The FDIC's Governance of Information Technology Initiatives

July 2018 **AUD-18-004**

Audit Report

Information Technology Audits and Cyber

☆☆☆☆☆☆☆☆

Integrity☆Independence☆Accuracy☆Objectivity☆Accountability

Office of Inspector General

Executive Summary

The FDIC's Governance of Information Technology Initiatives

The Federal Deposit Insurance Corporation (FDIC) relies extensively on information technology (IT) to accomplish its mission of insuring deposits, supervising insured financial institutions, and resolving the failure of insured financial institutions. The FDIC must subject its IT initiatives to appropriate governance and oversight. IT governance provides organizations such as the FDIC with a structured process to support IT investment decisions while promoting accountability, due diligence, and the efficient and economic delivery of IT services. Without effective IT governance, negative results can occur, such as investments that do not align with the FDIC's mission, goals, or objectives; information systems that do not satisfy stakeholder needs; and IT projects that do not meet cost, schedule, or performance expectations.

Federal statutes and Office of Management and Budget policy require agencies to establish and implement fundamental components of IT governance. These components include IT strategic planning, which defines the overall direction and goals for the agency's IT program, and an enterprise architecture (EA), which describes the agency's existing and target architecture and plan to achieve the target architecture. The FDIC's Chief Information Officer (CIO) has primary responsibility for IT governance within the agency. The FDIC's IT governance structure consists of a Governance Framework that includes the IT Strategic Plan and EA and Governance Processes that include oversight bodies and controls that govern IT projects, programs, or initiatives.

The objective of the audit was to identify key challenges and risks that the FDIC faces with respect to the governance of its IT initiatives. The audit focused on key components of the FDIC's IT governance–strategic IT planning, EA, and governance bodies and practices–as applied to three IT initiatives: (1) the migration of email operations to the cloud; (2) the deployment of laptop computers to FDIC employees and contractor personnel; and (3) the potential adoption of a managed services solution for mobile IT devices.

Results

The FDIC faced a number of challenges and risks with respect to its governance of IT initiatives. The FDIC had neither fully developed a strategy to migrate IT services and applications to the cloud nor obtained the acceptance of key business stakeholders before taking steps to initiate cloud projects. The FDIC also had not implemented an effective EA to guide either the three IT initiatives we reviewed or

the FDIC's broader transition of IT services to the cloud. An ineffective EA limited the FDIC's ability to communicate to business stakeholders how it intended to implement its new IT strategies. In turn, this caused stakeholders to question the decision to adopt new cloud technologies and their impact on their business processes.

The FDIC had not completed needed changes to its IT Governance Processes to ensure that sufficiently robust governance applied to all of its IT initiatives. We found that two of the three IT initiatives we reviewed would have benefited from more robust governance. In both cases, the FDIC established aggressive implementation schedules without first obtaining broad business stakeholder involvement in the early stages of the initiatives' lifecycles.

With respect to information security, the FDIC had not established an enterprise security architecture or adequately defined the roles and responsibilities of security officials in its IT governance structure. For two of the three IT initiatives we reviewed, the FDIC did not meet its planned implementation dates, in part, because it had not adequately addressed IT security concerns during the early phases of the initiatives. Further, the FDIC had not acquired needed resources and expertise to improve its IT Governance Framework and support adoption of cloud solutions. In addition, the FDIC did not use complete cost information or fully consider intangible benefits when evaluating cloud solutions.

Recommendations

We recommended that the CIO (1) coordinate with FDIC stakeholders to develop an implementation plan that supports the IT Strategic Plan; (2) incorporate cloud strategy principles into the IT Governance Framework; (3) implement an EA as part of the IT Governance Framework and use the EA to guide IT decision-making; (4) revise the FDIC's Governance Processes, including roles and responsibilities for governance bodies; (5) incorporate revisions to IT Governance Processes into applicable FDIC policies, procedures, and charters; (6) define and document roles and responsibilities for information security within the IT Governance Framework and Processes; (7) identify and document the IT resources and expertise needed to execute the IT Strategic Plan; and (8) define and document procedures for evaluating the costs and potential benefits associated with cloud projects.

In a written response to the report, the CIO Organization concurred with all eight recommendations. The CIO Organization stated that it completed actions to address six of the recommendations and plans to complete actions to address the remaining two recommendations by June 28, 2019.

Contents

July 26, 2018

Howard G. Whyte
Chief Information Officer and Chief Privacy Officer

Subject | ***The FDIC's Governance of Information Technology Initiatives***

The Federal Deposit Insurance Corporation (FDIC) relies extensively on information technology (IT) to accomplish its mission of insuring deposits, supervising insured financial institutions, and resolving the failure of insured financial institutions. During 2017, the FDIC allocated about $330 million (15 percent) of its budget for IT equipment, services, and projects. The FDIC also budgeted over $20 million for IT application development in its business divisions and offices. The FDIC must ensure that it manages its IT expenditures appropriately and in accordance with appropriate governance and oversight.

On June 8, 2016, the Office of Inspector General raised concerns with the FDIC regarding its governance over a number of planned and ongoing IT initiatives, including the deployment of laptop computers and a move to vendor-managed cloud technologies, including whether:

- The initiatives had reasonable schedules and could be successfully executed within the proposed timeframes;
- There had been adequate project planning, including ensuring that those responsible for carrying out the activities had engaged stakeholders;
- Benefits and risks had been fully assessed;
- Sufficient organizational resources existed to support the initiatives;
- New security risks would be introduced and addressed; and
- Policies and procedures were being followed, including those associated with the governance of IT projects.

In December 2016, the OIG initiated this audit to examine the FDIC's governance of recent IT initiatives, including the deployment of laptop computers and components of the FDIC's planned move to vendor-managed cloud technologies. This audit also summarizes the results of our work to review the FDIC's use of its enterprise

architecture[1] (EA) and strategic IT planning techniques in response to concerns raised by the Chairman of the Senate Committee on Banking, Housing, and Urban Affairs regarding FDIC's breach response activities.

The objective of the audit was to identify key challenges and risks that the FDIC faces with respect to the governance of its IT initiatives. The audit focused on key components of the FDIC's IT governance – strategic IT planning, EA, and governance bodies and practices – as applied to three IT initiatives: (1) the migration of email operations to the cloud; (2) the deployment of laptop computers to FDIC employees and contractor personnel; and (3) the potential adoption of a managed services solution for mobile IT devices.[2]

We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 includes additional details about our objective, scope, and methodology; Appendix 2 contains a glossary of terms; Appendix 3 contains a list of acronyms; and Appendix 4 contains the FDIC's comments. Appendix 5 contains a summary of the Corporation's corrective actions.

Background

The IT Governance Institute[3] described IT governance as the leadership and organizational structures and processes to ensure that IT functions and operations sustain the organization's business strategies and mission objectives. IT governance provides organizations with a structured decision-making process underlying IT investment decisions and promotes accountability, due diligence, and the efficient and economic delivery of IT services. When an organization does not maintain effective governance over its IT functions and operations, it can lead to negative results, including investments that do not align with the organization's mission, goals, or objectives; information systems that do not satisfy stakeholder needs; and IT projects that do not meet cost, schedule, or performance expectations. In turn, organizations such as the FDIC lose accountability for IT decision-making and limit their ability to achieve cost savings, efficiencies, and drive improvements in the delivery of IT services.

[1] Certain terms that are underlined when first used in this report are defined in Appendix 2, *Glossary of Terms*.
[2] The FDIC terminated the initiative relating to managed services for mobile devices during the course of our audit work.
[3] *See* IT Governance Institute, *Board Briefing on IT Governance*, 2nd Edition. The IT Governance Institute is a nonprofit corporation that conducts research on global IT governance practices. The organization helps leaders understand how effective governance can assist in ensuring that IT supports business goals, optimizes IT-related business investment, and appropriately manages IT-related risks and opportunities.

The Government Accountability Office (GAO) recognized the management of IT acquisitions and operations as a high-risk area for the entire federal government.[4] The GAO further noted that the federal government has spent billions of dollars on failed IT investments, because many of these investments suffered from a lack of disciplined and effective management, program oversight, and governance. According to the GAO, "executive-level governance and oversight across the government has often been ineffective, specifically from Chief Information Officers (CIOs)."

Federal Laws Governing IT Functions

The FDIC is a government corporation, and as such, laws, government-wide policies, and standards that apply to other federal agencies do not always apply to the FDIC. In such instances, the FDIC may voluntarily adopt certain concepts and principles. Those laws, policies, and standards that define the term "agency" to include government corporations and independent regulatory agencies apply to the FDIC. In the following sections, we identify laws, policies, and standards related to IT governance and discuss their applicability to the FDIC.

The Clinger-Cohen Act,[5] enacted in 1996, provides the impetus for the IT governance processes in use at federal agencies today. The Clinger-Cohen Act expanded upon the IT management requirements established by the Paperwork Reduction Act of 1980 as amended (PRA),[6] and defined new responsibilities for the OMB to improve the acquisition, use, and disposal of IT by the federal government.

The Clinger-Cohen Act also assigned responsibilities to agency heads, such as establishing a capital planning and investment control process to govern IT investments. Further, the statute defined additional responsibilities for CIOs, including implementation of a sound and integrated IT architecture, controls over system development risks, management of IT spending, and improvements in agency performance through information resources.

Enacted in 2014, the Federal Information Technology Acquisition Reform Act (FITARA)[7] sought to improve IT acquisition by federal agencies and hold them

[4] *See* GAO Report, *High Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others* (Feb. 2017).
[5] Pub. L. No. 104-106, 110 Stat. 186 (Feb. 10, 1996). The Clinger-Cohen Act applies to executive branch agencies, which does not include the FDIC. However, the FDIC has applied the concepts and principles of the statute to its capital planning, EA, and spending processes for IT.
[6] Pub. L. No. 96-511, 94 Stat. 2812 (Dec. 11, 1980), *amended by* Pub. L. 104-13, 109 Stat. 184 (May 22, 1995). The PRA provided the Office of Management and Budget (OMB) with policy-setting and oversight duties including, for example, the acquisition and use of automatic data processing and telecommunications equipment (information technology). The PRA also required agencies to carry out their information resources management (IRM) activities in an efficient, effective, and economical manner, and to comply with OMB policies and guidelines. To facilitate these objectives, the PRA required agency heads to designate a senior official who would report directly to the agency head in carrying out these responsibilities at the agency.
[7] Pub. L. No. 113-291, 128 Stat. 3292, 3438-50 (Dec. 19, 2014). The FDIC is not subject to the provisions of FITARA. However, the former CIO recommended that its provisions be considered when developing solutions to meet FDIC's IT priorities.

accountable for reducing duplication and achieving cost savings. Among other things, FITARA required CIOs to play a significant role in the decision-making process for IT budgeting, and in the management, governance, and oversight processes for IT. Accordingly, agency CIOs play a key leadership role in establishing and implementing effective IT governance.

OMB Policy and Guidance

On July 28, 2016, OMB issued a revised Circular A-130, *Managing Information as a Strategic Resource*,[8] which established overall policy for the planning, budgeting, governance, acquisition, and management of federal information resources. OMB Circular A-130 directed federal agencies, including the FDIC, to establish and implement fundamental components of IT governance that are critical to the success of any IT program, including:

IT Strategic Planning. Agencies must develop and maintain an IT Strategic Plan that describes the agency's technology and information resources goals. In addition, the IT Strategic Plan must support the goals of the agency's strategic plan required by the Government Performance and Results Modernization Act of 2010 (GPRA Modernization Act),[9] and demonstrate how the technology and information resources goals relate to the agency's mission and organizational priorities.

IT strategic planning is important because it defines the overall direction for an organization's IT program; links ongoing and planned IT initiatives to long term IT, security, and business goals and priorities; and facilitates efforts to measure progress relative to established goals and expectations. Strategic planning further helps to ensure that resources are directed toward priority areas.

Enterprise Architecture. Agencies must develop an EA that describes the agency's baseline architecture, target architecture, and a transition plan to attain the target architecture. An EA is critical to the successful implementation of an organization's IT Strategic Plan because the EA defines the roadmap and sequencing plan for executing IT initiatives throughout the organization. An EA also helps an organization eliminate waste and duplication in IT. OMB Circular A-130 requires agencies to ensure that their EA aligns with the agency's IT Strategic Plan and business and technology resources to achieve strategic outcomes.

[8] The FDIC has concluded that OMB Circular A-130, dated July 28, 2016, is generally applicable to the FDIC, and the FDIC should generally adhere to it, subject to certain caveats. These caveats include: (a) that the FDIC submits its budget to OMB for informational purposes, not approval; (b) the FDIC's statutory mission or requirements take precedence when OMB's instructions conflict with FDIC independence and supervisory authority; and (c) the Federal Information Technology Reform Act, one of the statutes in support of OMB's authority under OMB Circular A-130, is not legally binding to the FDIC, although voluntary compliance can be considered.

[9] Pub. L. No. 111-352, 124 Stat. 3866 (Jan. 4, 2011).

In May 2012, OMB issued *The Common Approach to Federal Enterprise Architecture*, which defined an overall approach that agencies can use to develop and apply an EA. The publication states, in part:

> Just as the blueprints of a building are the authoritative reference for how the structure will function, the organization's enterprise-wide architecture provides an integrated, consistent view of strategic goals, mission and support services, data and enabling technologies across the entire organization, including programs, services, and systems. When EA is recognized as the authoritative reference for the design and documentation of systems and services, issues of ownership, management, resourcing, and performance goals can be resolved in a more consistent and effective manner. EA also serves as a reference to promote the achievement and maintenance of desired levels of security and trust in an Agency's business and technology operating environment.

In addition, on January 29, 2013, OMB issued its *Federal Enterprise Architecture Framework*, Version 2, which described how agencies can implement *The Common Approach to Federal Enterprise Architecture*.[10] The *Federal Enterprise Architecture Framework* identified information security as a core component of an EA. According to the National Institute of Standards and Technology (NIST), the security architecture describes the structure and behavior of an organization's security processes, information security systems, personnel and organizational subunits, and shows their alignment with the organization's mission and strategic plans.[11]

The GAO also concluded that a well-defined EA is important to an organization.[12] When employed with other management disciplines, such as strategic planning and human capital management, an EA can increase the likelihood of configuring an organization to promote agility and responsiveness and address federal initiatives, such as leveraging cloud computing. Conversely, the GAO noted that ineffective utilization of EA can result in IT systems that are duplicative, poorly integrated, and costly to maintain and interface.

The FDIC's IT Governance Structure

IT governance encompasses two principal elements: a Governance Framework and Governance Processes.[13] The first element, Governance Framework, consists of

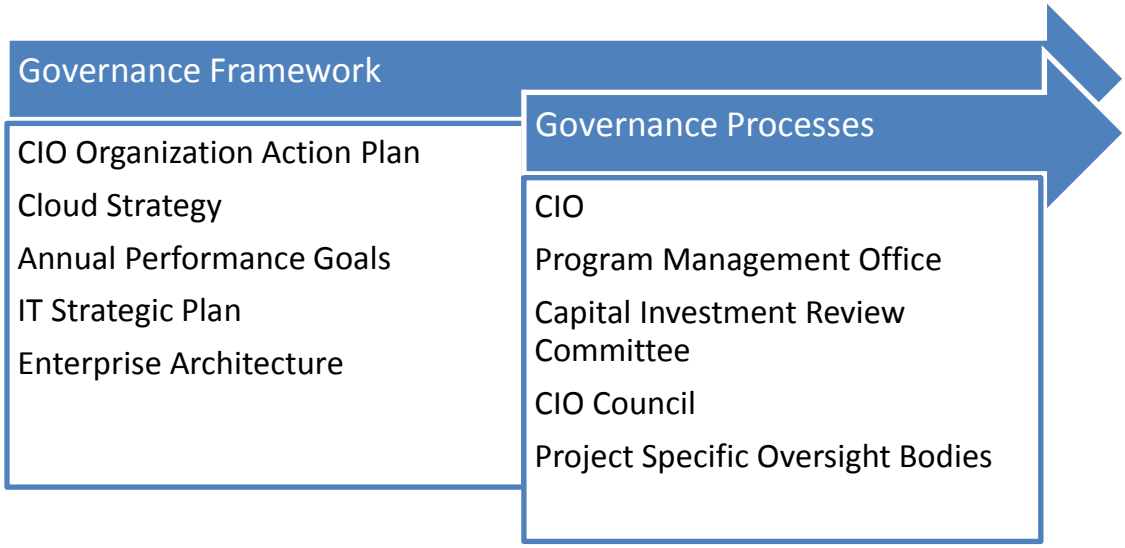
[10] The FDIC has determined that while *The Common Approach to Federal Enterprise Architecture* and *Federal Enterprise Architecture Framework* are not binding on the FDIC, it will establish and maintain its EA consistent with federal requirements to the extent that the EA requirements do not infringe upon the independence of the FDIC.
[11] *See* NIST Special Publication 800-39, *Managing Information Security Risk* (March 2011).
[12] *See* GAO Report, *Enterprise Architecture Use across the Federal Government Can Be Improved* (Feb. 2002).
[13] Gartner, Inc. (Gartner), *Practical Governance*, originally published Nov. 1, 2010 and revised Sept. 24, 2016.

multiple components, including the organization's IT Strategic Plan and EA, and it reflects the goals and priorities of the organization.

The second element of IT governance, Governance Processes, consists of: (i) standing processes that make routine IT decisions related to capital investments, portfolio management, and strategic planning and prioritization; and (ii) controls used to govern individual IT projects, programs, or transformations.

The FDIC's CIO has primary responsibility for establishing and implementing an IT governance structure within the organization. Figure 1 illustrates the key components of the FDIC's IT governance structure at the time of our audit.

Figure 1: Components of the FDIC's IT Governance Structure



Source: OIG analysis of IT governance documentation

FDIC Governance Framework

From late 2015 through early 2017, the FDIC developed four components within its Governance Framework: (i) a CIO Organization Action Plan; (ii) a high-level Cloud Strategy; (iii) Annual Performance Goals; and (iv) an IT Strategic Plan. The FDIC also worked to mature a fifth component of its Governance Framework, the EA.

CIO Organization Action Plan

In November 2015, the FDIC hired a new CIO (referred to herein as the former CIO). At that time, FDIC staff were working to update the FDIC's previous IT Strategic Plan (*2013–2017 Business Technology Strategic Plan*). This former CIO decided to postpone this ongoing update and instead establish a short-term action plan. The former CIO believed that there were "urgent security risks," which required

"immediate attention" to establish fundamental IT capabilities and mitigate security risks.

On June 28, 2016, the FDIC implemented the CIO Organization's Action Plan (2016 Action Plan). The Action Plan contained four objectives and three cross-cutting themes. The objectives focused on: (i) instituting the use of personal identity verification (PIV) cards to provide secure access to FDIC data; (ii) providing employees with laptops and other devices to improve workforce mobility; (iii) strengthening continuity of operations capabilities; and (iv) delivering innovative solutions to enhance business capabilities. The cross-cutting themes aimed at (i) maintaining a strong cybersecurity posture; (ii) improving communication; and (iii) delivering cost-optimized solutions that fully supported FDIC employees in meeting the FDIC's mission.

Figure 2: 2016 Action Plan Objectives and Themes

Objectives	**Access Control** **The FDIC uses personal identity verification enabled multi-factor authentication to provide access to information and data anytime, anywhere.**	**Mobility Managed Services** **Better devices and services enable employees to work from anywhere on FDIC-owned equipment at a reasonable cost.**	**Continuity of Operations** **FDIC mission essential business functions are operational within 12 hours of an adverse event.**	**Innovative Solutions** **Game changing ideas are introduced by technologists that rapidly interact, experiment, and deliver FDIC business capabilities.**
Themes	**Information Security** – All solutions are secure by design and cyber security risks are well understood and minimized.			
	Culture and Communication – There is a shared responsibility for IT delivery between business and IT, strong communication within the CIO Organization and outside, and high trust.			
	Operational Efficiency – Costs are optimized and well-categorized; policies and procedures are current; and work is identified, prioritized, funded, and tracked.			

Source: 2016 Action Plan (July 15, 2016)

The 2016 Action Plan introduced a fundamental shift in how the FDIC planned to deliver IT services and products. The FDIC CIO Organization had procured, developed, and maintained much of its IT services and products using on-premises solutions. The new 2016 Action Plan called for delivering IT services and products via cloud computing, whereby users access third party managed software, platforms, and technologies through the internet (rather than using the organization's servers). According to the 2016 Action Plan, commodity IT services, such as email and Microsoft SharePoint (an electronic document management and storage system), would be migrated to the cloud first. This step would be followed by moving the FDIC's primary data center from the FDIC's Virginia Square offices to a new

contractor owned and operated facility and then migrating applications to a shared services model.

Adopting a cloud approach was significant because it would require:

- An IT governance structure that addresses cloud strategies;
- An EA that addresses cloud standards, requirements, and roadmaps;
- Changes in procurement policies and procedures and contract oversight management and monitoring to address cloud solutions; and
- Staff with the appropriate knowledge, skills, and experience to develop and administer cloud contracts.

Cloud Strategy

The second component of the FDIC's Governance Framework is its Cloud Strategy. In January 2017, the former CIO issued a high-level document called "Cloud Strategy on a Page" to communicate to FDIC stakeholders that most of the FDIC's IT services and products would move to a cloud model. This Cloud Strategy was consistent with the 2016 Action Plan described above to move commodity services and then other applications to a shared services model. The former CIO believed that this approach would reduce costs and eliminate lengthy procurement and certification processes. In addition, the adoption of cloud solutions aligned with OMB's "Cloud First" policy, which directed federal agencies to adopt cloud technologies and increase the use of available cloud and shared services.[14] OMB, the Federal CIO Council, the Chief Acquisition Officers Council, and NIST each have issued guidance to support the acquisition of cloud services by federal agencies.

Annual Performance Goals

The third component of the FDIC's Governance Framework consists of Annual Performance Goals. On January 18, 2017, the then-Chairman announced the FDIC's Annual Performance Goals for 2017. Two of these goals supported the 2016 Action Plan and related Cloud Strategy to: (1) implement enhanced strategies for ensuring the security, confidentiality, integrity, and availability of the FDIC's automated information systems (Performance Goal 8), and (2) modernize and reduce the costs of delivering IT resources and services to FDIC employees while improving quality and customer satisfaction (Performance Goal 9). In order to implement these goals, the FDIC planned to:

[14] *See* OMB, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Dec. 9, 2010).

- Align the FDIC's EA with leading practices, the Federal Government's EA requirements, and FDIC mission requirements;
- Finalize an IT Strategic Plan for 2017-2020 that incorporates the 2016 Action Plan; and
- Continue implementation of the 2016 Action Plan including the use of shared services (*i.e.*, cloud computing) and the development and implementation of a Cloud Strategy that includes a transition plan and timetable for migrating IT services to the cloud.

IT Strategic Planning

The fourth component of the FDIC's Governance Framework is the IT Strategic Plan. Consistent with its *2017—2020 IT Strategic Plan* issued in June 2017*,* the FDIC seeks to:

- Review its IT governance structures and capabilities and develop them to provide effective direction and monitoring of existing and new IT investments;
- Review and update the role of its Capital Investment Review Committee (CIRC), CIO Council, and other governance bodies (described below in the Governance Processes section) to provide a coordinated IT decision-making process;
- Modernize and publish an EA, and communicate EA standards and requirements to its project managers to make the FDIC's entire IT portfolio easier to operate and maintain; and
- Improve the transparency of IT costs and performance, and review its IT development outsourcing strategies.

Enterprise Architecture

The fifth component of the FDIC's Governance Framework is EA. In June 2008, the FDIC issued a directive regarding EA principles, standards, guidelines, processes, models, and roadmaps. (FDIC Circular 1303.1, *FDIC Enterprise Architecture Program*).

FDIC Governance Processes

The CIO leads or oversees the CIRC, CIO Council, and Program Management Office (PMO)—three important standing governance bodies within the FDIC. The PMO has high-level oversight of all key CIO IT initiatives and establishes project management standards. The CIRC and CIO Council provide oversight of select IT initiatives that meet certain cost thresholds and funding requirements, or that are mission critical and/or high risk to the FDIC.

Table 1: Responsibilities of Key IT Governance Bodies

Governance Body	Responsibility
Program Management Office	The FDIC established the PMO in 2004 to improve the practice and results of the FDIC IT program and project management. The PMO, located within the Division of Information Technology (DIT), has high-level oversight over key CIO IT initiatives. The PMO 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 project management.
CIRC	The FDIC established the CIRC in 2003 to implement a systematic management review process that supports budgeting for the FDIC's capital investments and ensures regular monitoring and proper management of those investments, once funded. According to its charter, the CIRC reviews and oversees all major IT and non-IT investment initiatives with estimated capital outlays of more than $3 million, as well as certain other projects that cost less but are considered mission-critical and/or high risk to the FDIC. The CIRC determines whether these initiatives align with FDIC business requirements, provide substantial stakeholder involvement, meet cost and performance targets, mitigate IT security risks, and provide business value and technical compliance with the EA. The CIO and Chief Financial Officer co-chair the CIRC, and its members include the Chief Risk Officer, FDIC division directors, and the Director, Office of Complex Financial Institutions. As of December 31, 2017, there were three IT investments with a combined, multi-year investment budget of about $54.8 million subject to CIRC oversight.
CIO Council	The FDIC established the CIO Council in 2005 to advise the CIO on the adoption and use of IT at the FDIC. The Council reviews and recommends IT investments for the FDIC. The Council selects projects to enhance IT governance and reviews the progress of these projects to ensure they adhere to all governance guidelines. The CIO Council provides oversight for projects that generally cost less than $3 million and are funded by the CIO Council. The CIO chairs the CIO Council, and its 13 voting members include executive representatives for 12 FDIC divisions and offices and 6 regional offices. As of December 31, 2017, the CIO Council had oversight responsibilities for about $50.4 million in IT budget funds for Calendar Year 2017 and 19 IT development projects.

Source: OIG review of charters and other governance documentation

When an IT initiative does not meet the criteria for governance by the CIRC or CIO Council, the CIO Organization or sponsoring FDIC division(s) or office(s) establishes a project-specific governance structure. Such governance can include executive and project steering committees, project and program managers, risk managers, and cost, schedule, and performance reporting to senior management.

IT Initiatives Reviewed by the OIG

As part of this audit, we reviewed the IT governance applied to three IT initiatives started during 2016: (1) the migration of email operations to the cloud; (2) the deployment of laptop computers to FDIC employees and contractor personnel; and (3) the potential adoption of a third-party managed services solution for mobile IT devices. The FDIC initiated all three to accomplish one or more of its objectives in the 2016 Action Plan. None of these initiatives were subject to oversight by the CIRC or CIO Council.

Table 2: IT Initiatives Reviewed

IT Initiative	Description	Project Data
Email to the Cloud	On June 13, 2016, the CIO Organization initiated a project to migrate the FDIC's legacy email operations to the Microsoft Office 365 cloud computing platform. The project was part of a broader initiative to migrate other commodity IT services, such as Microsoft SharePoint to the cloud. The email to the cloud initiative was not subject to oversight by the CIRC or CIO Council because the CIO considered the project to be a technical refresh that was not high risk; estimated the cost of the project to be below $3 million; and funded the initiative through the CIO Organization's budget.	**Estimated Cost:** $345,631[a] **Governance:** CIO-led project steering and executive oversight committees with PMO oversight **Initial Planned Migration Date:** December 31, 2016 **Actual Completion Date:** September 19, 2017
Deployment of Laptop Computers	On June 1, 2016, the CIO Organization initiated a project to replace approximately 3,400 desktop computers located in the Washington, D.C. and regional offices with laptops computers. The CIO Organization purchased and deployed the laptop computers using expedited procedures. The deployment of laptop computers was not subject to oversight by the CIRC or CIO Council since the CIO Organization managed the project as a technical refresh of existing FDIC desktop computers.	**Estimated Cost:** $5,648,256[b] **Governance:** CIO and PMO oversight **Initial Planned Completion Date:** August 31, 2016 **Actual Completion Date:** June 9, 2017
Adoption of Mobile Managed Services	On January 2, 2016, the CIO Organization initiated a project to analyze the costs and feasibility of hiring a vendor to own, operate and manage the FDIC's mobile device portfolio. Devices covered under this initiative included laptops, iPhones and iPads. The CIO Organization terminated the Mobile Managed Services initiative in its early stages, as it was not cost-effective.	**Estimated Cost:** $12,883,703[c] **Governance:** CIO and PMO oversight **Initial Planned Completion Date:** December 14, 2017 **Actual Completion Date:** N/A

Source: OIG analysis of FDIC project documentation

[a] This figure represents the amount FDIC projected to pay a contractor to support its email migration and does not include FDIC internal costs.
[b] This figure includes $1,315,248 million in contractor surge labor costs to deploy laptop computers on an expedited basis (by August 31, 2016).
[c] This figure represents the estimated costs in excess of the projected status quo costs for maintaining the current service over a 5 year period.

Audit Results

We found that the FDIC faced a number of challenges and risks with respect to the governance of its IT initiatives. Specifically, the FDIC had not:

- Fully developed its strategy of migrating IT services and applications to the cloud prior to executing initiatives in support of its 2016 Action Plan, nor obtained the acceptance of organizational stakeholders across FDIC's divisions and offices;
- Implemented an effective enterprise architecture to govern its IT decision-making and guide the execution of its strategic goals and objectives;
- Completed needed revisions to its IT Governance processes to ensure that IT initiatives are subject to sufficiently robust governance;
- Established an enterprise security architecture or adequately defined the IT roles and responsibilities of information security officials within the Governance Framework and Governance Processes;
- Acquired the resources and expertise needed to improve its IT Governance Framework and support the implementation of its IT transformation in a timely manner; or
- Used complete cost information or fully considered intangible benefits when evaluating cloud solutions.

We found that these challenges and risks created uncertainty among corporate stakeholders regarding the implementation of the FDIC's IT strategic goals and objectives by the CIO Organization and the impact such efforts would have on their respective program areas. In addition, we found that due to the limited IT governance applied to two IT initiatives that we reviewed, the former CIO pursued overly aggressive implementation schedules and did not obtain broad business stakeholder involvement during their early stages. This resulted in unaddressed business needs and security risks, and it created inefficiencies, increased costs, and delayed the initiatives. Although the FDIC has taken steps during our audit, the agency still needed to implement further improvements to its IT Governance Framework and Processes.

FDIC IT Strategy Neither Fully Developed Nor Accepted

An IT strategy is an essential part of the Governance Framework. It defines and communicates the IT goals and priorities for the organization. OMB Circular A-130 requires that agencies have an IT Strategic Plan to show how technology and information resources map to the agency's mission and organizational priorities.

As previously discussed, the former CIO halted work on updating the long range IT Strategic Plan in early 2016 in order to focus on developing the 2016 Action Plan. The 2016 Action Plan defined short term IT actions to address what the former CIO considered to be the highest priority IT risks facing the FDIC. One such action involved migrating the FDIC's IT services and applications to the cloud beginning in 2016.

As discussed in the following sections, the CIO Organization did not obtain the acceptance of organizational stakeholders within the FDIC's divisions and offices, particularly for the adoption of cloud technologies, prior to executing its 2016 Action Plan. As a result, stakeholders were uncertain about the business impacts of the FDIC's IT strategy and approach.

Pursuit of a Cloud Strategy

While developing its IT Strategic Plan for 2017-2020, the FDIC decided to pursue cloud computing to address future business requirements. The FDIC also recognized the need for a comprehensive FDIC cloud strategy based on industry best practices. In addition, the FDIC hired an IT consultant, Gartner, Inc., to assist with this effort. In late 2015, Gartner completed an assessment of the FDIC's readiness for cloud adoption and confirmed that the FDIC would benefit from a cloud strategy that defined how the FDIC would utilize cloud services. Gartner also suggested that the cloud strategy be widely communicated to establish common understanding, acceptance, and alignment with business expectations. Gartner noted that gaining approval of a cloud strategy is a foundational step for transitioning IT services to the cloud, ensuring organizational commitment, and ensuring alignment with business expectations.

In June 2016, the same month that the FDIC completed its 2016 Action Plan, the former CIO embarked upon the Email to the Cloud initiative. The former CIO undertook this initiative based, in part, on Gartner's cloud readiness assessment completed in 2015 that identified that email was a foundational cloud service that the FDIC could adopt. The former CIO also noted that other organizations had already moved their email services to the cloud, indicating that many of the associated risks had already been addressed. Gartner determined that the FDIC could transition email to the cloud as early as the second half of 2016, or early 2017.

Based on FDIC internal documents, the CIO Organization planned to develop an enterprise cloud strategy and establish with client organizations a phased, multi-year transition plan and timetable for migrating FDIC systems to the cloud. However, the 2016 Action Plan contained only a high-level vision for adopting cloud technologies and did not constitute a complete enterprise cloud strategy. For example, the 2016

Action Plan did not describe the method and timing for transitioning systems and applications to the cloud.

By the fall of 2016, the CIO Organization had begun activities to migrate the FDIC's email operations to the cloud and planned to migrate other commodity IT services and applications to the cloud. During the FDIC's CIO Council meeting in December 2016, the former CIO acknowledged that the CIO Organization needed to address a number of areas specific to the cloud strategy. These areas included determining how to address mission critical applications that were not cloud ready, developing a clear understanding of how a cloud-based IT environment would operate, maturing the EA program, and mitigating risks associated with placing FDIC data with third parties. In response, some Council members expressed concern about the risks of moving some applications to the cloud before the CIO Organization completed a roadmap showing how it would implement its cloud strategy.

In January 2017, the CIO Organization developed a high-level document referred to as the "Cloud Strategy on a Page." This Cloud Strategy document called for the delivery of the majority of the FDIC's IT services and products via cloud solutions, and it explained a multi-phased approach for cloud adoption, with commodity IT services such as email migrating to the cloud first. CIO Organization officials presented the Cloud Strategy to members of the CIO Council on February 23, 2017. During the presentation, a representative of the CIO Organization stated that the Cloud Strategy would be further developed and released incrementally; however, the CIO Organization did not provide a timeframe for doing so. At the close of our audit, the CIO Organization had not yet finalized a comprehensive Cloud Strategy.

Impact on Stakeholders

The CIO Organization's approach of pursuing cloud initiatives without first developing and gaining acceptance of a comprehensive cloud strategy created uncertainty among business stakeholders. The lack of a fully developed cloud strategy mapping a path forward for adopting cloud technologies limited stakeholders' ability to understand the impacts to their business operations and make informed decisions regarding work prioritization, resources, and funding. We found that:

- During the CIO Council meeting in March 2017, members expressed concern that the CIO Organization was changing the original scope of planned work for the FDIC's Enterprise Data Warehouse (EDW)[15] project (consolidation) to move the application to the cloud. The members pointed out that moving

[15] A data warehouse is a storage architecture designed to hold data extracted from transaction systems, operational data stores, and external sources. The warehouse then combines that data in an aggregate, summary format suitable for enterprise-wide data analysis and reporting for predefined business needs. The FDIC's EDW is a centralized reporting environment that improves data accuracy, analysis, and reporting for authorized FDIC users.

applications such as EDW to the cloud and funding such initiatives should be part of a broader cloud strategy.

- During the CIO Council meeting in May 2017, a member expressed concern that the Council was not discussing the implications and impact of strategic IT decisions. The member stated that divisions and offices required more information regarding the impact of the new IT Strategic Plan on their business lines.

- During a meeting of the FDIC's Operating Committee in June 2017, division directors and other senior officials sought clarification on the CIO Organization's vision, plans, and priorities for adopting cloud solutions. Meeting participants indicated that they were unfamiliar with the risks and benefits associated with cloud technologies and what their role should be in facilitating cloud decision-making. Further, not all of the members shared the same view regarding whether their business applications and data should move to the cloud. As a first step in addressing these concerns, the CIO Organization provided the Operating Committee with a "Cloud 101" briefing in July 2017.

When we interviewed the current CIO (appointed as Acting CIO in October 2017 and named as permanent CIO that same month), DIT Director, and two Deputy DIT Directors, these officials indicated that the CIO Organization moved too rapidly in adopting cloud solutions. They acknowledged that the FDIC should have placed more emphasis on initial project planning and that this would have facilitated more substantive discussions and resolution of challenges with business stakeholders. It would have also enabled CIO Organization staff to support the technological changes and advocate for cloud projects.

As of December 8, 2017, the CIO informed us that the CIO Organization is reassessing the Cloud Strategy and associated initiatives. The CIO indicated that the CIO Organization plans to take a measured approach to cloud adoption and intends to integrate the Cloud Strategy into the EA, instead of developing a stand-alone Cloud Strategy.

Enterprise Architecture Ineffectively Implemented

An EA is the map of IT assets, business processes, and governance principles that drive ongoing investment and management decisions. An EA facilitates implementation of the IT strategic goals and objectives of the organization and provides the roadmaps and sequencing plans for transitioning IT services from their current state to a desired future state. OMB Circular A-130 requires agencies to develop an EA that describes baseline architecture, target architecture to strive toward, and a transition plan to attain the target. In addition, the GAO represented

that the effective use of a well-defined EA is a hallmark of successful organizations and a basic tenet of organizational transformation and systems modernization.[16]

In November 2001, the FDIC began developing an overarching EA to improve its method of managing technological change and help ensure sound IT investments.[17] Since that time, the FDIC established an EA program and the CIO Organization developed components of an EA. However, it was immature and it did not guide the three IT initiatives we reviewed or the FDIC's broader transition of IT services to the cloud. We previously reported that the lack of an effective EA exposes the FDIC to increased risk of inconsistently secured IT systems and higher IT maintenance costs.[18] The GAO also noted that ineffective utilization of EA can result in IT systems that are duplicative, poorly integrated, and unnecessarily costly to maintain and interface.[19] We found that an ineffective EA limited the CIO Organization's ability to communicate how it intended to implement its new IT strategies. This in turn created uncertainty among FDIC stakeholders regarding the direction of IT within the FDIC. This uncertainty caused stakeholders to question the adoption of new cloud technologies and question its impact to their business processes and overall suitability for the FDIC environment.

Historical EA Weaknesses

The OIG has reported on weaknesses in the FDIC's EA program since September 2001, including the lack of policies and procedures that adequately addressed security,[20] and limitations in the FDIC's EA repository used to store, classify, and organize data.[21] In addition, the GAO reported in 2002 that based on its maturity framework, the FDIC's maturity level for EA was at a "Stage 1" (Creating EA awareness). According to the GAO, Stage 1 agencies may have initiated some EA core elements, but they are *ad hoc* and unstructured, and do not provide the management foundation necessary for successful EA development.[22] Since then, the CIO Organization implemented policies and procedures to strengthen its EA program. However, recent assessments conducted on behalf of the CIO Organization found that the FDIC needed to further mature its EA program and use it to proactively guide IT investment decisions.

In November 2015, Gartner completed an assessment of the FDIC's readiness to transition IT services to the cloud. As part of that assessment, Gartner found that the

[16] *See* GAO Executive Guide *Organizational Transformation – A Framework for Assessing and Improving Enterprise Architecture Management* (Version 2.0) (Aug. 2010).
[17] *See* OIG Report, *Independent Evaluation of the FDIC's Information Security Program—2002* (Sept. 2002).
[18] *See* OIG Report, *Audit of the FDIC's Information Security Program—2017* (Oct. 2017).
[19] *See* GAO Report, *Enterprise Architecture Use across the Federal Government Can Be Improved* (Feb. 2002).
[20] *See* OIG Report, *Independent Evaluation of the FDIC's Information Security Program Required by the Government Information Security Reform Act* (Sept. 2001).
[21] *See* OIG Report, *Independent Evaluation of the FDIC's Information Security Program-2006* (Sept. 2006).
[22] *See* GAO Report, *Enterprise Architecture Can Use across the Federal Government Can Be Improved* (Feb. 2002).

FDIC needed to improve its EA program to support its IT strategies and guide IT investment decisions. For example, Gartner reported that the FDIC's EA did not serve as an authoritative reference that influenced governance of IT projects and had limited ability to affect cloud decisions. Gartner recommended that the FDIC adopt cloud architectures, including a set of guiding principles to govern the adoption of cloud services, and an initial set of reference architectures to describe the FDIC's capabilities for the cloud.

In January 2017, Gartner completed an assessment of the FDIC's EA. Gartner concluded that the maturity of the FDIC's EA program was at a Level 1 (or "non-existent") on a 5-point scale.[23] Notably, Gartner determined that the FDIC's EA maturity level was lowest in the area of Governance, and then recommended that the FDIC enhance its EA capability to support IT decisions, including the strategic shift toward cloud services.

Gartner further found that although the FDIC had developed "a number of important foundational documents including architectural artifacts in support of IT investment decisions, EA as a practice and as a capability was not being well utilized to proactively guide FDIC's IT decisions." For example, Gartner noted that the FDIC's EA staff predominantly spent their time on project-driven solutions, rather than on strategic EA. Gartner also determined that the FDIC lacked a key IT governance body, an EA Review Board, to ensure that FDIC organizational units and decisions comply with EA standards and principles.

In January 2017, the FDIC established a performance goal to align the FDIC's EA with leading practices, the Federal Government's EA requirements, and FDIC mission requirements. During the same time, the CIO Organization initiated actions to secure resources to enhance and mature the EA program at the FDIC. However, as discussed in our finding *Lack of Resources and Expertise to Improve Governance Framework*, the CIO Organization experienced difficulties and delays in obtaining these needed resources.

Impact on Stakeholders

The FDIC's immature EA program challenged CIO Organization efforts to implement a cloud model and negatively impacted stakeholders. CIO Organization executives we interviewed acknowledged that the weaknesses in the FDIC's EA program limited their ability to articulate to stakeholders the need for IT cloud initiatives and their suitability for the FDIC's environment. For example, the Deputy Director, Enterprise Technology Branch, DIT, stated that the FDIC did not have EA guiding principles and

[23] Gartner's maturity model designates Level 1 ("non-existent") as the lowest level of maturity when compared to other government and public sector peer groups, which have an average Gartner maturity model rating of Level 2 (or "reactive").

a roadmap to visually present how the FDIC intends to sequence events and transition to a new IT architecture, such as the cloud. This official also stated that the FDIC's EA program does not drive the IT strategy or adequately support its IT governance bodies. According to this Deputy Director, absent foundational documents such as EA guiding principles and a visual roadmap, the CIO Organization lacked the ability to explain how transitioning to a new technology made business sense. Consequently, the CIO Organization faced questions from FDIC stakeholders who wanted clearly articulated explanations and justifications for migrating to new technologies. For example, as previously discussed, CIO Council and Operating Committee members expressed concern and uncertainty regarding the benefits and risks, approach, and business impacts associated with the adoption of the Cloud Strategy.

CIO Organization executives we interviewed also acknowledged the need for a mature EA to support the successful development, communication, and execution of the IT Strategic Plan. For example, the Deputy Director, Enterprise Technology Branch, DIT, stated that the EA program needed to have an authoritative role in the governance structure so that it could effectively implement the strategic IT goals and objectives. The CIO stated that the FDIC needs to develop a reference architecture before further cloud adoption occurs.

Needed Revisions to IT Governance Processes

OMB Circular A-130 requires agencies to implement appropriate processes, standards, and policies to govern IT resources, and it requires the CIO, in coordination with appropriate governance boards, to define processes and policies in sufficient detail to address IT resources appropriately. These processes and policies must include appropriate measurements for agencies to evaluate the cost, schedule, and overall performance of IT projects.

Consistent with the principles and concepts in OMB Circular A-130, the FDIC established within its IT governance processes permanent bodies, such as the CIRC and CIO Council, to help ensure effective oversight of IT investments. These governance bodies are responsible for prioritizing potential IT investments for funding and for monitoring funded IT investments. The CIRC has responsibility for reviewing capital IT investments to determine whether they:

- Align with the FDIC's business requirements;
- Reduce risk by establishing both clear performance measures and accountability for project management and substantial stakeholder involvement and support throughout the project;

- Achieve cost, schedule, and performance targets;
- Provide business value and technical compliance with the EA, as appropriate; and
- Integrate information security to mitigate risks.

The CIO Council is responsible for governing a portfolio of IT projects and expenditures. The CIO Council's responsibilities include such things as prioritizing the portfolio of IT investments it oversees, monitoring the performance of that portfolio, and considering existing and changing corporate and divisional business needs.

We have previously reported that IT projects overseen by the CIRC or CIO Council, the FDIC's permanent governance bodies, generally met planned schedules, remained on budget, and met user expectations.[24] In that report, we observed several factors that helped to ensure the success of IT projects, including acceptance and representation from stakeholders during a project's development, marketing the benefits or reasons for the project, and managing the expectations of end users. The report also emphasized the importance of setting realistic milestones and deadlines for IT projects to allow time for adequate stakeholder communication.

Neither the CIRC nor the CIO Council governed the three IT initiatives that we reviewed. The CIO concluded that the Email to the Cloud initiative was a "low risk," technical refresh of a commodity IT service, would cost less than $3 million, and would be procured through an existing enterprise agreement. In addition, the Laptop Deployment initiative was a technical refresh of FDIC desktop computers. The CIO Organization funded both the Email to the Cloud and the Laptop Deployment initiatives with resources from the existing IT budget. Further, the FDIC terminated the Mobile Managed Services initiative as it was not found to be cost-beneficial. As a result, none of the three initiatives met the cost, risk, or funding requirements that would subject them to CIRC or CIO Council oversight.

The FDIC's existing IT governance processes and associated criteria allow divisions and offices to establish project specific governance over IT initiatives when the criteria for CIRC or CIO Council oversight are not satisfied. This can result in divisions and offices executing projects that consider their own more narrow interests in achieving a certain outcome, but may not adequately consider security, compliance with EA requirements, privacy controls, interdependencies with other systems, the potential for increased cost from duplicative processes and systems, and other agency-wide impacts.

[24] *See* OIG Report, *The FDIC's Information Technology Project Management Process* (July 2014).

Impacts of Applied Governance

The CIO established governance processes for two of the IT initiatives we reviewed (the Email to the Cloud and the Laptop Deployment) that generally conferred formal oversight and decision-making to the former CIO and CIO Organization officials. For both initiatives, the former CIO set aggressive implementation schedules, but did not obtain broad business stakeholder involvement in the early stages of the initiatives' lifecycles. This limited communication and led to unaddressed business needs, resulting in delays, inefficiencies, and increased costs. For example:

- The former CIO's staff considered the project schedule for the Email to the Cloud initiative to be overly aggressive.[25] Our interviews with CIO Organization officials and project team staff and our review of FDIC project documentation and emails for the initiative confirmed that this schedule was unrealistic as it abbreviated the time for obtaining organizational support, understanding business needs, and ensuring effective communication. CIO Organization managers also expressed concern over the aggressive schedule for the Laptop Deployment initiative (*i.e.*, completion within 60 days) stating that the schedule was unrealistic and did not allow for acceptance testing or effective communication with end-users in FDIC divisions and offices.

- The CIO Organization only engaged with representatives from the Division of Administration (DOA), the Legal Division, and the OIG during the early stages of the Email to the Cloud initiative to address known business needs related to e-discovery,[26] records retention, and email segregation. The CIO Organization did not meet with other FDIC divisions or offices to assess broader business needs and impacts until January 11, 2017, almost 7 months after starting the initiative.

- Gartner recommended in March 2016 that the FDIC develop a cloud adoption communication plan prior to executing cloud initiatives. The CIO Organization, however, did not complete a formal communications plan for the Email to the Cloud initiative until January 23, 2017, more than 7 months after the initiative began.

- The FDIC's Office of Complex Financial Institutions (OCFI), in coordination with DIT, was in the process of converting its laptops to desktops to help mitigate the risk of a breach of sensitive financial institution information contained in living wills.[27] OCFI executives suspended the deployment of laptops to their employees until further testing could assure them that the laptops met their security needs. In addition, laptops did not meet required

[25] The project began on June 13, 2016, with the goal of beginning migration of mailboxes to the cloud by December 31, 2016, approximately 6 months later.
[26] Electronic discovery (also called e-discovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal proceeding.
[27] OCFI took this step in response to a data breach of living will information discovered in 2015.

> data storage and/or processing needs for 302 end-users. While the CIO Organization was aware of these special configuration requirements, it did not obtain agreement from end-users on a solution prior to deploying the laptops. As a result, the CIO Organization had to perform additional testing of the laptops and purchase and install additional hardware at a cost of $45,000 to satisfy the data processing needs for 60 of these 302 end-users.

The FDIC would have benefited from robust governance over the planning and execution of these two initiatives, because it would have ensured greater transparency and communication of project goals and requirements with FDIC division and office representatives. Such governance would have been particularly beneficial for the Email to the Cloud initiative because of its relationship and interdependencies with other FDIC applications. Functionality for these applications utilized email for issuing passwords and automated notifications. The improved communication could have helped identify unique business needs of FDIC divisions and offices to ensure a greater understanding of the risks and benefits.

We have previously reported on the effects of weak oversight for IT projects that are not subject to CIRC and CIO Council governance. For example, in September 2015, we reported that the FDIC's Identity, Credential, and Access Management (ICAM) Program was not subject to sufficient and consistently robust governance.[28] Despite a relatively significant investment in resources, the ICAM program experienced higher than anticipated costs, delays, and limited success.

In addition, in March 2017, we reported that the FDIC established an overly aggressive transition schedule and did not meet key project milestones on its Failed Bank Data Services (FBDS) project. We also reported that FBDS project costs had exceeded estimates reported to and reviewed by the project governance.[29] We made recommendations for the FDIC to strengthen FBDS governance, project management, and contract oversight to reduce project-related risk.

The former CIO acknowledged the need to enhance the FDIC's IT governance processes. On May 12, 2017, the former CIO stated that the FDIC's IT governance structure was too focused on project-based investment decisions that addressed specific agency needs, rather than on portfolio-level planning and management. The former CIO acknowledged that IT decision-makers needed to better understand the business risks and impacts associated with IT investment decisions. In this regard, the former CIO recognized the need to enhance the role of business stakeholders in IT governance.

[28] *See* OIG Report, *The FDIC's Identity, Credential, and Access Management (ICAM) Program* (Sept. 2015).
[29] *See* OIG Report, *The FDIC's Failed Bank Data Services Project* (March 2017).

Further, CIO Organization officials that we spoke with, including the Acting Chief Information Security Officer (CISO) and the Director of DIT, acknowledged that the FDIC did not have adequate governance in place for the types of IT initiatives we reviewed. For example, the Director of DIT stated that the CIO Organization embarked upon IT initiatives, including the ones we selected, without first meeting with internal and external stakeholders to obtain support. These officials also indicated that the FDIC moved too rapidly to deploy these IT solutions and established aggressive timeframes without communicating them effectively with organizational stakeholders. The Director of DIT stated that the FDIC leadership should be cognizant of its customers regarding timeframe concerns when implementing IT initiatives.

At the close of our audit, the CIO was working to revise the roles and responsibilities of the FDIC's IT governance bodies to increase business line involvement. As part of this effort, the CIO should ensure that IT projects, including those not subject to CIRC and CIO Council oversight, are subject to appropriate governance.

Need for Enterprise Security Architecture and IT Security Planning

OMB Circular A-130 states that in support of agency missions and business needs, agencies must ensure "that information security and privacy be fully integrated into the system development process." OMB Circular A-130 also states that to be effective, information security and privacy considerations must be part of the day-to-day operations of agencies. According to OMB Circular A-130, this can best be accomplished by planning for the requisite security and privacy capabilities as an integral part of the agency's strategic planning and risk management processes, not as a separate activity.

In July 2016, the FDIC hired Booz Allen Hamilton (Booz Allen) to assess its IT security and privacy program. On December 29, 2016, Booz Allen reported the results and concluded that a key component of the FDIC's EA—the enterprise security architecture—was "*ad hoc* and inconsistently documented and implemented." According to the contractor, this limited the FDIC's ability to make informed decisions about technology acquisitions and upgrades and reduce vulnerabilities by leveraging common, approved, secure architectures and design patterns. Without a security architecture, FDIC has not defined its current and desired state of security.

In October 2017, we concluded, in our annual evaluation required by the Federal Information Security Modernization Act of 2014 (FISMA), that the lack of an enterprise security architecture increased the risk that the FDIC would develop information systems with inconsistent security controls that are more costly to maintain.[30] In response to our FISMA report, the CIO informed us that the FDIC intended to develop and integrate a security architecture into its EA, consistent with federal EA requirements. The CIO expected that the CIO Organization would complete this work by July 2018.

Enterprise Security Architecture

According to NIST, an enterprise security architecture describes the structure and behavior of an organization's security processes, information security systems, personnel and organizational subunits, and shows their alignment with the organization's mission and strategic plans. The enterprise security architecture links the components of an organization's security infrastructure as one cohesive unit, with the ultimate goal of protecting corporate information.

In addition to its observations on the FDIC's enterprise security architecture, Booz Allen also determined that the FDIC's IT governance processes did not consistently define or document clear roles and responsibilities for IT security. As a result, the contractor concluded that the CIO Organization did not consult key IT security stakeholders early in the lifecycle of IT initiatives when making IT decisions. Booz Allen identified certain examples where this occurred, including the Cloud Strategy, retirement of Entrust (the FDIC's email encryption solution), and the Laptop Deployment initiative.

As discussed in the following sections, two of the three IT initiatives we reviewed—the Email to the Cloud and Laptop Deployment initiatives—did not meet their planned implementation dates, in part, due to IT security concerns that were not adequately addressed during the early phases of the projects' lifecycles. In the case of the Laptop Deployment, unaddressed security concerns resulted in inefficiencies and limited the full benefits of $1.3 million in contractor surge labor.

Email to the Cloud

In October 2016, the FDIC determined that it needed to decommission Entrust by December 31, 2016 to migrate email to the cloud. In the weeks that followed, project team members met with security staff to discuss security risks and strategies for mitigating those risks. In early November 2016, the former CIO accelerated the Entrust retirement to accommodate the deployment of new security technologies and the migration of email to the cloud. In the days that followed, security staff

[30] *See* OIG Report, *Audit of the FDIC's Information Security Program—2017* (Oct. 2017).

expressed concern that this acceleration would not provide sufficient time to address unresolved security concerns.

On December 19, 2016, the former CIO notified his executives via email "we will and must retire [the legacy encryption solution] not later than [the] end of the second week (Friday) January 2017." In response, a security staff member informed the former CIO and Acting CISO that security concerns had not been resolved. These concerns, which were previously raised during project planning, included:

- There would not be adequate time for business stakeholders to react to the impact that retiring Entrust would have on their existing business processes;
- Sensitive emails on the internal network would not be stored in an encrypted format once Entrust was retired; and
- Employees would not be able to send email securely and comply with the FDIC's policy for protecting sensitive information if the FDIC did not identify and implement a replacement for Entrust before moving email to the cloud.

In response to concerns raised by IT security staff and external FDIC offices, in January 2017 the former CIO presented a three-phase approach for retiring Entrust and added the security concerns to a risk mitigation plan. Because the CIO Organization did not resolve security concerns early in the project, it was forced to revisit these previously raised concerns and delay the Entrust retirement until June 6, 2017, approximately 6 months later than the original retirement date.

Laptop Deployment

In early June 2016, the Acting CISO expressed concern to the former CIO about the planned laptop deployment initiative. The FDIC's existing laptop computers were not configured to minimize the risk of a data breach, and deploying additional laptops with the same configuration would further increase security risk for the FDIC. The Acting CISO cautioned the former CIO against proceeding with the laptop deployment until these vulnerabilities were resolved.[31]

During a mid-June 2016 strategy session, CIO Organization managers expressed concern to the former CIO about increased security risk and the aggressive schedule to deploy laptops by the end of July 2016. In late-June 2016, senior FDIC management authorized DIT to proceed with a procurement of up to 4,000 laptops at a not-to-exceed price of $5.12 million. The procurement authorization noted the "urgent timeline requirements" associated with the initiative. DIT separately allocated an additional $1.3 million in contractor labor costs to rapidly deploy the laptops.

[31] On June 8, 2016, the former CIO asked the Acting CISO to work with DIT staff to address this issue.

The CIO Organization began deploying the laptops in July 2016, but suspended the effort on August 25, 2016 due to continued security concerns expressed by FDIC staff, and similar security concerns raised by congressional members during a July 2016 hearing.[32] To resolve these concerns, the former CIO engaged contractors to perform security assessments of the laptops. Notably, one of the assessments identified several security vulnerabilities, one of which was similar to the concern that initially prompted the FDIC to suspend the laptop deployment. After assessing and addressing the security vulnerabilities identified by the contractors, the FDIC resumed the laptop deployment on January 20, 2017. The FDIC completed the laptop deployment in June 2017.

The FDIC suspended the Laptop Deployment initiative because the CIO Organization did not adequately address security concerns raised in the early stages of the initiative. As a result, the FDIC did not meet its planned deployment schedule. Further, the CIO Organization allocated approximately $1.3 million in contractor "surge" labor to support a rapid 60-day deployment for the laptops. However, DIT staff informed us that they had to find substitute tasks for the contractor personnel assigned to the expedited deployment after its suspension. These tasks included performing hardware and software maintenance and testing. As a result, the FDIC did not fully utilize the surge labor costs for its intended purpose. In addition, we previously reported that the FDIC delayed the deployment of the laptops to conduct a security assessment. As a result, approximately 6 months of the projected useful life for 2,900 laptops had expired by the time of deployment (17 percent of the projected useful life).[33]

Lack of Resources and Expertise to Improve Governance Framework

OMB Circular A-130 states that agencies must develop and maintain a current workforce planning process to ensure that the agency can maintain workforce skills in a rapidly developing IT environment and recruit and retain the IT talent needed to accomplish the agency's mission. OMB Circular A-130 also states that agencies must ensure that the workforce has the appropriate knowledge and skills to support the acquisition, management, maintenance, and use of information resources.

The FDIC's IT Strategic Plan and 2016 Action Plan called for a significant and rapid transformation in the delivery of IT resources. The success of this transformation relied upon individuals with expertise that the FDIC lacked in 2016. As described below, the FDIC experienced difficulties and delays in addressing these workforce

[32] *Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?: Hearing Before the H. Comm. on Science, Space, and Technology*, (July 14, 2016).
[33] *See* OIG Report, *The FDIC's Controls over the Information Technology Hardware Asset Management Program* (June 2017).

needs, which, in turn, slowed the FDIC's progress toward developing a mature governance structure, including a Cloud Strategy and improved EA program.

Knowledge, Expertise, and Experience

In late 2015 and early 2016, Gartner conducted its review of the FDIC's IT functions and services. Based on its work, Gartner concluded that the FDIC's adoption of cloud computing technologies and shared services would require a shift in approach from FDIC developing and operating IT assets to managing and monitoring cloud service vendors that would provide the needed services. Based on our interviews with CIO Organization officials, our review of Gartner and Booz Allen assessments, and industry research, we determined that cloud adoption requires specialized knowledge, skills, and experience, such as:

- Enterprise architects experienced in designing, implementing, and maintaining cloud-based systems, data, and IT architectures;
- Security professionals with skills in establishing cloud security requirements and monitoring capabilities for compliance;
- Procurement specialists experienced in developing and implementing cloud procurement policies, procedures, and contracts; and
- Project managers with skills in writing effective service level agreements (SLAs)[34] and contract oversight managers and monitors with skills in properly overseeing cloud service providers.

CIO Organization officials recognized the need for specialized knowledge, skills, and experience in the foregoing areas. These officials informed us that they initially planned to address this need by engaging contractors with such expertise who would transfer their subject matter expertise to FDIC staff over the course of time. Toward this end, in October 2016, the CIO Organization issued a sole-source solicitation to acquire a broad range of IT expertise to help the FDIC manage execution of both the 2016 Action Plan and the *2017—2020 IT Strategic Plan*. The CIO Organization intended this procurement to acquire contractor resources and expertise necessary to develop cloud adoption strategies; validate existing FDIC competencies and identify skill gaps for cloud adoption; develop an IT workforce training and staffing plan; develop cloud reference architectures; and establish an EA to serve as the foundation for cloud adoption across the FDIC. Notably, the Statement of Objectives

[34] According to the Federal CIO Council and the Chief Acquisition Officers Council, SLAs must contain certain elements: (1) define performance with clear terms and definitions, (2) demonstrate how performance is being measured, and (3) establish what enforcement mechanisms are in place to ensure the service providers meet the SLAs. *See* CIO Council and Chief Acquisition Officers Council *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service*, Feb. 24, 2012.

(SOO) stated that the FDIC planned to conduct these activities in a "very aggressive" timeframe.

An FDIC Technical Review Panel evaluated the contractor's proposal and concluded that the firm did not demonstrate the technical knowledge and capabilities to perform those requirements. As a result, the FDIC terminated the solicitation. According to CIO Organization officials, this setback delayed for a number of months, critical planning work needed to support the IT transformation.

Following this setback, the CIO Organization pursued an alternative strategy for acquiring the needed IT expertise through an arrangement with the National Institutes of Health Information Technology Acquisition and Assessment Center (NITAAC). In February 2017, the FDIC entered into an Interagency Agreement with NITAAC that allowed the FDIC to access certain Government-Wide Acquisition Contracts administered by NITAAC. However, it was not until May 2017 that the CIO Organization was able to begin procuring IT services through this arrangement. The Deputy Director, Enterprise Technology Branch, DIT, informed us that by this time, the CIO Organization was significantly behind schedule in developing a mature IT governance structure.[35] At the close of our audit, the CIO Organization planned to hire staff with specialized expertise in the near future.

Impact of Delays

The CIO Organization planned to complete a comprehensive Cloud Strategy and establish an EA program consistent with leading practices, the federal government's EA requirements, and FDIC mission requirements by December 29, 2017. These efforts were critical to maturing the FDIC's IT governance framework and processes and achieving FDIC's performance goals. However, without needed contractor resources and expertise, the CIO Organization could not develop a mature IT governance framework. For example, according to CIO Council meeting minutes, the CIO Organization delayed planned communications regarding the Cloud Strategy until it obtained contractor resources.

Need for Cost Information to Support IT Decision-Making

OMB Circular A-130 states that decisions concerning the selection of information system technologies and services must consider various factors, including the ability to meet operational or mission requirements, total life cycle cost of ownership,

[35] For example, the CIO Organization established a project in February 2017 to develop and execute a comprehensive Cloud Strategy by December 2017. Further, the CIO Organization established plans in March 2017 to enhance its EA program by implementing the recommendations from Gartner's EA program assessment by December 2017. Progress reports for these efforts showed that they were behind schedule and required contractor resources to complete.

performance, security, privacy, accessibility, ability to share or reuse, resources required to switch vendors, and availability of quality support. These factors support informed IT decision-making. As discussed below, the CIO Organization lacked necessary financial information to evaluate and justify IT initiatives supporting the 2016 Action Plan.

Lifecycle Cost Information

Based on work conducted in late 2015 and 2016, Gartner concluded that the FDIC's financial and budgeting processes did not support effective cloud decision-making. The lack of transparency into the cost of existing IT projects made it difficult for project managers and business liaisons to develop firm business cases for cloud projects from the outset. This is because cloud solutions are typically evaluated on a total cost of ownership (TCO) basis, and the FDIC did not track TCO costs for its IT projects, as OMB Circular A-130 required. Absent TCO data, it is difficult to compare the cost of proposed cloud projects to the cost of the FDIC's existing IT projects. In addition, Gartner found that there were no financial metrics within DIT to track cloud services because DIT had not established a consistent definition of what constituted cloud services. As a result, Gartner concluded that the FDIC had limited transparency into how much it spent on cloud technologies. Gartner added that the FDIC needed a better understanding of the costs involved as the agency moved forward with its cloud strategy. Such information can facilitate sound IT decision-making, including the evaluation of costs and benefits for proposed IT projects, as described below.

Cost-benefit Analyses

OMB Circular A-130 states that agencies must establish an IT investment decision-making process that includes criteria for analyzing projected and actual costs, benefits, and risks. In the late summer 2016, the FDIC's Division of Finance (DOF) introduced a new requirement that the CIO Organization must justify funds for all non-security DIT initiatives using a cost benefit analysis (CBA). The analysis must demonstrate that the initiative provides a cost savings that can be achieved over multiple years.

During budget formulation discussions in July 2016 for the FDIC's 2017 budget, the then-Chairman provided broad guidance to DOF about containing IT costs at the FDIC. Thereafter, according to the Deputy DOF Director, Corporate Planning and Performance Management, DOF instituted this guidance through the CBA guidance referenced above.

In January 2017, the FDIC established a 2017 Performance Goal to "modernize and reduce the costs of delivering IT resources and services to FDIC employees while

improving quality and customer satisfaction." A priority action to address this goal was to "complete the development of a template and process for cost-benefit analysis of major new IT spending initiatives." The then-Chairman informed us that he approved the 2017 Performance Goal and priority initiative; however, he was not consulted by DOF on the CBA process or how it would be implemented.

The introduction of the CBA requirement had a significant impact on the CIO Organization's IT initiatives, including those supporting the 2016 Action Plan. For example, the CIO Organization terminated the Mobile Managed Services initiative after the CBA concluded that the project would result in increased costs of approximately $13 million over 5 years. Similarly, the CIO Organization halted the migration of SharePoint to the cloud because costs for the initiative were higher than anticipated.

The Deputy Director, Enterprise Technology Branch, DIT, informed us that the CIO Organization experienced considerable difficulty in obtaining funds for new IT projects during 2016 and 2017 due to the focus on reducing IT spending. This official explained that the CIO Organization spent considerable time and effort attempting to justify new initiatives. The official added that the CBAs used to evaluate IT initiatives did not fully consider all relevant intangible benefits. Such benefits can be difficult to quantify and include improved functionality for users, productivity enhancements (e.g., responding to issues more quickly), or opportunities to avoid costs that may be incurred in the future.

The FDIC recognized the need to improve financial information needed to support informed decision-making. The FDIC established several priority initiatives in its 2017 performance goals (Performance Goal 9) to improve cost reporting and better inform decision-making on IT spending. In addition, on May 12, 2017, the former CIO acknowledged that the FDIC needed to mature its IT governance so that IT governance processes provide "transparency and a comprehensive view of IT spending and its impacts on business."

Conclusion and Recommendations

On October 19, 2017, the FDIC appointed a new CIO. At the close of our audit, the CIO was working to mature the FDIC's EA in order to facilitate implementation of the IT Strategic Plan and support sound IT decision-making. The CIO was also working to revise the roles and responsibilities of existing governance bodies and create an advisory board that will review new investment proposals, establish IT standards, conduct assessments and make recommendations, and coordinate with the CIRC and CIO Council. In addition, the CIO said that his office will strive to improve communications with business stakeholders, promote greater transparency, and shift to a measured approach for cloud adoption.

We are making the following eight recommendations to improve IT governance at the FDIC.

We recommend that the CIO:

(1) Develop an implementation plan to support the IT Strategic Plan, in coordination with FDIC stakeholders. The implementation plan should reflect the priorities of the FDIC and resources needed to execute the implementation plan.

(2) Incorporate the Cloud Strategy principles into the FDIC's IT governance framework.

(3) Implement an EA that is part of the FDIC's IT Governance Framework and used to guide IT decision-making.

(4) Revise the FDIC's IT Governance Processes, including roles and responsibilities for governance bodies.

(5) Incorporate the revised IT Governance Processes into applicable FDIC policies, procedures, and charters.

(6) Define and document roles and responsibilities for information security within the IT Governance Framework and Governance Processes.

(7) Identify and document the IT resources and expertise needed to execute the FDIC's IT Strategic Plan.

(8) Define and document procedures for evaluating the costs and potential benefits associated with cloud projects.

FDIC Comments and OIG Evaluation

The CIO Organization provided a written response, dated July 13, 2018, to a draft of this report. The response is presented in its entirety in Appendix 4. The CIO Organization concurred with all eight of the report's recommendations. The CIO Organization stated that it completed actions to address six of the recommendations and plans to complete actions to address the remaining two recommendations by June 28, 2019. All eight recommendations will remain open until we confirm that corrective actions have been completed and are responsive. Appendix 5 contains a summary of FDIC's corrective actions.

Objective

The objective of the audit was to identify key challenges and risks that the FDIC faces with respect to the governance of IT initiatives. The audit focused on key components of the FDIC's IT governance in relation to three IT initiatives: (1) the migration of email operations to the cloud; (2) the deployment of laptop computers to FDIC employees and contractor personnel; and (3) the potential adoption of a managed services solution for mobile IT devices. We focused on the areas of strategic IT planning, EA, and governance bodies and practices applied to these initiatives.

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. Except as noted in the report, our findings and conclusions are as of June 2017. In December 2017, the OIG conducted follow-up interviews with CIO Organization officials to gather information related to FDIC's progress in addressing IT governance challenges identified during fieldwork.

Scope and Methodology

The scope of our audit included a review of the FDIC's planning activities and deliverables for the three IT initiatives we selected. We also performed assessments of key controls related to the FDIC's written policies and procedures for IT governance, including the charters for key IT governance bodies.

To achieve the audit objective, we:

- identified and reviewed relevant criteria, including OMB Circular A-130, *Managing Information as a Strategic Resource*, OMB's *Federal Cloud Computing Strategy*, OMB's *25 Point Implementation Plan to Reform Federal Information Technology Management*, and the Federal CIO Council and the Chief Acquisition Officers Council Report *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service*.

- assessed relevant FDIC IT planning and governance policies, procedures, and guidance, including the *FDIC Information Technology Strategic Plan 2017 – 2020*, FDIC Cloud Strategy, FDIC 2017 Performance Goals, FDIC Circular 1303.1, *FDIC Enterprise Architecture Program*, dated June 16, 2008,

FDIC Policy 09-004, *Information Technology Project Management*, dated December 28, 2009, FDIC's Capital Investment Review Committee (CIRC) Charter dated November 19, 2014, FDIC's CIO Council (CIOC) Charter dated September 6, 2012, and FDIC's Financial Analysis Committee Charter dated February 19, 2014.

- assessed relevant FDIC IT initiative project deliverables and third-party reports completed between 2015 and 2017, including the FDIC IT initiative specific project plans, FDIC IT initiative specific cost benefit analyses, Gartner Cloud Readiness Assessment of FDIC, Gartner Cloud Strategy Organizational Capabilities Assessment of FDIC, Gartner Cloud Strategy Operationalization Plan of FDIC, Gartner Enterprise Architecture Program Support Final Improvement Plan and Roadmap for FDIC, and Booz Allen's Independent End-to-End Review of FDIC's IT Security and Privacy Program; and

- interviewed FDIC officials to determine roles, responsibilities, and perspectives related to project management, governance, and oversight for the three IT initiatives we selected. Such officials included the:

  - IT initiative Project Managers;
  - DIT Director;
  - Enterprise Technology Branch Deputy Director;
  - PMO staff;
  - CIO;
  - Corporate Planning and Performance Management Deputy Director; and
  - Various FDIC Divisional staff as necessary.

We did not rely upon computer-processed information in the scope of our audit. Regarding compliance with laws and regulations, we analyzed FDIC's compliance with relevant provisions of OMB circulars and memoranda pertaining to cloud computing, IT governance, EA, and strategic planning. In addition, we assessed the risk of fraud and abuse related to our objective in the course of evaluating audit evidence.

We performed our work at the FDIC's Headquarters offices in Washington, D.C., and at Virginia Square in Arlington, Virginia.

Term	Definition
Capital Investment Review Committee	The CIRC reviews and oversees all major IT and non-IT capital investments at the FDIC. The committee determines whether a proposed investment is appropriate for the FDIC Board of Directors' consideration, oversees approved investments throughout their life cycle, and provides quarterly status reports to the Board of Directors.
Chief Acquisition Officers Council	The CAOC is the principal interagency forum for monitoring and improving the federal acquisition system and promoting the President's specific acquisition-related initiatives and policies. Congress established the CAOC pursuant to Section 16A of the Office of Federal Procurement Policy (OFPP) Act, as amended.
Cloud Architectures	Identifies the components and subcomponents required for cloud computing including the major participants and their activities and functions in the cloud. For example, security and privacy are major architectural components of the cloud. The major cloud participants include the cloud consumer, cloud provider, and cloud carrier.
Cloud Computing	Cloud computing is a form of computing in which users have access to scalable, on demand capabilities that are provided through internet-based platforms and technologies. As computing resources are often provided by another organization (*i.e.*, provider), it has the potential to provide IT services more quickly and at a lower cost.
Cloud Reference Architectures	Depicts an architecture that is intended to facilitate an understanding of the requirements, uses, characteristics, and standards for cloud computing.
Commodity IT Services	Commodity services are widely available systems or services used to carry out routine tasks (*e.g.*, e-mail, SharePoint, identity and access management, data centers, networks, desktop computers and mobile devices).
Continuity of Operations	Continuity of Operations (COOP), as defined in the National Continuity Policy Implementation Plan (NCPIP) and the National Security Presidential Directive- 51/Homeland Security Presidential Directive- 20 (NSPD-51/HSPD-20), is an effort within individual executive departments and agencies to ensure that Primary Mission Essential Functions (PMEFs) continue to be performed during a wide range of emergencies, including localized acts of nature, accidents and technological or attack-related emergencies.

Term	Definition
Cost Benefit Analysis	A procedure requiring (1) identification of all costs and benefits of a proposed action and its alternatives, (2) translation of those costs and benefits into a common unit of measure (such as dollars), (3) discounting of future costs and benefits into the terms of a given year, and (4) ranking alternatives according to net dollar benefits (total dollar benefits less total dollar costs).
Enterprise Architecture	Enterprise Architecture can be viewed as a blueprint for organizational transformation and IT modernization. It consists of the enterprise's current, or "as-is," operational and technological environment and its target, or "to-be," environment and includes a capital investment road map for transitioning from the current to the target environment.
Federal CIO Council	Originally established in 1996 Executive Order 13011 (Federal Information Technology) and later codified by the E-Government Act of 2002, the CIO Council is the principal interagency forum for improving federal agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal information resources.
Financial Analysis Committee	Provides analysis, advice, and guidance to the FDIC Capital Investment Review Committee (CIRC) with regard to financial plans, proposals, and ongoing operations for projects under consideration by the CIRC. The Committee is chaired by the Deputy Director, Corporate Planning and Performance Management, Division of Finance, or their designee. Members may include representatives from FDIC's Division and Offices (*e.g.*, Division of Finance, Legal Division, Division of Supervision and Consumer Protection, Division of Resolutions and Receivership, Division of Administration, CIO Organization).
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Resources Management	The process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collection burdens on the public.
Living Will	Living wills are documents large financial institutions produce pursuant to the Dodd–Frank Wall Street Reform and Consumer Protection Act. These documents contain both public and confidential sections, describing how the large financial institution would dissolve itself in a timely and orderly manner under the U.S. Bankruptcy Code in the event of serious financial distress or failure of the company.

Term	Definition
Multi-factor Authentication	A security enhancement that requires an individual to present two pieces of evidence (*i.e.*, credentials) when logging in to an account. Credentials fall into any of these three categories: something you know (like a password or personal identification number), something you have (like a smart card), or something you are (like your fingerprint).
National Institute of Standards and Technology	Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST issues publications on information technology usage and best practices, including cloud computing. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems.
Operating Committee	A senior level management committee composed of directors from FDIC Divisions and Offices (*e.g.*, Division of Risk Management Supervision, Division of Finance, Legal Division, Division of Depositor and Consumer Protection, Division of Resolutions and Receivership, Division of Administration).
Reference Architecture	A reference architecture consists of information accessible to all project team members that provides a consistent set of architectural best practices.
Service Level Agreements	A Service Level Agreement is a contract between a service provider (*e.g.*, cloud service provider) and the end user that defines the level of service expected and other measurable outcomes.
Shared Services	An IT function that is provided for consumption by multiple organizations within or between Federal agencies (*e.g.*, email, SharePoint, help desk).
Technical Refresh	A planned process for the periodic replacement of old or obsolete technology assets.
Total Cost of Ownership	A comprehensive review of IT and other costs across an organization over time. In the context of IT, the total cost of ownership includes all related costs such as hardware and software acquisition, management and support, communications, end-user expenses, power consumption and floor space.

Appendix 3 Acronyms and Abbreviations

CBA	Cost Benefit Analysis
CIO	Chief Information Officer
CIRC	Capital Investment Review Committee
CISO	Chief Information Security Officer
DIT	Division of Information Technology
DOA	Division of Administration
DOF	Division of Finance
EA	Enterprise Architecture
EDW	Enterprise Data Warehouse
FBDS	Failed Bank Data Services
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Modernization Act of 2014
FITARA	Federal Information Technology Acquisition Reform Act
GAO	Government Accountability Office
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IRM	Information Resources Management
IT	Information Technology
NIST	National Institute of Standards and Technology
NITAAC	NIH Information Technology Acquisition and Assessment Center
OCFI	Office of Complex Financial Institutions
OMB	Office of Management and Budget
PMO	Program Management Office
PIV	Personal Identity Verification
PRA	Paperwork Reduction Act of 1980
SLA	Service Level Agreement
SOO	Statement of Objectives
TCO	Total Cost of Ownership

FDIC

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500 Office of the Chief Information Officer

DATE: July 13, 2018

TO: Mark F. Mulholland
Assistant Inspector General for
Information Technology Audits and Cyber

THROUGH: Howard G. Whyte **/Signed/**
Chief Information Officer and Chief Privacy Officer

FROM: Zachary N. Brown **/Signed/**
Chief Information Security Officer

Russell G. Pittman **/Signed/**
Director
Division of Information Technology

SUBJECT: Management Response to the Draft Audit Report Entitled *The FDIC's Governance of Information Technology Initiatives* (Assignment No. 2017-011)

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report on *The FDIC's Governance of Information Technology Initiatives* issued June 14, 2018. Information technology (IT) governance processes ensure that IT functions and operations support the FDIC's business strategies and mission objectives, and that IT investments align with those goals and objectives. The FDIC understands the criticality of IT Governance and its importance in driving risk-based decisions, cost savings, efficiencies, and improvements in the delivery of IT services.

During the course of the audit (December 2016 – June 2018), the CIO Organization (CIOO) made significant progress in the areas of IT Governance and Enterprise Architecture (EA). The CIOO initiated a multi-year effort focused on maturing the FDIC's enterprise architecture, strategic management, and program and portfolio management domains that is intended to run through year-end 2019. This effort already has resulted in the successful completion of two CIOO FDIC Performance Goals (FPGs) for 2018 related to the Enterprise IT Maturity effort. The CIOO's FPG efforts were completed subsequent to the June 2017 findings and conclusions identified in this draft report. The Performance Goals and progress made by the CIOO are summarized below:

- **FPG 9.01 (Governance):** *Develop and secure Operating Committee concurrence by March 31, 2018, for recommended changes to the current governance process for the FDIC's IT program.*
  - Established a new charter for the Operating Committee that reflects a strategic role in IT governance (March 2018);
  - Revised charter for the CIO Council to include increased business division membership and pedestrian changes for clarity (March 2018);

  - Established a charter and began operation of a new governance body, the Security and Enterprise Architecture Technical Advisory Board (SEATAB)[1] to govern the enterprise architecture and implement the information technology strategic direction of the FDIC through the development and adoption of technical guidance and standards (January/February 2018); and
  - Confirmed the scope and membership of the Capital Investment Review Committee (CIRC) to ensure alignment with the recommended governance approach.

- **FPG 9.01 (Enterprise Architecture):** *Secure concurrence from the Operating Committee by 02/28/2018 on an updated EA program that identifies target platforms for FDIC application systems (including the possible use of cloud platforms), encompasses a new security architecture, and aligns the FDIC's EA with leading practices and the Federal Government's EA requirements.*
  - Issued a set of *Enterprise Architecture Principles*; the principles are high-level definitions of fundamental values that guide the IT decision-making process, serving as the foundation for the IT architecture, development policies, and standards. (Adopted on November 30, 2017 and updated on March 15, 2018);
  - Updated the *Enterprise Architecture Blueprint* to establish the target state for the FDIC that spans the architecture domains of Business, Information, Application, Infrastructure and Security. The blueprint is aligned to the Federal Enterprise Architecture Framework (FEAF) 2.0. Industry best practices defined in the Cyber Security Framework and NIST standards are fully adopted by FDIC in the security domain, with tailored guidance integrated into all other architectural domains and enforced through all phases of solution development. (Adopted on November 30, 2017); and
  - Updated the *Applications Development Technology Standards* to orient the technical capabilities, development tooling and products that support IT service delivery toward reducing costs and improving quality. The updated standards identify cloud.gov and Salesforce as approved development platforms consistent with the FDIC's IT Strategic Plan objective to evaluate safe, secure cloud computing options. (Adopted on January 22, 2018 and updated in February, 2018).

In its report, the OIG audit team made eight (8) recommendations to the CIOO. We have carefully considered and concur with each of the recommendations. As a result of the above efforts, the CIOO has already completed action for six (6) of the eight (8) recommendations. This response outlines the CIOO's completed or planned corrective actions and the corresponding completion dates.

[1] The SEATAB is both a decision-making and an advisory body. The SEATAB is responsible for establishing and approving technical standards, guidance, and artifacts, including technical strategy documents. The SEATAB is responsible for evaluating and approving the introduction of all new information technologies to the FDIC. The SEATAB will evaluate requests for new technologies for appropriateness and suitability within the FDIC's enterprise architecture. The SEATAB will perform technical assessments and provide recommendations, using a risk-based approach, for proposals presented to the CIO, CIO Council, Operating Committee, or CIRC.

MANAGEMENT RESPONSE

Recommendation 1

We recommend that the CIO:

1. Develop an implementation plan to support the IT Strategic Plan, in coordination with FDIC stakeholders. The implementation plan should reflect the priorities of the FDIC and resources needed to execute the implementation plan.

   Management Decision: Concur

   Corrective Action:

   The CIOO has completed an implementation plan to support the IT Strategic Plan, in coordination with FDIC stakeholders. The implementation plan reflects the priorities of the FDIC and resources needed to execute the implementation plan. The plan is known as the CIOO 2018 Tactical Plan and was developed in coordination with the FDIC stakeholders. The draft plan was provided to CIOO employees, Division/Office Directors, and the Chief Information Officer Council (CIO Council) for review and the final version was published in March 2018.

   Estimated Completion Date: Completed – March 2018.

Recommendation 2

We recommend that the CIO:

2. Incorporate the Cloud Strategy principles into the FDIC's IT governance framework.

   Management Decision: Concur

   Corrective Action:

   The CIOO has completed incorporation of cloud into both the FDIC's enterprise architecture and IT governance frameworks. Within the *Enterprise Architecture Blueprint* (version 4.0 adopted November 2017), the target state for the infrastructure domain is a physical footprint that is modern, lean, and designed for demand management. Applications are modernized and hosted on a virtualized or cloud platform – whether on premise or outsourced. Within the Applications Development Technology Standards (updated February 2018), cloud.gov and Salesforce are identified as approved development platforms consistent with the FDIC's IT Strategic Plan objective to evaluate safe, secure cloud computing options.

As part of IT governance, the SEATAB is responsible for conducting risk-based technical assessments of proposed IT investments. The SEATAB technical assessment focuses on the proposed solution architecture and use of information technology resources across the five domains of application, business, information, infrastructure, and security. The SEATAB, in its advisory role, makes a recommendation to the project team and the appropriate governing body whether the project may proceed as planned or whether adjustments are necessary in order for the project to comply with EA principles and standards. The assessment includes the use of cloud options, consistent with the EA framework as noted above.

Estimated Completion Date: Completed – February 2018.

Recommendations 3

We recommend that the CIO:

3. Implement an EA that is part of the FDIC's IT Governance Framework and used to guide IT decision-making.

Management Decision: Concur

Corrective Action:

The CIOO has implemented an EA that is part of the FDIC's IT Governance Framework and used to guide IT decision-making. Specifically, the governance component of the EA Program is implemented through the SEATAB. The SEATAB governance body began operation in January 2018, replacing and absorbing the following governance bodies: Enterprise Architecture Board, Technical Review Group, and Development Tool Committee. The SEATAB implements the information technology strategic direction of the FDIC through the development and adoption of technical guidance and standards. The SEATAB performs technical assessments and provides recommendations, using a risk-based approach, for IT investment proposals and projects for consistency with the EA Principles and applicable EA standards.

The original SEATAB charter was updated and signed by the CIO on March 7, 2018.

Estimated Completion Date: Completed – January 2018 (operation); March 2018 (charter update/signature).

Recommendation 4

We recommend that the CIO:

4. Revise the FDIC's IT Governance Processes, including roles and responsibilities for governance bodies.

   Management Decision: Concur

   Corrective Action:

   The CIOO has completed updates to the IT governance processes, incorporating roles and responsibilities for governance bodies in revised and/or new charters. Specifically, the CIOO:

   - Established a new charter for the Operating Committee that reflects a strategic role in IT governance (March 2018);
   - Revised the charter for the CIO Council to include increased business division membership and pedestrian changes for clarity (March 2018);
   - Established a charter and began operation of a new governance body, SEATAB, to govern the enterprise architecture and implement the information technology strategic direction of the FDIC through the development and adoption of technical guidance and standards (January/February 2018); and
   - Confirmed the scope and membership of the Capital Investment Review Committee (CIRC) to ensure alignment with the recommended governance approach.

   Also, a high-level overview of the FDIC's Enterprise IT Governance Process was published in March 2018, highlighting changes made in the first quarter of 2018 that enhance, consolidate, and streamline governance processes

   Estimated Completion Date: Completed – March 23, 2018

Recommendation 5

We recommend that the CIO:

5. Incorporate the revised IT Governance Processes into FDIC policies, procedures, and charters.

   Management Decision: Concur

   Corrective Action:

   The CIOO has completed, or is planning to undertake, the update of the following documents to incorporate the revised IT Governance Processes:

   - Operating Committee Charter (completed; see recommendation 4 above)

- SEATAB Charter (completed; see recommendation 4 above)
- CIO Council Charter (completed; see recommendation 4 above)
- FDIC Directive 1300.7 – Information Technology Development Policy (planned)
- FDIC Directive 1303.1 - FDIC Enterprise Architecture Program (planned)
- FDIC Directive 1301.3 – FDIC Enterprise Information Management Program (planned)

Estimated Completion Date: June 28, 2019 (date by which the Directives will be issued and published by the Division of Administration)

Recommendation 6

We recommend that the CIO:

6. Define and document roles and responsibilities for information security within the IT Governance Framework and Governance Processes.

Management Decision: Concur

Corrective Action:

The CIOO has defined and documented roles and responsibilities for information security within the IT Governance Framework and Governance Processes. Specifically, the CIOO:

- Integrated security and privacy within the EA Principles and EA Blueprint.
- Added the Office of the Chief Information Security Officer (OCISO) as a member of the Operating Committee.
- Added the Chief Information Security Officer as a voting member to the CIO Council.
- Ensured the security domain is fully represented within the SEATAB. The Deputy of the Enterprise Technology Branch (ETB) from the Division of Information Technology and the Deputy Chief Information Security Officer (OCISO) serve as executive sponsors of the SEATAB. Voting members include the Chief of the Security Architecture Section (SAS) and the Chief, Security Engineering Section (SES) from the OCISO.
- Commissioned the development of an Enterprise Security Architecture that documents the role of the CISO and SEATAB for ensuring integration of security and privacy controls into IT projects to protect FDIC's sensitive data.

Estimated Completion Date: Completed – March 2018

Recommendation 7

We recommend that the CIO:

7. Identify and document the IT resources and expertise needed to execute the FDIC's IT Strategic Plan.

   Management Decision: Concur

   Corrective Action:

   As part of the CIOO's ongoing Enterprise IT Maturity Program, the CIOO will develop a workforce planning process which will ensure the identification and documentation of the IT resources and expertise needed to execute the FDIC's IT Strategic Plan.

   Estimated Completion Date: May 20, 2019

Recommendation 8

We recommend that the CIO:

8. Define and document procedures for evaluating the costs and potential benefits associated with cloud projects.

   Management Decision: Concur

   Corrective Action:

   The CIOO has completed the definition and documentation of procedures for evaluating the costs and potential benefits associated with all IT projects, including cloud, through a new Budget Formulation Process. This process covers both CIO Council and CIOO projects and includes procedures established by the Division of Finance (DOF) for completing a cost-benefit analysis of all IT projects, including cloud projects, which is just one option for delivery.

   Additionally, the SEATAB has been included in the above procedures. The SEATAB evaluates requests for new technologies for appropriateness and suitability within the FDIC's enterprise architecture. The SEATAB performs technical assessments and provides recommendations, using a risk-based approach, for proposals presented to the CIO, CIO Council, Operating Committee, or CIRC. The evaluations and assessments include the use of cloud options, consistent with the EA framework. The EA Principle of Technical Diversity Control is also applied, to ensure that technology diversity is controlled and managed to minimize IT expenses and the cost of

maintaining expertise across multiple environments and technologies while ensuring required business capabilities are provided.

Estimated Completion Date: Completed – March 2018

If you have any questions regarding this response, please contact Rack D. Campbell, Chief, Audit and Internal Control Section, DIT on 703-516-1422.

cc: E. Marshall Gentry, Deputy Director, DOF, Risk Management and Internal Control
Greg Kempic, DOF, Risk Management and Internal Control
Howard Pope, Acting Deputy Director, DIT, Business Administration Branch
Ken Weaver, Deputy Director, DIT, Enterprise Technology Branch

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	Completed/Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The CIO Organization, in coordination with other FDIC stakeholders, established an implementation plan (the CIO Organization 2018 Tactical Plan) to support the IT Strategic Plan. The implementation plan reflects the priorities of the FDIC and resources needed for execution.	March 2018	No	Yes	Open
2	The FDIC incorporated cloud strategy principles into its EA and IT governance framework. The FDIC revised its EA Blueprint to address IT infrastructure and applications. The FDIC also updated its Applications Development Technology Standards to establish cloud.gov and Salesforce as approved development platforms. Further, the FDIC created the Security and Enterprise Architecture Technical Advisory Board (SEATAB), which conducts risk-based technical assessments of proposed IT investments and advises project teams and governance bodies on whether IT projects can proceed as planned, or whether changes are needed to comply with EA principles and standards.	February 2018	No	Yes	Open
3	The FDIC implemented an EA as part of its IT Governance Framework to guide IT decision-making. The governance component of the EA Program is implemented through the SEATAB, which replaced the EA Board, Technical Review Group, and Development Tool Committee. The SEATAB provides IT strategic direction through the development and adoption of technical guidance and standards.	March 7, 2018	No	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Completed/Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
4	The FDIC updated its IT governance processes and incorporated roles and responsibilities for governance bodies into revised and/or new charters. Specifically, the FDIC established a charter for the Operating Committee that reflects a strategic role in IT governance; revised the charter for the FDIC CIO Council to increase business division membership; established a charter for the SEATAB to govern the EA and provide strategic IT direction through the development and adoption of technical guidance and standards; and confirmed the scope and membership of the CIRC.	March 23, 2018	No	Yes	Open
5	The FDIC updated its IT governance body charters and plans to update several IT policy directives to reflect revised IT Governance Processes.	June 28, 2019	No	Yes	Open
6	The FDIC defined and documented roles and responsibilities for information security within the IT Governance Framework and Governance Processes by integrating security and privacy in the EA Principles and EA Blueprint; adding the Office of the CISO as a member of the Operating Committee; adding the CISO as a voting member to the FDIC CIO Council; ensuring that security is fully represented in the SEATAB; and developing an Enterprise Security Architecture.	March 2018	No	Yes	Open
7	The FDIC will develop a workforce planning process to identify and document the IT resources and expertise needed to execute the FDIC's IT Strategic Plan.	May 20, 2019	No	Yes	Open
8	The FDIC has defined and documented procedures to evaluate the costs and potential benefits associated with all IT projects through a new Budget Formulation Process.	March 2018	No	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 partially concurs or 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.