM solution.

Security and Enterprise Architecture Technical Advisory Board. In February 2018, the CIOO established the SEATAB in response to an Office of Inspector General (OIG) audit of the FDIC's IT governance structure.[4] Our prior audit found that the FDIC had not established sufficiently robust governance over its IT initiatives or implemented an effective Enterprise Architecture (EA)[5] to guide its IT initiatives. According to its charter, SEATAB serves as the overall governance body for the FDIC's EA, and as the initial gateway for any new technology introduced into the FDIC's environment.

Engineering Review Board. In February 2013, the CIOO established the ERB to approve, prioritize, and allocate resources for engineering projects managed by the Division of Information Technology's (DIT),[6] Infrastructure Services Branch. The ERB reviews and evaluates proposed IT infrastructure projects, and conducts milestone reviews of the projects as they progress through the development lifecycle. As part of its work, the ERB ensures that project teams complete necessary activities and project management documentation.

Change Control Board and Change Advisory Board. In April 2009, the CIOO established the CCB, which is responsible for reviewing and approving changes needed to the FDIC's IT infrastructure. To obtain CCB approval, the CAB must first review and approve the project. In April 2009, the CIOO established the CAB as a working group that reviews technical designs and infrastructure changes for IT projects as they progress through the project development lifecycle. The CAB advises the CCB on the technical impacts and risks of infrastructure changes.

---

[4] OIG Report, *The FDIC's Governance of Information Technology Initiatives* (AUD-18-004) (July 2018). Our office made eight recommendations to improve IT governance at the FDIC. As of December 7, 2020, our office had closed seven of the eight recommendations.

[5] According to the Office of Management and Budget (OMB) Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016) (OMB Circular A-130), an EA consists of an agency's baseline architecture, target architecture, and transition plan to attain the target architecture.

[6] DIT is a component office within the CIOO that has responsibility for providing innovative, timely, reliable, and secure IT services to the FDIC.

The CCB establishes processes for reviewing and approving changes to the IT infrastructure and the technical architecture, a subcomponent of the EA, to ensure that project teams adequately plan, communicate, and coordinate changes.

OCISO and the Authorizing Official

OMB Circular A-130 requires Federal agencies to develop and maintain system security plans (SSP) for their information systems. SSPs document the security controls in the system and describe the implementation of those controls. Because the proposed MDM solution met the definition of an information system, the Project Team was required to work with the Governance Risk and Compliance Section (GRC)—a component within the OCISO—to develop an SSP.

Many FDIC stakeholders rely on SSPs when making important risk management decisions. For example, the FDIC's Authorizing Official relies on SSPs (together with other information describing the security state of information systems) to authorize systems to operate and to determine whether to accept the associated residual risk.[7] In addition, the OCISO uses SSPs to plan and conduct assessments of the effectiveness of system security and privacy controls as required by the Federal Information Security Modernization Act of 2014. Therefore, properly documenting the security controls for the proposed MDM solution in an SSP was critically important for supporting a decision on whether to authorize the solution to operate in the FDIC's IT environment.

NIST SP 800-37, Revision 2,[8] states that Authorizing Officials may issue an ATO or an Interim Authority to Test when authorizing their information systems to operate. FDIC guidance refers to an Interim Authority to Test as a Limited ATO. FDIC guidance allows the CIO to issue either type of authorization.

ATO. According to NIST SP 800-37, Revision 2, Authorizing Officials may issue an ATO after reviewing a system authorization package. The system authorization package contains various security risk management documents, such as an SSP, privacy plan, results of security and privacy control assessments, and plans of action and milestones (POA&Ms).[9] NIST SP 800-37,

[7] OMB Circular A-130 requires Federal agencies to authorize their information systems to operate. A senior management official (the Authorizing Official) reviews security-related information describing the security posture of systems, and using that information, determines whether the risk to mission/business operations is acceptable. If the Authorizing Official determines that the risk is acceptable, then the official explicitly accepts the risk. The Chief Information Officer (CIO) serves as the FDIC's Authorizing Official.
[8] NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations* (December 2018). The FDIC has taken the position that relevant NIST SPs contain statements of best practices or guidance and are generally not binding on the FDIC. The CIOO has incorporated NIST SP 800-37, Revision 2, into its internal operating policies.
[9] A POA&M is a corrective action plan for managing the resolution of information system security and privacy weaknesses. POA&Ms detail the required resources to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Revision 2, states that the Authorizing Official uses this information to determine whether the mission/business risk of operating a system or providing common controls[10] is acceptable. If the Authorizing Official determines that the risk is acceptable, the Authorizing Official explicitly accepts the risk. Once the Authorizing Official makes this decision, the system becomes operational in a live environment.

Limited ATO. According to NIST SP 800-37, Revision 2, Authorizing Officials may issue a Limited ATO to allow the operation of a system only for a short period of time if it is necessary to test the system in the operational environment before all security controls are in place. In this case, the duration of the ATO is limited to the time needed to complete security control testing. When issuing a Limited ATO, the Authorizing Official may choose to implement certain conditions, such as increased monitoring of the system or limitations on the number of users who can access the system.

Procurement

Prior to November 2019, the CIOO's Office of CIO Management Services developed, coordinated, and executed IT acquisition functions for the CIOO.[11] The Office of CIO Management Services also coordinated with DOA's ASB to implement procurement actions. When ASB receives a procurement package from the CIOO, ASB handles the contract solicitation, award, and administration.

Timeline of Events

A timeline of key events from the inception of the proposed MDM solution through its termination follows.

- **August 20, 2019.** The Project Team sought and obtained SEATAB approval for the proposed MDM solution. SEATAB's approval indicated that the proposed MDM solution aligned with the FDIC's EA and security architecture.

- **September 5, 2019.** The Project Team submitted a final procurement package to the Office of CIO Management Services.

- **September 12, 2019.** The Office of CIO Management Services submitted the procurement package to ASB.

[10] Common controls are controls inherited by one or more IT systems.
[11] In November 2019, FDIC management approved a plan to reorganize the CIOO. As part of the reorganization, a new CIO Acquisition Strategy and Innovation Branch was created within the CIOO to strengthen IT acquisition and planning. In the months that followed, the CIOO transitioned staff and resources from the former Office of CIO Management Services to the CIO Acquisition Strategy and Innovation Branch. The CIOO completed these transition activities by April 2020.

- **September 18, 2019.** The Project Team presented the proposed MDM solution to the ERB, and obtained the ERB's approval to proceed on the same date.

- **September 24, 2019.** The CAB completed its review of the design, configuration, and functional requirements of the proposed MDM solution, and provided its approval for the project to proceed on the condition that the Project Team complete several required tasks.

- **October 3, 2019.** The Project Team presented the proposed MDM solution to the CCB. On the same day, the CCB approved the baseline configuration and infrastructure changes for the proposed MDM solution. However, the CCB conditioned its approval by stating that the proposed MDM solution needed to receive an ATO in the FDIC's IT environment prior to implementing any changes to the FDIC's IT infrastructure.

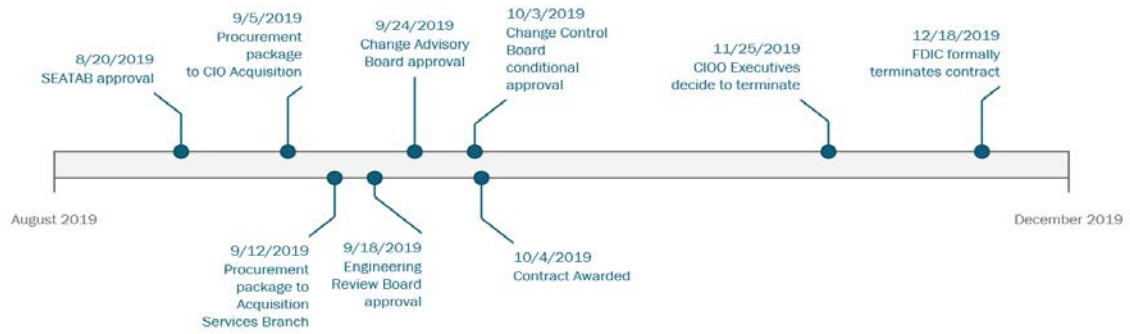
- **October 4, 2019.** ASB awarded a contract to purchase 5,000 subscriptions[12] of the proposed MDM solution covering a 1-year period at a cost of $965,000.

- **November 25, 2019.** CIOO Executives decided to terminate the contract for the proposed MDM solution due to security concerns.

- **December 18, 2019.** ASB sent a Notice of Termination to the vendor. The FDIC agreed to compensate the vendor $343,533. This amount reflected a proration for the number of months that the FDIC had access to the 5,000 subscriptions and associated vendor support.

Figure 1 summarizes the key events described above.

Figure 1: Timeline for the Proposed MDM Solution



Source: OIG analysis of CIOO documentation.

[12] The contract for the proposed MDM solution was for 5,000 user subscriptions for Software as a Service. Software as a Service allows a user to utilize a third party's infrastructure to access software applications.

AUDIT RESULTS

We found that the Project Team coordinated with the necessary IT governance bodies and OCISO to evaluate the proposed MDM solution. However, the CIOO did not:

- Identify elevated and growing risks associated with the proposed MDM solution in reports describing the health and status of the project that were provided to CIOO Executives and other FDIC stakeholders;
- Resolve security concerns identified by the OCISO prior to procuring the proposed MDM solution; or
- Establish roles and responsibilities in its procedures for managing the use of Limited ATOs.

In addition, ASB did not engage the Legal Division to review the procurement of the proposed MDM solution consistent with FDIC guidance. The FDIC ultimately terminated the contract for the proposed MDM solution in response to security concerns and incurred unnecessary costs. In addition to internal and contractor resources expended on the project, the FDIC compensated the vendor $343,533 for the proposed MDM solution. The FDIC never used the solution for which it signed a contract to purchase.

Project Risks Not Reported to CIOO Management

OMB Circular A-130 requires Federal agencies to implement appropriate processes, standards, and policies to govern their IT resources. According to OMB A-130, these requirements include measurements to evaluate the cost, schedule, and overall performance of IT projects. Further, the FDIC's internal guidance for project managers states that identifying, analyzing, and responding to risks that arise over the lifecycle of a project will help the project remain on track and meet its objectives.[13]

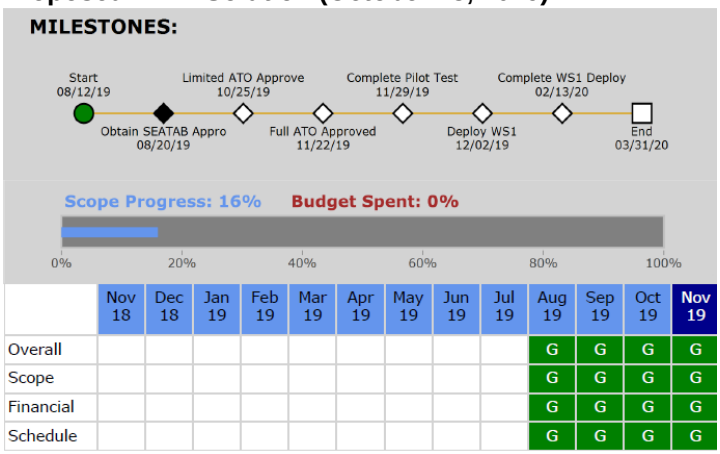
Project teams within the CIOO track and communicate the status, health, and risk of their IT projects to CIOO Executives and other FDIC stakeholders through Weekly Status Reports. The Program Management Office (PMO)[14] within the CIOO developed a Quick Reference Guide (See Appendix 3) and other guidance

[13] Risk Manager Guidance (February 2020) developed by the FDIC's Division of Finance, Risk Management and Internal Controls.
[14] The PMO provides high-level oversight of key IT initiatives within the CIOO and serves as a resource for FDIC personnel engaged in the operations and oversight of IT projects. In addition, the PMO provides guidance and standards for IT projects.

materials[15] to help ensure that project teams uniformly apply health ratings and report information in Weekly Status Reports in a consistent manner. The Weekly Status Reports contain project health ratings based on a color-coded traffic light protocol (Green, Yellow, and Red). These ratings reflect the overall health of the project, and its scope, finance, and schedule components. According to the PMO's guidance, the Weekly Status Reports should include a justification to explain the ratings, a description of risks jeopardizing projects, and the expected future performance of projects.

We found that the Weekly Status Reports for the proposed MDM solution did not reflect elevated and growing security risks associated with the project. The status report reflected in Figure 2 shows that the Project Team consistently reported the overall status and health of the project (including the associated scope, financial, and schedule components) as Green.[16] However, elevated and growing security concerns with the project were present in September 2019. Specifically, by late September 2019, GRC staff had advised the Project Team that a significant number of security controls in the SSP lacked a description of how security controls were implemented. GRC needed this information to conduct a security control assessment of the proposed MDM solution. Without a complete security control assessment, the CIO could not authorize the proposed MDM solution to operate.

Figure 2: Reported Project Status and Health for the Proposed MDM Solution (October 23, 2019)



Source: Weekly Status Report as of October 23, 2019 reflecting the current and future health ratings and performance.

In October 2019, GRC attempted to obtain documentation for the security controls from the vendor of the proposed MDM solution. However, the vendor could not provide security documentation at a level of detail that would allow GRC to determine how the security controls were implemented. Without documented security controls, the Project Team and GRC were unable to assess the security controls for the

[15] The PMO's guidance provides standard descriptions for completing and reporting the overall status of projects, as well as assigning scope, financial, and schedule health ratings.
[16] According to the PMO's Quick Reference Guide, an overall health rating of Green indicates that the effort is performing and delivering the agreed-upon scope and expects to continue to perform according to plan.

proposed MDM solution. The Weekly Status Reports did not identify the difficulties associated with documenting the security controls. During the month of October 2019, the Project Team extended the project milestone for obtaining a Limited ATO four times. In its last Weekly Status Report for October 2019, the Project Team removed the milestone for obtaining a Limited ATO and added a new milestone to research alternative solutions by November 29, 2019. Table 1 describes how the Project Team continually extended milestones in the Weekly Status Reports.

Table 1: Analysis of Changes in Project Milestones

Weekly Status Report Date	OIG Analysis
October 3, 2019	• No mention that the Project Team missed the October 1st milestone for obtaining a Limited ATO. • Milestone for obtaining a Limited ATO extended to October 7th.
October 10, 2019	• No mention that the Project team missed the October 7th milestone for obtaining a Limited ATO. • Milestone for obtaining a Limited ATO extended to October 11th. • Key accomplishments and planned activities remained the same.
October 17, 2019	• No mention that the Project Team missed the October 11th milestone for obtaining a Limited ATO. • Milestone for obtaining a Limited ATO extended to October 18th. • Key accomplishments and planned activities remained the same.
October 24, 2019	• No mention that the Project Team missed the October 18th milestone for obtaining a Limited ATO. • Milestone for obtaining a Limited ATO extended to October 25th. • Key accomplishments and planned activities remained the same.
October 31, 2019	• No mention that the Project Team missed the October 25th milestone for obtaining a Limited ATO. • The Project Team removed milestones for obtaining a Limited ATO. • The Project Team established a new milestone of November 29th to research alternative solutions.

Source: OIG review of Weekly Status Reports for the proposed MDM solution for the month of October 2019.

During November 2019, at the request of CIOO Executives, the Project Team began researching alternative solutions in response to GRC's identification of security concerns with the proposed MDM solution. On November 25, 2019, the Project Team presented CIOO Executives with three alternatives.[17] Rejecting these alternatives, CIOO Executives decided to terminate the project. However, the Project Team continued to report the overall health and status of the project as Green in the Weekly Status Report for December 5, 2019.

Members of the Project Team stated that they continued to report the status and health of the project as Green, because they did not receive information from GRC

[17] The options included replacing the subscriptions purchased by the FDIC with a version of the vendor's MDM solution authorized by the Federal Risk and Authorization Management Program (FedRAMP). During November 2019, the vendor was pursuing FedRAMP authorization for a version of its MDM solution. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

regarding potential delays in obtaining a Limited ATO until mid-November 2019. Our review of CIOO email correspondence, however, found that GRC security officials had notified the Project Team members of these concerns as early as September 2019. For example, a GRC representative sent an email to the CISO on September 23, 2019, that contained a chronology of events associated with the proposed MDM solution. This chronology showed that GRC informed the Project Team on multiple occasions that the Project Team had not sufficiently documented security controls in the SSP. However, just 11 days later, on October 4, 2019, ASB awarded the contract for the proposed MDM solution. Subsequently, on October 17, 2019, the CISO sent an email to other CIOO Executives stating:

> *At this point, we've only been able to validate 5% of the control implementation assertions. With that, and considering the pace at which the evidence and access has been provided to date, a full ATO by 11/15 is not likely.*

If project teams do not effectively identify, assess, and promptly communicate project risks, the FDIC may not undertake risk mitigation measures, and projects may experience delays and cost overruns. The lack of effective risk identification in the Weekly Status Reports for the proposed MDM solution created a perception that the project was performing consistent with expectations, when in fact it was not. Accurate reporting of risks for this project could have allowed CIOO management to take risk mitigation actions earlier in the project's lifecycle. For example, CIOO management could have delayed the procurement of the proposed MDM solution until the Project Team and GRC resolved the security risks. CIOO management also could have terminated the contract for the proposed MDM solution sooner than it did, reducing costs to the FDIC.

Without accurate reporting of project risk information, CIOO Executives cannot effectively manage risks consistent with the FDIC's Risk Appetite and Risk Tolerance levels,[18] or assess whether risks warrant consideration at an enterprise level.[19] In the case of the proposed MDM solution, CIOO management did not include the project's risks in the FDIC's Risk Inventory or Risk Profile.[20] The lack of accurate risk information prevented CIOO management from considering the project's risk in the context of other IT risks for potential inclusion in the Risk Inventory and Risk Profile.

[18] OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (OMB Circular A-123, July 2016), states that Risk Appetite serves as a guidepost to establish strategy and select objectives and a Risk Tolerance. OMB Circular A-123 states that Risk Tolerance is the acceptable level of variance in performance relative to the achievement of objectives.

[19] The FDIC has established an Enterprise Risk Management (ERM) Program to manage risks across the organization. The CIOO developed the *Information Security Risk Management Guide* (July 2018) which states that the CIOO will follow ERM Program guidance for Risk Appetite, Risk Profiles, and Risk Tolerance.

[20] The Risk Inventory refers to a list of risks facing the agency. The Risk Profile is a prioritized inventory of significant risks identified and assessed by an agency through its risk assessment process.

Recommendation

We recommend that the CIO:

1. Reinforce guidance and provide training on the need for effective identification and assessment of IT project risks, and the prompt and accurate reporting of such risks.

Award of Contract Notwithstanding Significant Security Concerns

NIST SP 800-37, Revision 2, recommends that agencies use the NIST Risk Management Framework to integrate system security and privacy requirements into the acquisition process. To address these requirements, agencies must develop and approve an SSP that describes the system's security and privacy controls and their implementation.[21] Agencies use the information in the SSP to help inform officials regarding necessary security and privacy requirements that must be resolved in the acquisition process.

Throughout September 2019, the Project Team worked to develop an SSP for the proposed MDM solution so that GRC could assess the security and privacy controls and pursue a Limited ATO from the Authorizing Official. GRC raised concerns to the Project Team on multiple occasions regarding the lack of documented security controls in the SSP. On September 23, 2019, a GRC representative notified the CISO that GRC had informed the Project Team that:

> *7 of the FDIC Critical Security Controls[22] are described as not in place. . . This includes access control, boundary protection, configuration management, contingency planning, vulnerability scanning and identification and authentication. A review of their SSP also shows 125 other controls are being implemented by [the vendor] but there is no description of how.*

On September 26, 2019, a GRC representative stated that there were "too many unknowns to recommend authorization." This statement referred to the lack of security control documentation in the SSP that prevented GRC from assessing controls and recommending authorization of the proposed MDM solution. The GRC representative further recommended that the Project Team use a FedRAMP

[21] OMB Circular A-130 states that agencies shall develop and maintain security plans and privacy plans for an information system that provide an overview of the security and privacy requirements for the information system and describe the security and privacy controls in place or planned for meeting those requirements.
[22] According to CIOO policy, *Security Control Assessment Methodology* (August 2019), critical security controls have significant impact on the FDIC's mission, critical assets, sensitive data and/or other systems across the enterprise with potential for magnitude of harm to the FDIC by an attacker if not appropriately implemented.

authorized version of the proposed MDM solution once a FedRAMP version became available. Despite these concerns, the Project Team decided to continue its efforts to develop the SSP by meeting with the vendor directly in an attempt to obtain needed security documentation. However, these efforts were not successful. The Project Team did not notify ASB of the security concerns, and on October 4, 2019, ASB awarded a contract for the proposed MDM solution.

The CIOO's policies and processes for acquiring new technologies did not require the concurrence of the OCISO prior to submitting a procurement package to ASB for award. Such a control would ensure that the CIOO fully considers security risks associated with new technologies before initiating a procurement. In the case of the proposed MDM solution, the CIOO moved forward with the procurement of a new technology even though significant concerns had been identified regarding the FDIC's ability to verify whether the technology could meet the FDIC's security requirements.

A control requiring OCISO concurrence prior to procuring new technologies would also help ensure that all stakeholders are aware of potential security concerns. ASB procurement officials pursued an award for the proposed MDM solution without knowledge of the security concerns. Had all stakeholders been aware of the security concerns, the FDIC may not have procured 5,000 user subscriptions for 12 months. If instead, the FDIC had established a Memorandum of Understanding (MOU) with the vendor, this vehicle would have allowed the CIOO to assess a small number of subscriptions on a test basis, without awarding a contract. An MOU can protect the FDIC should it find a product unsuitable for its IT environment, such as when a product may introduce an unacceptable level of security risk. Had the FDIC utilized an MOU in this manner, the FDIC could have: (a) avoided the purchase of 5,000 subscriptions for a product that lacked necessary security control documentation; (b) reduced the costs it incurred in attempting to document the security controls, rescind the procurement, and review the settlement proposal from the vendor; and (c) eliminated the compensation it paid to the vendor to terminate the procurement.

The FDIC can reduce the risk of spending unnecessary funds by implementing a control that requires the OCISO's concurrence prior to submitting procurement packages for new technologies to ASB. Had this control been in place, the FDIC could have identified the security issue before awarding a contract, thereby avoiding costs of $361,533. This figure is based on the termination payment ($343,533) and payments made to a contractor after OCISO had already identified security concerns ($18,000). If the FDIC takes action to implement Recommendation 2 below, it could avoid similar instances of unnecessary spending on future IT procurements and put at least $361,533 to better use.

Further, based on our interviews, members of the Project Team, Office of CIO Management Services, and ASB did not have a clear understanding of the roles that SEATAB and GRC play with respect to evaluating security for new technologies. Some individuals had the perception that SEATAB's approval of the proposed MDM solution meant that it was feasible to implement in the FDIC's IT environment. However, SEATAB's approval of the proposed MDM solution meant only that it aligned with the FDIC's EA and security architecture. SEATAB's review and approval of the proposed MDM solution was just one part of the FDIC's process to evaluate whether the technology met the FDIC's security requirements. GRC had a separate role to assess the effectiveness of the proposed MDM solution's security and privacy controls and identify the associated risk. The results of GRC's work serves as input to the Authorizing Official in deciding whether to authorize the technology to operate in the FDIC's IT environment.

Recommendations

We recommend that the CIO:

2. Establish and implement a control that requires the concurrence of security and privacy officials prior to submitting a procurement package for new technologies to the Acquisition Services Branch. [Estimated funds put to better use of $361,533.]

3. Clarify and communicate the roles and responsibilities of SEATAB and GRC with respect to security requirements for new technologies.

Guidance for Limited ATOs Warrants Clarification

NIST Federal Information Processing Standard (FIPS) Publication 200[23] states that policies and procedures play an important role in the effective implementation of enterprise-wide information security programs within the Federal government. According to NIST FIPS Publication 200, agencies must develop and promulgate documented policies and procedures governing the minimum security requirements set forth in the standard, including authorizing information systems to operate. Further, NIST SP 800-53, Revision 4,[24] states that organizations should develop,

[23] NIST FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006), defines minimum security requirements for Federal information and information systems. FIPS is mandatory standard under the Federal Information Security Modernization Act of 2014. However, it is the FDIC's position that FIPS 200 is not binding on the FDIC because the Secretary of Commerce, who approved FIPS 200, does not have the authority to impose mandatory requirements on the FDIC. Nevertheless, the FDIC views the document as guidance for "best practices" in implementing security measures for information systems.

[24] NIST SP 800-53, Revision 4, provides guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the Federal government to meet the requirements of FIPS 200.

document, and disseminate security authorization policies, as well as procedures to facilitate their implementation.

The CIOO had developed guidance to support the authorization of systems to operate in the FDIC's IT environment.[25] In June 2020, during the course of the audit, the CIOO expanded this guidance by issuing the *FDIC System Security Authorization Process Guide* (Authorization Guide). The Authorization Guide provides stakeholders with an overview of the security authorization process and serves as the standard operating procedure for achieving authorizations to operate for new systems.

In addition to defining a process for issuing ATOs, the Authorization Guide also allows for the issuance of Limited ATOs. The Authorization Guide states that a Limited ATO is:

> *[A] temporary, condition bound authorization to facilitate early adoption of technologies and solutions that the FDIC has not yet fully implemented. This method provides the Authorizing Official with a risk-based approach to tailor control implementation and assessment requirements in order to support urgent and time-sensitive business objectives.*

The Authorization Guide presents a broad description of conditions that may warrant the issuance of a Limited ATO. However, the Authorization Guide does not define who has responsibility for deciding whether "urgent and time-sensitive business objectives" exist to justify pursuing a Limited ATO. The Authorization Guide also does not define who has responsibility for deciding how security controls will be tailored to support a Limited ATO. In the case of the proposed MDM solution, there was confusion among Project Team members and GRC regarding the expectations and requirements for achieving a Limited ATO.

A representative of GRC stated that the Authorization Guide does not include roles and responsibilities for Limited ATOs because GRC anticipates a limited need for this type of authorization in the future. However, clarifying roles and responsibilities for Limited ATOs would establish clear accountability and expectations for all FDIC stakeholders. Clarified guidance would also help to ensure proper, consistent, and disciplined implementation of processes supporting Limited ATOs.

[25] Such guidance includes the *Information Security Risk Management Guide: Systems and Applications* (July 2018) and the *ISM Program Technical Guide for Stakeholders* (updated March 2020). The CIOO has also developed templates for completing SSPs, Security Profiles, and Security and Privacy Impact Analyses. This guidance and these templates address information on lead times for processing various types of ATOs, frequently asked questions, required authorization paths for cloud services, and NIST standards.

Recommendation

We recommend that the CIO:

4. Clarify roles and responsibilities for authorizing the use of Limited ATOs and the associated security control tailoring.

Legal Review of Proposed MDM Procurement Not Performed

The FDIC's Acquisition Policy Manual (APM), and the accompanying Acquisition Procedures, Guidance, and Information (PGI), contain guidance for obtaining legal reviews of FDIC procurement documents and actions. The FDIC Legal Division conducts these legal reviews to help ensure that procurements comply with governing laws and FDIC policy. Section 5.1503 of the PGI includes a Legal/Acquisition Participation Agreement (Participation Agreement)[26] that defines the working relationship between ASB and the Legal Division's Contracting and Leasing Group (CLG). The Participation Agreement also establishes standard operating procedures for requesting and conducting legal reviews. According to the Participation Agreement, ASB will engage CLG in all stages of the acquisition lifecycle.

The Participation Agreement requires Contracting Officers in ASB to engage CLG to review all procurement actions with a total estimated value greater than $1 million, and any other procurement matter having the potential to set legal precedent or raise novel or complex legal issues. The Participation Agreement states that regardless of dollar value, the Contracting Officer will request a legal review by CLG for subscription agreements.[27] The contract for the proposed MDM solution included, among other items, 5,000 user subscriptions. However, ASB did not request a legal review of the proposed MDM solution until after the FDIC decided to terminate the contract.

A representative of ASB stated that ASB did not request a legal review of the proposed MDM solution prior to the Solicitation (Request for Proposals) because ASB did not believe a legal review was required. The ASB representative stated that a legal review of the solicitation would have been required only if the vendor proposed a separate written agreement that included software license or subscription terms and conditions. In contrast, a representative of CLG informed us that ASB should have engaged the Legal Division during ASB's development of the Request for Proposals for the proposed MDM solution. The CLG representative stated that the circumstances warranted legal review, because the procurement involved a

[26] The Participation Agreement became effective on July 31, 2019. The FDIC incorporated the Participation Agreement into the PGI in June 2020.
[27] PGI Appendix F, Section IV. B., *General Coordination Guidance for Acquisition Actions*.

subscription agreement. The CLG representative explained that vendors may not provide the FDIC with subscription terms and conditions when they submit their proposals. Instead, vendors may provide subscription terms and conditions when they deliver their IT product. The CLG representative added that CLG strives to review subscription terms and conditions prior to contract award.

CLG provides legal advice on procurements to protect the FDIC's legal and business interests. For example, CLG can review the terms and conditions of subscriptions, including usage and restrictions, to ensure they are acceptable to the FDIC. In addition, CLG can advise ASB on appropriate language to include in contracts to protect the FDIC's business interests. Further, the PGI provides an option for the FDIC to pursue an MOU with a vendor that would allow the FDIC to test and evaluate an IT product without having to execute a contract.[28]

It is important that ASB and the Legal Division have a common understanding of the Participation Agreement requirement for legal review of subscription agreements, including triggering events for ASB to engage the Legal Division during the acquisition process. Absent a common understanding, Contracting Officers may not consistently request legal reviews of procurement actions, resulting in inadequate consideration of the FDIC's legal and business interests in procurements.

Recommendation

We recommend that the Deputy to the Chairman and Chief Operating Officer and the General Counsel:

5. Clarify the intent and expectation of the Participation Agreement between the Legal Division and ASB regarding legal reviews of procurement actions involving subscriptions.

FDIC COMMENTS AND OIG EVALUATION

FDIC management provided a written response, dated December 18, 2020, to a draft of this report. The response is presented in its entirety in Appendix 4. In the response, management concurred with all five of the report's recommendations. Management also agreed that the FDIC could achieve funds put to better use in the future if it implements Recommendation 2. However, management stated that the actual amount of funds put to better use is unknown and will depend on future circumstances that cannot be accurately predicted.

[28] Section 2.105(e)(3) of the PGI.

All five recommendations will remain open until we confirm that corrective actions have been completed and are responsive. A summary of the FDIC's corrective actions is contained in Appendix 5.

Objective

The objective of the audit was to assess the adequacy of the FDIC's governance over the proposed MDM solution. We assessed the role of the FDIC's IT governance bodies, Project Team, and security staff in researching alternative MDM solutions and assessing the proposed MDM solution for fitness in the FDIC's IT environment and alignment with the EA. In addition, we reviewed the efforts of the Project Team and GRC to document and assess security controls for the proposed MDM solution. Further, we assessed the processes followed by the CIOO and DOA to procure the proposed MDM solution, and the factors that led to the CIOO's decision to terminate the contract for the proposed MDM solution.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We conducted the audit from January through September 2020.

Scope and Methodology

We assessed internal controls that we deemed to be significant to the audit objective. Specifically, we assessed 9 of the 17 principles associated within the 5 components of internal control defined in the Government Accountability Office's Standards for Internal Control in the Federal Government (September 2014) (Green Book). Table 2 summarizes the principles we assessed.

Table 2: Internal Controls and Principles Assessed

Control Environment
Principle 2 - Exercise Oversight Responsibility
Principle 3 - Establish Structure, Responsibility, and Authority
Risk Assessment
Principle 6 - Define Objectives and Risk Tolerance
Principle 7 - Identify, Analyze, and Respond to Risks
Control Activities
Principle 10 - Design Control Activities
Principle 12 - Implement Control Activities

Information and Communication
Principle 13 - Use Quality Information
Principle 14 - Communicate Internally
Monitoring
Principle 17 - Evaluate Issues and Remediate Deficiencies

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

We assessed the design, implementation, and/or operating effectiveness of internal controls and identified deficiencies that we believe could affect the FDIC's governance over the proposed MDM solution. The report presents the internal control deficiencies that we identified within the findings. Because we limited our audit to the principles presented above, it may not have disclosed all internal control deficiencies existing at the time of this audit. The following section provides details regarding the procedures we performed to conduct our audit and assess internal controls relevant to the audit objective.

To address the audit objective, we:

- Reviewed FDIC policies, procedures, processes, and guidance for conducting market research, procuring IT solutions, and terminating contracts;
- Reviewed FDIC policies, procedures, and guidance for documenting and assessing security controls, and granting ATOs and Limited ATOs;
- Reviewed the charters and other governance documentation for the SEATAB, ERB, CCB, and CAB, as well as proposals and other project documentation provided to these governance bodies pertaining to the proposed MDM solution;
- Examined documentation related to the FDIC's market research of alternative MDM solutions, and the award and termination of the proposed MDM solution contract;
- Examined IT security documentation related to the proposed MDM solution;
- Reviewed Weekly Status Reports provided by the PMO describing the status and health of the proposed MDM solution project; and
- Interviewed FDIC staff, including representatives of the Project Team, GRC, CIO Acquisition Strategy and Innovation Branch, ASB, Legal Division, SEATAB, and CCB to assess:

  - The requirements for conducting market research, submitting procurements to the CIO Acquisition Strategy and Innovation Branch and ASB, and terminating contracts;
  - The FDIC's efforts to document and assess security controls, and the process for issuing Limited ATOs and ATOs;
  - The purpose and requirements for presenting to SEATAB and CCB, as well as their roles and responsibilities;
- Reviewed relevant government-wide policy issued by OMB, and security standards and guidelines published by NIST.

In addition, we obtained and reviewed FDIC email correspondence related to the proposed MDM solution project to obtain a detailed understanding of the FDIC's actions and decision-making pertaining to the project. We obtained the email correspondence by requesting that the FDIC perform an email vault search[29] using names of employees and contractor staff who worked on the proposed MDM solution, together with search terms associated with the project. Our email vault search covered the period of August 1, 2019 through December 31, 2019. We exported the emails generated by the vault search into the FDIC's eDiscovery system for review.

[29] The FDIC stores emails in an Enterprise Vault in accordance with the FDIC's data retention and legal discovery requirements. The FDIC can search the Enterprise Vault for archived emails based on various search criteria, such as words, sender names, and dates.

Appendix 2 Acronyms and Abbreviations

APM	Acquisition Policy Manual
ASB	Acquisition Services Branch
ATO	Authorization to Operate
CAB	Change Advisory Board
CCB	Change Control Board
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
CLG	Contracting and Leasing Group
DIT	Division of Information Technology
DOA	Division of Administration
EA	Enterprise Architecture
ERB	Engineering Review Board
ERM	Enterprise Risk Management
FDIC	Federal Deposit Insurance Corporation
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
GRC	Governance Risk and Compliance Section
IT	Information Technology
MDM	Mobile Device Management
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OCISO	Office of the Chief Information Security Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PGI	Procedures, Guidance, and Information
PMO	Program Management Office
POA&M	Plans of Action and Milestones
SEATAB	Security and Enterprise Architecture Technical Advisory Board
SP	Special Publication
SSP	System Security Plan

PROJECT HEALTH RATING DEFINITIONS

Overall	Green: The effort is performing and delivering the agreed upon scope or definition of done. It is expected to continue to perform according to plan.	Yellow: The effort varies slightly from plan. It may be slightly over budget, slightly behind schedule or the outcome may not conform to minor aspects of agreed upon scope or definition of done. Corrective action(s) are underway to address the issues.	Red: The effort varies significantly from plan, likely to be over budget, behind schedule and/or the delivered scope will not conform to the expected outcome or definition of done. The effort needs immediate corrective action(s) and/or management involvement to resolve the issues.
Scope	Green: There is a high likelihood the agreed upon scope and objectives for the effort will be met, even if the project is experiencing minor schedule or financial issues.	Yellow: The agreed upon scope and objectives may not conform in minor aspects with quality expected. Corrective action(s) are underway.	Red: The agreed upon scope and objectives will not conform or the ability to successfully achieve the scope is in jeopardy given the quality required for the schedule and budget. Corrective action(s) are underway.
Schedule	Green: The project schedule for delivery of agreed upon scope is expected to be met or vary no more than 10% from the baseline end date. Critical path may have some slack and project is expected to meet any mandated dates.	Yellow: The project schedule is delayed in delivering agreed upon scope by no more than 15% from baseline end date. The critical path has limited slack. The project expects to meet any mandated dates. Corrective actions are underway.	Red: The project schedule is delayed in delivering agreed upon scope by more than 15% from the baseline end date. The critical path has no remaining slack and the project is expected to exceed a mandated date. Corrective actions are underway.
Financial	Green: The current planned spend is on target and within 10% of the total budget and the effort is not expected to require additional funding.	Yellow: The current planned spend varies between 10 to 15 percent of the total budget and additional funding above the defined budget may be needed to complete the effort. Corrective actions are underway.	Red: The current planned spend varies by more than 15 percent of the total budget and additional funding is needed to complete the effort. Corrective actions are underway.
Forecast	Green: During the next month, the effort is expected to be on track as planned for scope, schedule and/or financial components. Efforts to resolve issues yielding expected results.	Yellow: During the next month, the effort is expected to vary slightly from plan. Efforts will be underway to address issues and return to baseline for scope, schedule and/or financial.	Red: During the next month, the effort is expected to diverge significantly from plan. Efforts to resolve issues are not likely to yield expected results. Significant risks are materializing impacting the project's health.

12/2018

Source: FDIC's PMO Quick Reference Guide

FDIC

3501 Fairfax Drive, Arlington, VA 22226-3500 Chief Information Officer & Chief Privacy Officer

December 18, 2020

TO: Mark F. Mulholland
Assistant Inspector General for Audits

FROM: Sylvia Burns
Chief Information Officer and Chief Privacy Officer
Digitally signed by ZACHARY BROWN
Date: 2020.12.18 14:08:43 -05'00'

Arleas Upton Kea
Deputy to the Chairman and Chief Operating Officer
DANIEL BENDLER
Digitally signed by DANIEL BENDLER
Date: 2020.12.18 19:55:06 -05'00'

Zachary N. Brown
Chief Information Security Officer
ZACHARY BROWN
Digitally signed by ZACHARY BROWN
Date: 2020.12.18 14:00:30 -05'00'

Nicholas Podsiadly
General Counsel
NICHOLAS PODSIADLY
Digitally signed by NICHOLAS PODSIADLY
Date: 2020.12.18 17:43:30 -05'00'

SUBJECT: Management Response to the Draft Audit Report Entitled *Governance of the FDIC's Mobile Device Management Solution* (Assignment No. 2020-004)

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report on *The Governance of the FDIC's Mobile Device Management Solution* issued on November 20, 2020. The FDIC is committed to maintaining effective governance processes while evaluating, procuring, and authorizing contracts such as the mobile device security solution.

The OIG made five recommendations intended to strengthen the effectiveness of governance practices. FDIC management concurs with the report's findings and is committed to addressing each of the OIG's recommendations by designated timeframes. In the interim, the FDIC has taken additional steps to strengthen governance practices to prevent re-occurrence of the OIG's findings.

For example, the CIOO has established and is in the process of fully implementing a centralized demand management function. Demand management will be tightly integrated with the Project and Portfolio Management team to improve data driven decisions about project requests, strengthen reporting on the IT portfolio and individual projects, and enhance transparency and coordination with Divisions and Offices. CIOO has also established a new Secretariat function to document and provide reporting on CIOO governance decisions, including collecting and publishing CIOO performance data.

Additionally, the CIOO continues to strengthen processes that integrate information security and privacy throughout the system development lifecycle through implementation of processes that are aligned to the National Institute of Standards and Technology (NIST) Risk Management Framework and the Corporation's broader information security and privacy program. Finally, the newly created CIO Acquisition Strategy and Innovation Branch continues to introduce processes that strengthen controls associated with information technology (IT) acquisitions and vendor oversight as the CIOO strives to provide modern, efficient and secure solutions that enhance the Corporation's IT operating environment and operational efficiencies.

We appreciate your staff's time and effort, and we expect that the FDIC actions already in progress and refinements that are responsive to this draft report will further improve governance processes. Responses to each recommendation are below:

MANAGEMENT RESPONSE

Recommendation 1 –

We recommend that the CIO/CPO:

1. Reinforce guidance and provide training on the need for effective identification and assessment of IT project risks, and the prompt and accurate reporting of such risks.

   Management Decision: Concur

   Corrective Action: The FDIC will brief IT project teams and other stakeholders to reinforce guidance regarding the need for effective identification and assessment of IT project risks along with prompt and accurate reporting of such risks.

   Estimated Completion Date: 8/31/21

Recommendation 2 –

We recommend that the CIO/CPO:

2. Establish and implement a control that requires the concurrence of security and privacy officials prior to submitting a procurement package for new technologies to the Acquisition Services Branch. [Estimated funds put to better use of $361,533.]

   Management Decision: Concur

Corrective Action: CIOO will develop and implement an acquisition planning guide to include controls which require concurrence of security and privacy officials prior to awarding a contract for new technologies.

Note: Management agrees that $361,533 could have been put to better use by avoiding the termination payment to the vendor ($343,533) and payments made to a contractor after OCISO had already identified security concerns ($18,000). Management also agrees that, by implementing Recommendation 2, the FDIC may achieve funds put to better use in the future; however, the actual amounts of such funds is unknown and will depend on future circumstances that cannot be accurately predicted.

Estimated Completion Date: 6/30/2021

Recommendation 3 –

We recommend that the CIO/CPO:

3. Clarify and communicate the roles and responsibilities of SEATAB and GRC with respect to security requirements for new technologies.

Management Decision: Concur

Corrective Action: The FDIC will include GRC as a voting member of SEATAB and communicate the updated responsibilities to all relevant stakeholders.

Estimated Completion Date: 7/31/21

Recommendation 4 –

We recommend that the CIO/CPO:

4. Clarify roles and responsibilities for authorizing the use of Limited ATOs and the associated security control tailoring.

Management Decision: Concur

Corrective Action: The CIOO will update the System Security Authorization Process guide to add specific guidelines on Limited ATOs.

Estimated Completion Date: 3/31/2021

Recommendation 5 –

We recommend that the Deputy to the Chairman and Chief Operating Officer and the General Counsel:

5. Clarify the intent and expectation of the Participation Agreement between the Legal Division and ASB regarding legal reviews of procurement actions involving subscriptions.

Management Decision: Concur

Corrective Action: The DOA/ASB will work with the Legal Division/Contracts and Risk Management Unit to discuss, mutually agree, and formally document legal reviews of procurement actions involving subscriptions.

Estimated Completion Date: 3/31/2021

If you have any questions regarding this response, please contact Montrice Yakimov, Chief, IT Risk Governance and Policy, Enterprise Strategy Branch, at 877-275-3342.

cc: E. Marshall Gentry, Deputy Director, DOF, Risk Management and Internal Controls Branch
Stephen Beard, Deputy Director, Division of Administration

Summary of the FDIC's Corrective Actions

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

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The FDIC will brief IT project teams and other stakeholders to reinforce guidance on the need for effective identification and assessment of project risks, as well as prompt and accurate reporting of such risks.	8/31/2021	$0	Yes	Open
2	The FDIC will develop and implement an acquisition planning guide to include controls requiring concurrence from security and privacy officials prior to awarding a contract for new technologies.	6/30/2021	$361,533	Yes	Open
3	The FDIC will include GRC as a voting member of the SEATAB and communicate updated responsibilities to all stakeholders.	7/31/2021	$0	Yes	Open
4	The FDIC will update the System Security Authorization Process guide to address guidelines for Limited ATOs.	3/31/2021	$0	Yes	Open
5	ASB, the Legal Division, and Risk Management Unit will discuss, mutually agree, and document legal reviews of procurement actions involving subscriptions.	3/31/2021	$0	Yes	Open

[a] Recommendations are resolved when —

1. Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.
2. Management does not concur with the recommendation, but alternative action meets the intent of the recommendation.
3. Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an 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	Twitter	OVERSIGHT.GOV ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE
www.fdicoig.gov	@FDIC_OIG	www.oversight.gov/