Critical Functions in FDIC Contracts

March 2021 **EVAL-21-002**

Evaluation Report

Program Audits and Evaluations

☆☆☆☆☆☆☆☆

Critical Functions in FDIC Contracts

The FDIC relies on contractors to support a range of activities from janitorial to Information Technology support services. Contractors provide a multitude of staff with highly specialized technical skills and knowledge in current industry best practices and regulations. However, if the agency cannot provide a sufficient number of knowledgeable staff to oversee the contracts, the contractors could inappropriately influence government decision-making. Further, if the agency does not establish and maintain a proper control environment, it may lose control of its mission and operations.

In response to this risk, in September 2011, the Office of Management and Budget (OMB) provided guidance in OMB Policy Letter 11-01 on managing the performance of Inherently Governmental Functions and Critical Functions in order "to ensure that government action is taken as a result of informed, independent judgments made by government officials." In addition, the OMB Policy Letter 11-01 defined a Critical Function as "a function that is necessary to the agency being able to effectively perform and maintain control of its mission and operations. Typically, critical functions are recurring and long-term in duration."

There are numerous risks that may arise from an agency's use of third parties, including performance, monetary, legal, and reputational risks. If the FDIC does not manage the risks associated with Critical Functions prudently, it may:

- Become over-reliant on a third party to achieve its mission and conduct operations;
- Fail to control the Agency's mission and operations;
- Create inefficiencies through increased cost and decreased operational effectiveness;
- Fail to perform needed procedures;
- Fail to identify and evaluate alternative courses of action;
- Fail to provide independent judgments and informed oversight; and
- Compromise the trust (or data) by failing to exercise due care in establishing appropriate controls to protect sensitive information and to identify and mitigate data breaches.

Over a 3-year period, from 2017 to 2019, the FDIC awarded nearly 4,000 contracts valued at more than $1.3 billion. One contractor, The Blue Canopy Group, LLC (Blue Canopy), performed services in support of the FDIC's information security and

privacy program. For 2019, Blue Canopy services comprised 38.3 percent ($16.2 million) of the FDIC's annual operating expenses for Information Security ($42.3 million). Previously, we found that the FDIC had hired Blue Canopy to assess the same IT security controls that it had designed and executed. Therefore, we had determined in our prior report that Blue Canopy lacked independence in its assessments.

Our evaluation assessed whether Blue Canopy performed Critical Functions as determined by OMB Policy Letter 11-01 and best practices; and if so, whether the FDIC retained sufficient management oversight of Blue Canopy to maintain control of its mission and operations in accordance with best practices.

Results

We found that the FDIC did not have policies and procedures for identifying Critical Functions in its contracts, as recommended by the best practices in OMB Policy Letter 11-01 and embodied in industry standards. Therefore, while we determined that Blue Canopy performed Critical Functions at the FDIC, as defined by OMB Policy Letter 11-01 and best practices, the FDIC did not identify these services as Critical Functions during its procurement planning phase.

As a result, the FDIC also did not implement heightened contract monitoring activities for Critical Functions as stated in OMB's Policy Letter 11-01, and best practices identified and used by other government agencies. Such heightened contract monitoring activities would include: (1) performing a procurement risk assessment, (2) establishing a management oversight strategy, (3) conducting periodic reviews, and (4) providing formal reports to the Board on an individual and aggregate basis.

Without these best practices in place, the FDIC cannot be assured that it will provide sufficient management oversight of Blue Canopy or other contractors performing Critical Functions. In particular, the FDIC may not ensure that it has an adequate number of employees with the appropriate training, experience, and expertise to oversee the procurements of Critical Functions.

Recommendations

We made 13 recommendations to the FDIC's Deputy to the Chairman and Chief Operating Officer. The recommendations include incorporating provisions of the OMB Policy Letter 11-01 into the FDIC's policies and procedures, identifying Critical Functions during the procurement process, and implementing heightened contract monitoring for Critical Functions.

Management concurred with 1 of the 13 recommendations, and plans to complete corrective action by May 31, 2021. The FDIC stated that it partially concurred with the remaining 12 recommendations; however, the FDIC response did not provide specific actions taken or planned. As a result, we consider the remaining 12 recommendations to be unresolved at this time. To resolve these 12 recommendations, we would expect that the FDIC provide a clear indication of the specific actions within the next 6 months, and we will determine whether the recommendations may be converted to being "resolved" at that time, or whether they will remain as "unresolved." For the 12 unresolved recommendations, the FDIC plans to consider and further study the issues and does not intend to implement corrective actions for another year (between March 31 and June 30, 2022).

Contents

Federal Deposit Insurance Corporation
Office of Inspector General
Office of Program Audits and Evaluations

March 31, 2021

Subject | ***Critical Functions in FDIC Contracts***

According to the Government Accountability Office (GAO), the use of a contractor poses a risk of fraud, waste, and abuse. Therefore, agencies need to ensure a proper internal control environment to oversee and maintain control of their operations. Agencies should consider internal controls such as approval authorities, segregation of duties, and independence and non-conflict of interest standards. The failure to establish or maintain a proper control environment jeopardizes the reasonable assurance that an entity's objectives will be achieved and may affect the ability of an entity to maintain control of its mission and operations.

The FDIC relies on contractors to support a range of activities from janitorial to Information Technology support services. Contractors provide a multitude of staff with highly specialized technical skills and knowledge in current industry best practices and regulations. However, if the agency cannot provide a sufficient number of knowledgeable staff to oversee the contracts, the contractors could inappropriately influence government decision-making. Further, if the agency does not establish and maintain a proper control environment, it may lose control of its mission and operations.

In response to this risk, in September 2011, the Office of Management and Budget (OMB) provided guidance on managing the performance of Inherently Governmental Functions and Critical Functions in order "to ensure that government action is taken as a result of informed, independent judgments made by government officials." OMB's Office of Federal Procurement Policy issued *Publication of the Office of Federal Procurement Policy (OFPP) Policy Letter 11–01, Performance of Inherently Governmental and Critical Functions* (September 2011) (OMB Policy Letter 11-01). OMB Policy Letter 11-01 defines the terms "Inherently Governmental Function" and "Critical Function" as follows:

- An ***Inherently Governmental Function*** is "a function that is so intimately related to the public interest as to require performance by Federal Government employees." The term includes functions that require either the exercise of discretion in applying Federal Government authority or the making of value judgments in making decisions for the Federal Government, including judgments relating to monetary transactions and entitlements.

- A ***Critical Function*** is "a function that is necessary to the agency being able to effectively perform and maintain control of its mission and operations. Typically, critical functions are recurring and long-term in duration."

We note that the definition of a "Critical Function" as defined by OMB Policy Letter 11-01 is similar to the definition of an "Essential Function" found in the FDIC's Continuity of Operations Program.[1] It is also similar to the definition of "Critical Functions" in the FDIC Chief Information Officer Organization *Business Continuity Plan* (January 2019) which are defined as "business activities or information that could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization." For purposes of this report, we will use the term and definition of "Critical Function" from OMB Policy Letter 11-01 which is widely accepted across the Federal government.

OMB Policy Letter 11-01 requires certain agencies[2] to take specific actions, before and after contract award, to prevent contractor performance of Inherently Governmental Functions and to prevent over-reliance on contractors in the performance of Critical Functions. Government agencies must ensure that (1) contractors do not perform work that should be reserved for Federal employees; and (2) Federal officials are appropriately managing and overseeing contractor performance. Federal agencies need to ensure proper management and oversight of procured services for Critical Functions in order to prevent over-reliance on the contractor and the loss of control of the agency's mission and operations. These actions are in addition to the standard controls and processes that agencies follow in procuring goods and services.

Ultimately, if an agency fails to ensure proper management and oversight of procured Critical Functions, contractors may take actions that are not based on informed, independent judgments made by Government officials. Such actions by contractors create risks that governance and decisions of significant public interest are not made by Government officials who are accountable to the President and bound by laws controlling the conduct and performance of Federal employees. These laws are intended to protect the public and ensure the proper use of governmental funds. In particular, a loss of control could result in actions and decisions that are not in the public interest, and instead may be focused on the contractor's business development, profitability, or unsuitable influences.

The Blue Canopy Group, LLC (Blue Canopy) performed a range of cybersecurity and privacy support services for the FDIC. While agencies often rely upon third-party contractors to perform a wide variety of services and other activities, there are numerous

[1] According to FDIC Directive 1500.6, *Continuity of Operations (COOP) Program* (November 2019), **Essential Functions** are a subset of government functions that are determined to be critical activities. These essential functions are then used to identify supporting tasks and resources that must be included in the organization's continuity planning process.

[2] OMB Policy Letter 11-01 established Executive Branch policy and was addressed to the heads of civilian and Executive Departments and agencies. An **Executive Agency** is a Federal agency that is housed under the Executive Office of the President or one of the 15 Cabinet departments within the Executive Branch. According to the FDIC Legal Division, "the FDIC does not fall within the definition of "executive agency" in the [Office of Federal Procurement Policy] Act."

risks that may arise from an agency's use of third-party contractors, including performance, monetary, legal, and reputational risks. For example, if not managed and supervised prudently, the agency may:

- Become over-reliant on a third-party contractor to achieve its mission and conduct operations;[3]
- Fail to control the agency's mission and operations;
- Create inefficiencies through increased cost and decreased operational effectiveness;
- Fail to perform needed procedures;
- Fail to identify and evaluate alternative courses of action;
- Fail to provide independent judgments and informed oversight; and
- Compromise trust (or data) by failing to exercise due care in establishing appropriate controls to protect sensitive information and to identify and mitigate data breaches.

Over a 3-year period, from 2017 to 2019, the FDIC awarded nearly 4,000 contracts valued at more than $1.3 billion. For 2019, Blue Canopy services comprised 38.3 percent ($16.2 million) of the FDIC's annual operating expenses for Information Security ($42.3 million). Previously, we found that the FDIC had hired Blue Canopy to assess the same IT security controls that it had designed and executed. Therefore, we had determined in our prior report that Blue Canopy lacked independence in its assessments.[4]

Our evaluation assessed whether Blue Canopy performed Critical Functions as determined by OMB Policy Letter 11-01 and best practices; and if so, whether the FDIC retained sufficient management oversight of Blue Canopy to maintain control of its mission and operations in accordance with best practices.

In order to answer our objectives, we reviewed Blue Canopy's two existing contracts, as of May 2020,[5] with the FDIC's Chief Information Officer Organization (CIOO), and the FDIC's acquisition process to identify and manage procured Critical Functions. We also reviewed documentation and interviewed employees familiar with Blue Canopy's work to determine if the FDIC maintained control of its mission and operations. Our methodology relied on identifying best practices from various reputable sources,

[3] An agency may be deemed over-reliant on a service provider if it does not have the capacity (number of Federal employees) and capability (Federal employees with appropriate training, experience, and expertise) to understand the agency's requirements, formulate alternatives, manage the work product, monitor the contractors used to support the Federal workforce, and adequately mitigate the potential impact on mission performance if contractors were to default on their obligations.
[4] *Security Configuration Management of the Windows Server Operating System* (AUD-19-004) (January 2019). https://www.fdicoig.gov/sites/default/files/publications/19-004AUD_0.pdf
[5] Contracts CORHQ-14-C-0769 and CORHQ-14-C-0778.

including OMB Policy Letter 11-01, GAO reports, industry standards, and other Federal agencies, and comparing the FDIC's acquisition process with these best practices.

According to the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation, evaluations are systematic and independent assessments of the design, implementation, and results of operations, programs, or policies. OIGs use evaluations to determine the efficiency, effectiveness, impact, and sustainability of operations, programs, or policies. OIGs may also use evaluations to share best practices and approaches.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation.

.

Appendix 1 of this report includes additional details on our objective, scope, and methodology. Additional appendices include acronyms and abbreviations, the Agency's comments on a draft of this report, and a summary of the Agency's corrective actions.

BACKGROUND

The Federal Deposit Insurance Act authorizes the FDIC to acquire services and to establish policies and procedures to achieve its mission and operations.[6] The FDIC's acquisition process involves a number of organizations within the Agency, including the Program Office that initiates a procurement to obtain the services or goods it needs, the Division of Administration's (DOA) Acquisition Services Branch (ASB), the Legal Division, and the FDIC Board of Directors (Board).

- **Program Office.** The Program Office is responsible for determining its procurement needs and initiating the acquisition process by submitting a procurement request to DOA's ASB. The Program Office is also responsible for nominating the Oversight Manager and Technical Monitor(s).[7]
- **Division of Administration, Acquisition Services Branch.** DOA's ASB is responsible for issuing the policies governing the contracting program and the procedures for implementing those policies. When DOA's ASB receives an acquisition request from a Program Office, it assigns the request to a Contracting Officer.[8] The Deputy Director of the ASB appoints Contracting Officers with the

[6] 12 U.S.C. § 1819(a). In particular, the Federal Deposit Insurance Act authorizes the FDIC "[t]o make contracts", "[t]o appoint … such officers and employees … to define their duties", and "[t]o prescribe, by its Board of Directors, bylaws… regulating the manner in which its general business may be conducted…."
[7] The **Technical Monitor** is responsible for assisting the Oversight Manager in monitoring and evaluating contractor performance under an FDIC contract.
[8] The **Contracting Officer** is responsible for ensuring the performance of all actions necessary for efficient and effective contracting, ensuring compliance with the terms of contracts, and protecting the interests of the FDIC in all of its contractual relationships.

authority to enter into, administer, and terminate contracts on behalf of the FDIC. The Contracting Officer works with the Program Office throughout the acquisition process, and, based on the Program Office's nominations, appoints the Oversight Manager and Technical Monitor(s).

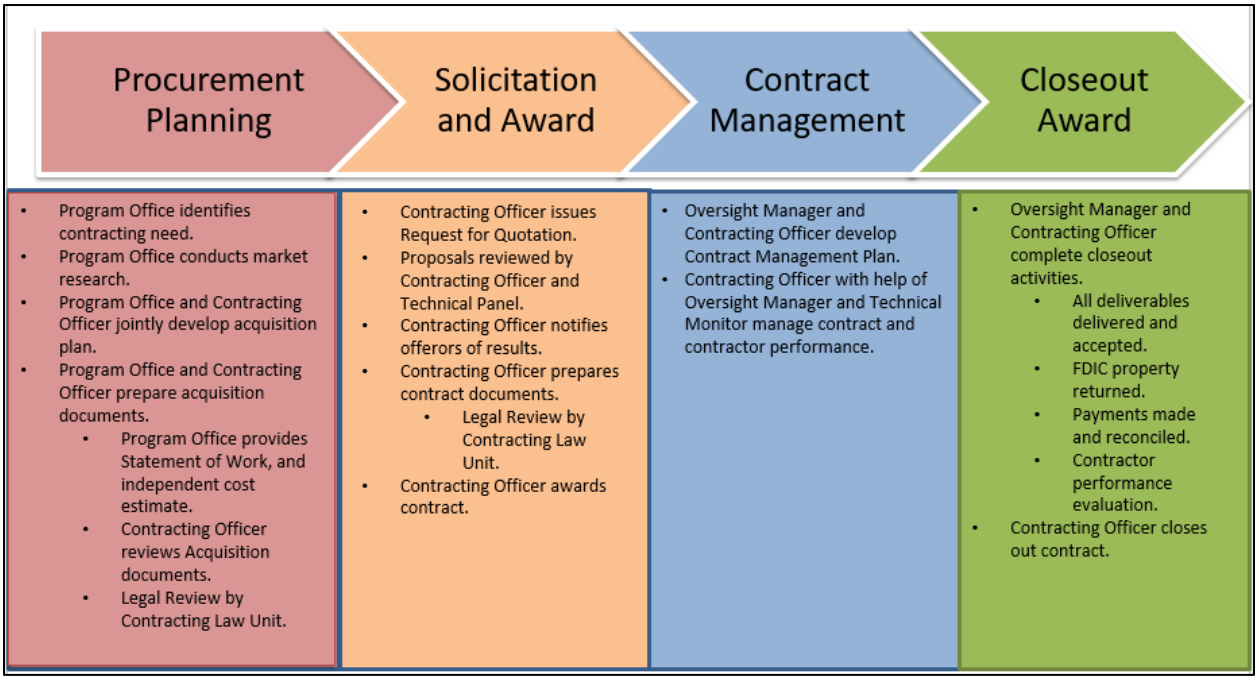
- **Legal Division.** The FDIC's Legal Division provides legal advice and counsel to Contracting Officers to ensure that acquisitions and other contract actions are conducted in accordance with governing laws and FDIC policy.
- **The FDIC Board of Directors.** The Board approves the execution of contracts with dollar values over $20 million and contract modifications to contracts previously approved by the Board that increase the award amount or period of performance by more than 15 percent.

The FDIC's Acquisition Process

The FDIC's acquisition process is divided into four phases: (1) Procurement Planning; (2) Solicitation and Award; (3) Contract Management; and (4) Closeout Award.

Figure 1 shows the four phases of the FDIC's acquisition process and provides an overview of the activities within each phase.

Figure 1: The FDIC's Existing Acquisition Process



Source: OIG analysis of the *FDIC Acquisition Policy Manual* (August 2008) and the *Acquisition Procedures, Guidance and Information* (January 2020).

The FDIC and Blue Canopy's Contractual Relationship

Blue Canopy was founded in 2001 and is an information technology advisor and service provider that offers mission support, cybersecurity, technology and systems development, data analytics, and cloud and mobility solutions to Government and commercial clients. The FDIC began working with Blue Canopy in May 2009 when the FDIC's CIOO, Office of the Chief Information Security Officer (OCISO), and DOA,[9] procured the services of Blue Canopy to provide Information Security Support Services to the FDIC after the initial contractor filed for bankruptcy. Since then, the procured services have been re-competed and re-issued twice. Specifically, the acquisition process was initiated in January 2010 and then again in June 2014. In June 2014, the FDIC Board of Directors authorized senior management to contract for services in support of the information security and privacy program and to increase the prior contract ceiling. The FDIC re-competed and re-issued these services to Blue Canopy under two new contracts with a total Award Value of $101.3 million.[10] Both contracts had 7-year terms (a 3-year base period and four 1-year options), and one became effective in December 2014, and the second one in March 2015.[11]

In October 2019, the FDIC changed its procurement strategy for the two contracts to two Basic Ordering Agreements (BOA)[12] and included multiple service providers on the BOAs. The BOAs have a total Award Value of $398 million. The Board authorized a 7 1/2-year term for Security Operations Center and Vulnerability Management Services and a 10-year term for security and privacy professional services. To date, four task orders have been awarded under the BOAs to two different service providers. By May

[9] The **OCISO**'s mission is to develop and maintain Agency-wide information security and privacy programs that support the mission of the FDIC. The OCISO is comprised of four sections: Governance, Risk and Compliance; Privacy; Security Architecture; and Security Operations. In 2009 and 2010, the services obtained were overseen by the FDIC's Division of Information Technology. Since then, the FDIC re-organized and placed oversight responsibility within the CIOO OCISO.

[10] The FDIC separated the information security support services into two contracts to potentially increase the number of vendors that placed bids and to attract higher quality bids by vendors that specialized in only one set of services. By separating the support services, the FDIC could have reduced reliance on one contractor for both sets of services. However, the FDIC awarded both contracts to Blue Canopy, which did not reduce reliance on a single contractor for information security support services. From July 2005 to December 2019, the FDIC issued three contracts (or sets of contracts) for information security support services. The FDIC's contract Award Values, for these services, increased from the initial modified Award Value of $27.6 million to $56.3 million, and then to $101.3 million – for a total increase of 267 percent (101.3 million – $27.6 million) / $27.6 million). According to the Board memorandum, *Request for Authority to Contract for Services in Support of the Information Security and Privacy Program and to Increase the Current Contract Ceiling* (June 2014), and the FDIC memorandum, *Justification for Non-Competitive Procurement* (March 2019), these increased procurement costs were mainly due to the expansion of Federal information security standards and corresponding services.

[11] The FDIC Division of Resolutions and Receiverships (DRR) also has a contract with Blue Canopy for an approximate Award Value of $1 million, and a 5-year term. DRR's contract with Blue Canopy was beyond the scope of this review.

[12] According to the FDIC's Acquisition Procedures, Guidance and Information (January 2020), a Basic Ordering Agreement (BOA) is "a written instrument of understanding negotiated between the FDIC and a contractor for future delivery of as yet unspecified quantities of goods or services. A BOA becomes a binding contract when a task order is issued."

2021, the FDIC expects to transition information security and privacy program services to multiple service providers by awarding additional task orders under the BOAs.

In 2019, the services provided by Blue Canopy comprised 38.3 percent ($16.2 million) of the OCISO's annual operating expenses ($42.3 million). Over a 4-year period (2015-2019), the FDIC's OCISO spent between 35 percent to 44 percent of its operating expenses annually on Blue Canopy services.

Through the two contracts, Blue Canopy provided the following services:

(1) Information Security and Privacy Support Services for the FDIC's Security Operations Center (SOC) and Computer Security Incident Response Team (C-SIRT). The services provided under this contract included intrusion monitoring; incident investigation; event escalation; reporting; vulnerability research, analysis, and response; incident detection; incident response; and after-hours support.

(2) Information Security and Privacy Support Services for outsourced functions. The services provided under this contract included an annual technical security assessment, vulnerability management, annual Federal Information Security Modernization Act of 2014 (FISMA) self-assessment,[13] continuous controls assessment, privacy program (support services),[14] security engineering and technical assistance, and internal controls.

Inherently Governmental Functions and Critical Functions

OMB Policy Letter 11-01 provides guidance on managing the performance of Inherently Governmental and Critical Functions. The policy letter adopted the definition of an Inherently Governmental Function based on the established statutory definition in the *Federal Activities Inventory Reform Act* (FAIR Act),[15] and it eliminated variations of this definition found in other documents.

As such, OMB Policy Letter 11-01 defined an ***Inherently Governmental Function*** as "a function that is so intimately related to the public interest as to require performance by Federal Government employees… The term includes functions that require either the

[13] The ***Federal Information Security Modernization Act of 2014*** **(FISMA)** amended and clarified the *Federal Information Security Management Act of 2002*. Title III of the E-Government Act, entitled the *Federal Information Security Management Act* of 2002 requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency. FISMA requires each agency to perform an annual self-assessment. The FDIC and Blue Canopy's contractual arrangement supported the FDIC's internal annual self-assessment, as required by FISMA.
[14] The FDIC's **Privacy Program** is a risk-based program that focuses on protecting the privacy rights of individuals by ensuring that Personally Identifiable Information is handled and protected in accordance with applicable Federal and FDIC requirements and industry standards. The contract provides various support activities to the Privacy Program.
[15] Public Law 105-270.

exercise of discretion in applying Federal Government authority or the making of value judgments in making decisions for the Federal Government, including judgments relating to monetary transactions and entitlements." OMB Policy Letter 11-01 requires certain Federal agencies to ensure that contractors do not perform Inherently Governmental Functions.

In addition, OMB Policy Letter 11-01 established a definition for a **Critical Function** as "a function that is necessary to the agency being able to effectively perform and maintain control of its mission and operations. Typically, Critical Functions are recurring and long-term in duration." The policy letter recommends that Federal employees should perform and/or manage Critical Functions to the extent necessary for the agency to operate effectively and maintain control of its mission and operations.

The FDIC's Legal Division has maintained that OMB Policy Letter 11-01 does not apply to the FDIC, but it may be used for guidance.[16] We focused our evaluation on assessing the FDIC's procurement of Critical Functions given their importance in achieving the Agency's mission; we did not evaluate Inherently Governmental Functions as part of this review.

Best Practices for Procuring Critical Functions

According to the GAO, best management practices:

> [R]efer to the processes, practices, and systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas. Successfully identifying and applying best practices can reduce business expenses and improve organizational efficiency.[17]

For our evaluation, we identified best practices for procuring Critical Functions by reviewing OMB Policy Letter 11-01, GAO reports, industry standards,[18] and interviewing officials at several other Federal agencies.[19] We compared these best practices with the FDIC's existing procurement process, using Blue Canopy as an example, to determine the extent to which the FDIC incorporated these best practices into its process. Table 1 summarizes these best practices.

[16] The FDIC Legal Division concluded that OMB Policy Letter 11-01 did not apply to the FDIC, because (1) the FDIC did not fall within the definition of "executive agency" in the Office of Federal Procurement Policy Act; and (2) the FDIC was not funded by congressionally appropriated funds.
[17] GAO Report, *Best Practices Methodology: A New Approach for Improving Government Operations* (GAO/NSIAD-95-154) (May 1995).
[18] We considered industry guidance promulgated by the FDIC to financial institutions, such as the FDIC's Financial Institution Letter titled, *Third-Party Risk Guidance for Managing Third-Party Risk* (FIL-44-2008) (June 2008).
[19] Our interviews at other Federal agencies included the National Credit Union Administration (NCUA), Consumer Financial Protection Bureau (CFPB), Office of the Comptroller of the Currency (OCC), Federal Reserve Board of Governors (FRB), the OMB, General Services Administration (GSA), National Aeronautics and Space Administration (NASA), Department of Agriculture (USDA), and Department of Energy (DOE).

Table 1: Best Practices for Critical Functions by Source

Best Practice	OMB	GAO	Industry Standard	Select Federal Agencies
Identify planned procurement of Critical Functions	✓	✓	✓	✓
Implement heightened contract monitoring processes for Critical Functions	✓	–	✓	✓
Perform a procurement risk assessment for Critical Functions	✓	✓	✓	✓
Perform a cost effectiveness analysis	✓	–	✓	✓
Develop a management oversight strategy	✓	✓	✓	✓
Determine contract structure	–	–	✓	✓
Conduct periodic reviews of controls and processes	✓	–	–	✓
Report to the Board on procured Critical Functions	–	–	✓	–

Source: OIG analysis of OMB guidance, GAO reports, industry standards and guidance, and interview statements from Federal agencies.
Legend: ✓ The source identified this item. | – The source did not mention this item.

EVALUATION RESULTS

We found that the FDIC did not have policies and procedures for identifying Critical Functions in its contracts, as recommended by the best practices in OMB Policy Letter 11-01 and embodied in industry standards. In addition, we determined that Blue Canopy performed Critical Functions at the FDIC, as defined by OMB Policy Letter 11-01 and best practices. In particular, Blue Canopy performed a range of cybersecurity and privacy support services for the FDIC, including continuous monitoring, vulnerability management, internal control reviews, and privacy assessments. These services are critical to ensuring the security and protection of the FDIC's Information Technology

infrastructure and data. In 2019, these services comprised 38.3 percent ($16.2 million) of the OCISO's annual operating expenses ($42.3 million). A breach or disruption in these services could impact the security, confidentiality, integrity, and availability of FDIC information. Therefore, the FDIC needed proper oversight of the Critical Functions performed by Blue Canopy to ensure such a breach or disruption of service did not occur. Due to the lack of policies and procedures in this area, the FDIC did not identify these Critical Functions by Blue Canopy during its procurement planning phase.

As a result, the FDIC also did not implement heightened contract monitoring activities for Critical Functions as stated in OMB's Policy Letter 11-01, and best practices identified and used by other government agencies. Such heightened contract monitoring activities would include: (1) performing a procurement risk assessment, (2) establishing a management oversight strategy, (3) conducting periodic reviews, and (4) providing formal reports to the Board for its review of Critical Functions on an individual and aggregate basis.

Without these best practices in place, the FDIC cannot be assured that it will provide sufficient management oversight of Critical Functions in its contracts. In particular, the FDIC may not ensure that it has an adequate number of employees with the appropriate training, experience, and expertise to oversee the procurements of Critical Functions.

Blue Canopy Performed Critical Functions

As noted above, the OIG identified best practices from OMB Guidance, the GAO, industry standards, and several other Federal agencies. These best practices support the view that the FDIC should establish and document a process for identifying procurements of Critical Functions. Appendix 2 contains a detailed description of the best practices related to procured Critical Functions. Further, GAO recommendations and other Federal agencies support that this process should be addressed within policies and procedures.

In addition, the GAO's *Standards for Internal Control in the Federal Government*, (GAO-14-704G) (September 2014), states that agencies should implement internal control standards and activities to achieve agency objectives and respond to risks, and should implement these activities through policies.

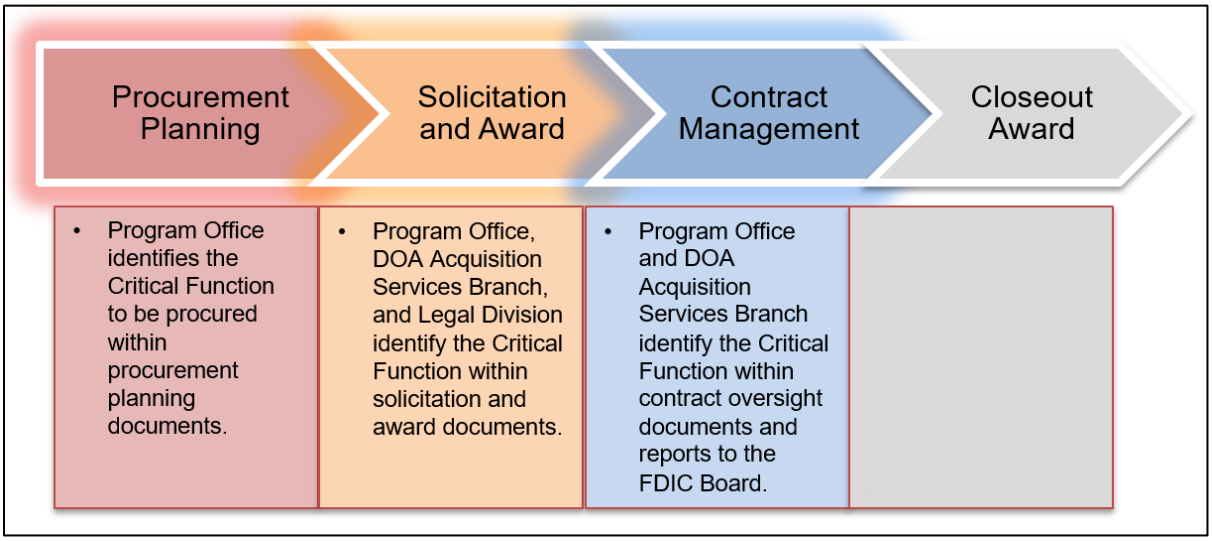
No FDIC Process for Identifying Critical Functions

Based on our review of documentation and interviews with FDIC contracting officials, we found that the FDIC does not have a process for identifying Critical Function procurements. Therefore, the FDIC did not identify the Information Technology services

performed by Blue Canopy as Critical Functions during the procurement planning phase, solicitation and award phase, or contract management phase of the acquisition process.

Figure 2 illustrates the best practices for identifying planned and procured Critical Functions during the FDIC's acquisition process. Of particular note, the failure to identify Critical Functions during the procurement planning phase results in a cascading failure throughout the acquisition process. A risk management process would identify, measure, monitor, report, and mitigate the operational and procurement risks for acquired Critical Functions.

Figure 2: Best Practices for Identifying Planned and Procured Critical Functions



Source: OIG analysis of identified best practices and the FDIC's policy and procedures.

Information Technology services at the FDIC have been identified as critical to the FDIC operations in numerous documents, including the FDIC's 2019 Annual Report, Enterprise Risk Management Risk Inventory,[20] and National Institute of Standards and Technology (NIST) guidance. In particular, we noted the following:

- **The FDIC 2019 Annual Report.** Within the FDIC 2019 Annual Report, the FDIC recognized that "Information technology (IT) is an essential component in virtually all FDIC business processes…"; and that "[t]he FDIC's information security

[20] **Enterprise Risk Management** (ERM) is an agency-wide approach to addressing internal and external risks facing an agency. ERM provides an enterprise-wide view of challenges that enables agencies to allocate resources, prioritize and proactively manage risk, improve the flow of risk information to decision makers, and work towards successful accomplishment of their missions. ERM provides transparency and accountability in business practices, reporting, and governance, which can improve stakeholder confidence in the agency's work. A **Risk Inventory** is a list of the risks facing the agency. Risks are identified from various sources and are captured in the risk inventory. The Risk Inventory includes an assessment of impact and likelihood, and risks are prioritized and summarized into one of four risk levels: critical, significant, moderate, and low.

program is integral to the agency's ability to carry out its mission of maintaining stability and public confidence in the nation's financial system." In particular, the FDIC highlighted its continuing efforts to strengthen its information security functions and progress towards optimizing the Security Operations Center, privacy controls, and information and network security.

The FDIC relied on Blue Canopy to develop, operate, and service the Security Operations Center as well as information and network security. These services are important for the FDIC to maintain security, confidentiality, integrity, and availability of data; and, the trust and confidence of the public in the financial industry.

- **Enterprise Risk Management Risk Inventory.** Within the FDIC's *Enterprise Risk Management Risk Inventory* (October 2019), the FDIC recognized that the Agency was subject to significant risk related to a cyber-attack and/or data breach resulting in the loss of Personally Identifiable Information, and disruptions in system operations and data availability.

  Although not identified within the FDIC's Risk Inventory, the Agency relied heavily on Blue Canopy to operate and service the corresponding risk management mitigating controls.

- **National Institute of Standards and Technology Guidance.** Blue Canopy provided critical services that were essential to the FDIC's mission and operations. The FDIC relied on Blue Canopy to conduct activities within the FDIC's Security Operations Center, Computer Security Incident Response Team, and Information Security and Privacy Program Support, which were recognized within NIST guidance as foundational security controls or "protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of systems." Without these foundational security controls, the FDIC could not ensure the security, confidentiality, integrity, and availability of its information – thus jeopardizing the Agency's mission and operations. (Appendix 3 describes the NIST guidance we identified related to procured Critical Functions.)

DOA and CIOO officials acknowledged that the FDIC had not incorporated OMB Policy Letter 11-01 (September 2011), and related best practices, into the FDIC's *Acquisition Policy Manual* (August 2008), or *Acquisition Procedures, Guidance and Information* (January 2020).

Without a process for identifying planned and procured Critical Functions, the FDIC cannot ensure that it will take appropriate actions based on "informed, independent

judgments made by governmental officials"[21] for all contracts covering Critical Functions. Further, the FDIC may not maintain control of its mission and operations, and may become over-reliant on contractors. An agency may become over-reliant on a service provider if it does not have the capacity (number of Federal employees) and capability (Federal employees with appropriate training, experience, and expertise) to oversee the contractor properly. In particular, Federal employees must be able to understand the agency's requirements, formulate alternatives, manage the work product, monitor the contractors used to support the Federal workforce, and adequately mitigate the potential impact on mission performance if contractors were to default on their obligations.

According to the GAO, the use of a contractor poses a risk of fraud, waste, and abuse. Agencies need to establish a proper internal control environment to oversee and maintain control of their operations. Agencies should consider internal controls such as approval authorities, segregation of duties, and independence and non-conflict of interest standards. The failure to establish or maintain a proper control environment jeopardizes the reasonable assurance that an entity's objectives will be achieved, and may affect the ability of an entity to maintain control of it mission and operations.

In August 2017, a former FDIC senior executive expressed concern with the FDIC's contractual relationship with and over-reliance on Blue Canopy. As previously noted, Blue Canopy's services represented a significant percentage of the OCISO's annual operating expenses. In addition, a prior OIG report, *Security Configuration Management of the Windows Server Operating System* (AUD-19-004) (January 2019) concluded that Blue Canopy lacked independence. This represented a failure of the FDIC to maintain control of its operations.

Prior OIG report. The OIG's report, *Security Configuration Management of the Windows Server Operating System* (AUD-19-004) (January 2019), noted that "the FDIC hired [Blue Canopy] to assess certain security controls, including configuration management controls, for which the FDIC had also assigned the firm duties related to design and/or execution. According to NIST guidance, this arrangement limited the firm's independence and impaired the firm's ability to conduct impartial security control assessments. The FDIC relies on the results of security control assessments to identify security weaknesses and inform key risk management decisions." Within this report, the OIG recommended that the FDIC "[e]stablish requirements to ensure the independence of security control assessors."

If the FDIC identified planned and procured Critical Functions, it would be able to provide senior management and the Board with the knowledge, insight, and transparency on planned Critical Function procurements; the volume, depth, and concentration of procured Critical Functions; and the degree of reliance on contractors to perform Critical Functions.

[21] OMB Policy Letter 11-01.

Procured Critical Functions Not on FDIC Risk Inventory

The FDIC annually captures the risks it faces through its Enterprise Risk Management Risk Inventory. The Risk Inventory lists risks to the FDIC's ability to achieve its goals and objectives. As part of the FDIC's Enterprise Risk Management program, after the Divisions and Offices identify their risks, they assess the likelihood of those risks occurring on both an inherent[22] and a residual[23] basis. The OIG previously reported on the FDIC's implementation of Enterprise Risk Management and concluded that improvements will help ensure that risks across the FDIC are considered, for example, as part of operations support and program management. For this report, risks must be considered in regard to procurement operations and IT services for Critical Functions.

Blue Canopy performed a range of cybersecurity and privacy support services for the FDIC. In 2019, these services comprised 38.3 percent ($16.2 million) of the OCISO's annual operating expenses ($42.3 million). The FDIC Risk Inventory acknowledged the risks associated with these cybersecurity and privacy support services, including a potential cyber-attack on the FDIC's systems and a security incident involving Personally Identifiable Information.[24] In addition, the FDIC Risk Inventory recognized the risk associated with managing contracts throughout the contract lifecycle, including the potential for increased costs for goods and services, increased contractor claims, and delivery of inferior goods and services to support the FDIC mission.

Prior OIG report. The OIG report, *The FDIC's Implementation of Enterprise Risk Management* (EVAL-20-005) (July 2020), assessed the FDIC's implementation of Enterprise Risk Management against relevant criteria and best practices. The report concluded that "the FDIC needs to establish a clear governance structure, and clearly define authorities, roles, and responsibilities related to [Enterprise Risk Management]. This will help ensure that the FDIC integrates [Enterprise Risk Management] into its culture, practices, and capabilities so that risks across the enterprise are considered and prioritized as part of operations support, program management, budget decisions, and strategic planning … Having well-defined authorities, roles, and responsibilities for [Enterprise Risk Management] will help to ensure that the range of risks facing the Agency and banking sector are properly identified."

However, the FDIC's Risk Inventory did not recognize procured Critical Functions as a separate and distinct risk, or as an analytical factor in determining inherent or residual risk related to the risks associated with cybersecurity and privacy support services.

[22] According to the FDIC's *Enterprise Risk Management Standard Operating Procedure* (May 2020), **Inherent Risk** is the exposure arising from a specific risk before any action has been taken to manage it beyond normal operations.
[23] According to the FDIC's *Enterprise Risk Management Standard Operating Procedure* (May 2020), **Residual Risk** is the exposure remaining from an inherent risk after action has been taken to manage it.
[24] **Personally Identifiable Information** is any information about an individual that can be used to distinguish or trace that individual's identity, or any other personal information that is linked or linkable to that individual. Examples of Personally Identifiable Information include an individual's full name, Social Security Number, driver's license, medical information, or home telephone number.

Further, the FDIC's Risk Inventory did not recognize the specific risks related to Blue Canopy performing such a large percentage of the FDIC's IT security budget.

Based on our review of GAO and industry standards,[25] procured services involving contractors result in a greater level of inherent risk than an agency directly performing these services. In particular, the FDIC warned its regulated institutions of such risk and, therefore, should assess and address the risk itself. For example, according to the FDIC's Financial Institution Letter, *Third-Party Risk Guidance for Managing Third-Party Risk* (FIL-44-2008) (June 2008), "[t]here are numerous risks that may arise from … use of third parties. Some of the risks are associated with the underlying activity itself, similar to the risk faced by an institution directly conducting the activity. Other potential risks arise from or are heightened by the involvement of a third party."

The FDIC's Chief Financial Officer Organization, Office of Risk Management and Internal Controls guidance titled, *Enterprise Risk Management Standard Operating Procedure* (May 2020), states that the FDIC currently assesses all risks facing the Agency, including inherent and residual risks, and considers existing control mitigations that reduce inherent risks.

Without the identification of procured Critical Functions and its associated risk, the FDIC may not accurately capture and assess the Agency's inherent and residual risk related to its contracts and contractors. In addition, the FDIC's Enterprise Risk Management program may not ensure that the FDIC has appropriately identified, measured, monitored, reported, and mitigated the FDIC's significant risks for contracts and contractors.

As demonstrated by the FDIC and Blue Canopy's contractual relationship, the FDIC's acquisition and risk management processes did not identify the procurement risk of Critical Functions, nor did the FDIC heighten its management oversight for these procured services. This potentially jeopardizes the FDIC's ability to maintain control of its mission and operations by failing to ensure that government actions are taken as a result of informed, independent judgments made by government officials; work products are adequately managed; and contractors are appropriately monitored.

[25] GAO, *Standards for Internal Control in the Federal Government* (GAO-14-704G) (September 2014); and the FDIC's Financial Institution Letter, *Third-Party Risk Guidance for Managing Third-Party Risk* (FIL-44-2008) (June 2008).

Recommendations

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

1) Incorporate the provisions of OMB Policy Letter 11-01 guidance into the FDIC Acquisition Policy Manual (August 2008) and Acquisition Procedures, Guidance and Information document (January 2020).

2) Identify Critical Functions during the procurement planning, award, and contract management phases of the acquisition process.

3) Assess whether the FDIC's Enterprise Risk Management program should identify the impact of procured Critical Functions, and procurement risk related to contractors performing Critical Functions, within the FDIC's Risk Inventory.

The FDIC Did Not Implement Heightened Monitoring for Critical Functions

As noted above, the OIG identified best practices from OMB Guidance, the GAO, industry standards, and Federal agencies. These best practices support the view that the FDIC should develop and implement heightened contract monitoring processes for Critical Functions. Based upon the best practices, these processes should include the following:

Procurement Risk Assessment. A procurement risk assessment should be performed during the procurement planning phase of the acquisition process. This assessment should consider, for example, the sufficiency of the agency's internal capacity and capability to control its mission and operations based on an adequate number of Federal employees with appropriate training, experience, and expertise, and a cost effectiveness analysis to ensure that it is cost effective to contract for the services.

Management Oversight Strategy. Management should identify performance criteria, internal controls, reporting needs, and contractual requirements that would be critical to the ongoing assessment and control of risk in contracts containing Critical Functions. A management oversight strategy considers, for example, the contract structure (including key provisions) for procuring Critical Functions, and oversight tasks personnel can perform.

In particular, the FDIC should have a process for ensuring that specific expectations and obligations of both parties are outlined in a written contract prior to entering into the arrangement. Management should also ensure that the statement of work recognizes the procurement of Critical Functions. The contract should define key contract

terminology[26] and incorporate key provisions necessary to mitigate the risk associated with procuring Critical Functions.

Periodic Reviews of Controls and Processes. Management should periodically evaluate the adherence to and effectiveness of its internal management controls and procedures to address the objectives and requirements of OMB Policy Letter 11-01. The objective of these reviews should address the controls' effectiveness in deterring or mitigating the agency's over-reliance on the contractor, and ensuring that the agency maintains control of its mission and operations. Areas of review include contractor and agency personnel performance, and human capital planning.

In particular, an over-reliance assessment should be performed regularly, on an independent basis, to validate the agency's compliance with and the effectiveness of established controls. Periodic reviews should identify indicators of potential operational/process failures and conclude on the FDIC's ability to retain sufficient management oversight of the procured services to maintain control of its mission and operations. An agency may become over-reliant on a service provider if it does not have the capacity (number of Federal employees) and capability (Federal employees with appropriate training, experience, and expertise) to oversee the contractor properly. Federal employees must be able to understand the agency's requirements, formulate alternatives, manage the work product, monitor the contractors used to support the Federal workforce, and adequately mitigate the potential impact on mission performance if contractors were to default on their obligations. Periodic reviews should determine if the agency needs to take corrective measures to address any over-reliance on contractors for Critical Functions.[27]

Ultimately, when an agency is over-reliant on a contractor, the agency potentially jeopardizes its ability to maintain control of its mission and operations by failing to ensure that government actions are taken as a result of informed, independent judgments made by government officials; work products are adequately managed; and the contractors used to support the Federal workforce are appropriately monitored.

Board Reporting. The Board should be involved in reviewing management's risk assessment, contract structuring, and monitoring reports for procured Critical Functions on an individual and aggregate basis. Appendix 2 contains a description of the best practices related to procured Critical Functions.

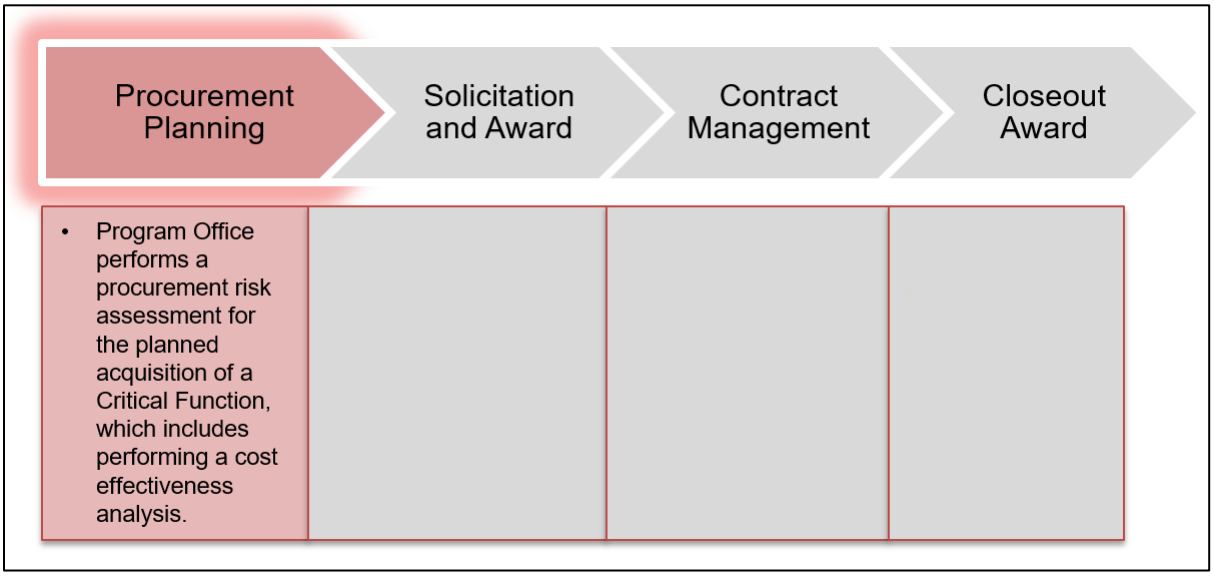
[26] **Contract terminology** are specialized words or meanings relating to a particular field, such as the term Critical Function in the Federal acquisition process.

[27] **Corrective Measures.** Management should consider, in part, the following corrective measures for identified instances of contractor over-reliance: (1) reviewing and adjusting contractor services; (2) reassessing and adjusting human capital needs (staff and funding); (3) in-sourcing all or part of the function; (4) reviewing the contracting process from beginning to end to understand how the agency lost control; and (5) reestablishing or strengthening controls over contractor responsibilities.

The FDIC Did Not Perform a Procurement Risk Assessment for Critical Functions

The FDIC did not perform a procurement risk assessment for Critical Functions obtained from Blue Canopy during the procurement planning process. Figure 3 illustrates the best practices for performing a procurement risk assessment during the FDIC's acquisition process.

Figure 3: Best Practices for Performing a Procurement Risk Assessment



Source: OIG analysis of identified best practices and the FDIC's policy and procedures.

The FDIC implemented its established procurement process, but that process did not include an analysis of the underlying services in order to identify the risks and to determine the need for heightened oversight procedures and controls for the procured Critical Functions. Without the requisite analysis, the FDIC cannot be assured that it has appropriately identified and mitigated the existing procurement and operational risks.

The FDIC also did not document a cost effectiveness analysis, as recommended by best practices. In particular, FDIC management did not present to the Board an analysis that demonstrated whether it was cost effective to procure the desired Critical Functions or to perform those functions internally with Federal employees or some combination of Federal employees and contractor personnel. Without a proper cost effectiveness analysis, an agency cannot identify, analyze, and determine (on an informed basis) the most cost effective alternative or course of action.

We recognize that the FDIC calculated and presented to the Board the Independent Government Cost Estimates (IGCE)[28] that were used to conclude on the reasonableness and feasibility of the proposals received. However, we found that the Agency did not document and present to the Board a complete cost effectiveness analysis that evaluated whether a Critical Function should be procured or performed internally. The FDIC documented and presented to the Board a qualitative justification for procuring Blue Canopy services. However, it did not document and present to the Board a cost effectiveness analysis that included the scope and methodology, assumptions, quantitative and qualitative analyses, conclusions, and rationale for the Agency's final procurement decision.

For one of the Blue Canopy contracts, the IGCE supporting documentation showed that the FDIC calculated that it would be more expensive to procure the services than to perform them internally with FDIC employees. Specifically, the FDIC calculated that it would cost the FDIC an additional $2.55 million to procure the services ($26,387,825 versus $23,834,747).[29] However, the FDIC did not include this information in the Board Case Package, nor was it discussed with the Board as demonstrated by the corresponding Board minutes. According to OMB Policy Letter 11-01, in order "to meet its fiduciary responsibility to the taxpayers, the agency must have sufficient internal capability to control its mission and operations and must ensure it is cost effective to contract for the services."

A CIOO official stated that the IGCE represented a cost effectiveness analysis. In particular, the official stated that the IGCE included a comparison of the costs to conduct the planned activities internally against the cost for a vendor(s) to perform those same activities. The official also stated that, in conjunction with the IGCE, the CIOO conducted an analysis to determine whether the FDIC's costs associated with Information Security and Privacy support services were in line with other Federal agencies.

As discussed above, however, the FDIC's IGCE did not include the scope and methodology, analyses (both quantitative and qualitative), conclusions, and rationale for the Agency's final procurement decision as suggested by best practices. In addition, the

[28] According to the FDIC's *Acquisition Procedures, Guidance and Information* (January 2020), the **Independent Government Cost Estimate** is the FDIC's estimated cost for the acquisition. According to the FDIC's Selection Recommendation Report titled, *Security Operations Center and Computer Security Incident Response Team Services* (February 2015), the Independent Government Cost Estimate was calculated based on information acquired through historical data from the prior 3 years, as well as projects anticipated over the life of the proposed contract. The primary purpose of the Independent Government Cost Estimate is to assess the reasonableness of the price proposals received from contractors against the Agency's estimated procurement cost.

[29] For **Contract CORHQ-14-C-0778**, the FDIC's IGCE estimated that it would cost $26,387,825 to procure the services from a third party versus the estimated cost of $23,834,747 to perform the services internally with Federal employees, a variance of $2,553,077. In March 2015, Blue Canopy was awarded the contract with an Award Value of $18,608,671, and in March 2019, the contract was modified to the FDIC Board of Directors, pre-approved Award Value ceiling limit of $26,400,000. The increase allowed the contract to continue to its full period of performance of March 2022.

FDIC did not perform a procurement risk assessment and develop a management oversight strategy for procured Critical Functions (identifying heightened controls and processes, and appropriate internal capacity and capability of internal resources) that would have informed the analysis of cost and assured the Agency it could control its own mission and operations. Ultimately, as recommended by best practices, a complete cost effectiveness analysis for Critical Functions, clear and distinct from the IGCE, should be performed and presented to the Board for its review and consideration.

Recommendations

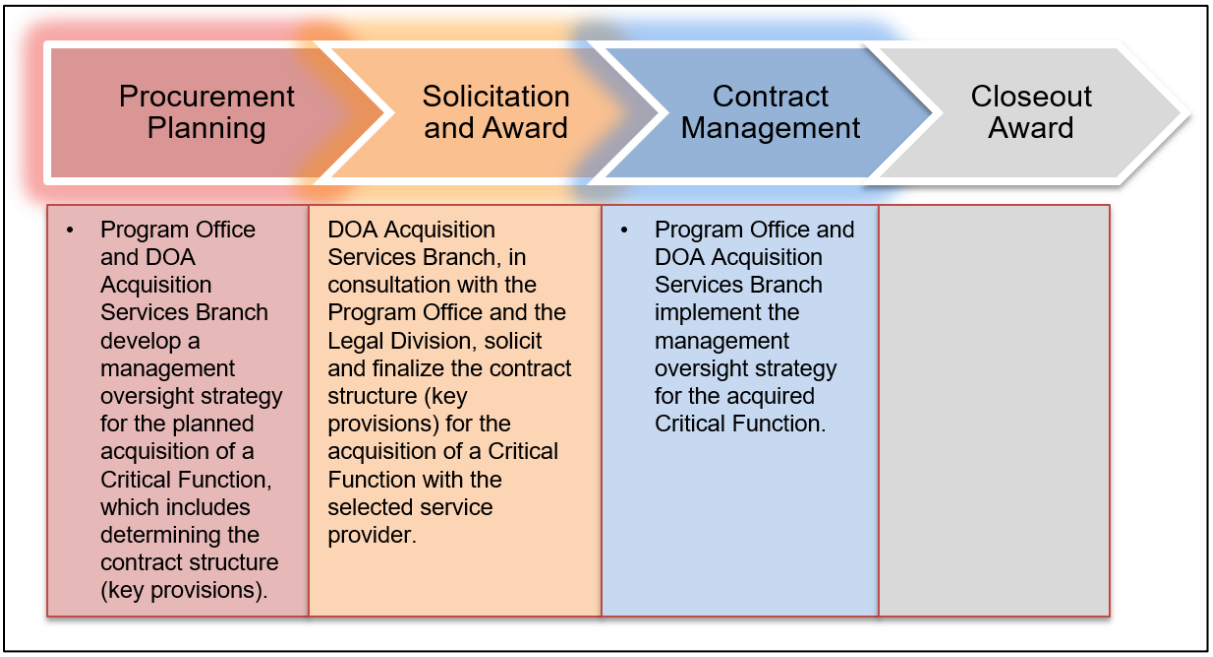
We recommend that the Deputy to the Chairman and Chief Operating Officer:

4) Conduct a procurement risk assessment for Critical Functions during the procurement planning process, for each contract involving Critical Functions. As part of the procurement risk assessment, include a cost effectiveness analysis.

The FDIC Did Not Develop a Management Oversight Strategy for Critical Functions

The FDIC did not develop a management oversight strategy for Critical Functions obtained from Blue Canopy during the procurement planning process, as part of the procurement risk assessment. The FDIC also did not identify the contract structure as recommended by best practices. Figure 4 illustrates the best practices for implementing a management oversight strategy as part of the FDIC's acquisition process.

Figure 4: Best Practices for Implementing a Management Oversight Strategy



Source: OIG analysis of identified best practices and the FDIC's policy and procedures.

Based on our review, we found that the Blue Canopy contracts provided limited coverage of the contractor's obligations and responsibilities for the following:[30]

- **Reports.**[31] As part of the procurement risk assessment, or as a separate management oversight strategy, an agency should identify the contract structure and key contract provisions, such as the types and frequency of reports to be provided and reviewed. Although the contracts required Blue Canopy to submit certain management reports, the contracts did not require Blue Canopy to submit financial reports, audit reports, security reports, business resumption testing reports, and exception-based reports of Blue Canopy's operations. Best practices state that for procured Critical Functions, an agency should periodically

[30] The FDIC has warned its regulated institutions to identify contractual requirements critical to the ongoing assessment and control of risks and, therefore, the FDIC should do the same in its contracts. According to the FDIC Financial Institution Letter, *Third-Party Risk Guidance for Managing Third-Party Risk* (FIL-44-2008) (June 2008), an effective risk management process should identify, in part, contractual requirements that would be critical to the ongoing assessment and control of specific identified risks. The guidance provides, in part, that **reports (types and frequency of management information) and business resumption and contingency plans** should be considered as a contract is structured, with the applicability of each dependent upon the nature and significance of the third-party relationship.

[31] According to FIL-44-2008, for **reports**, "[t]he contract should specify the type and frequency of management information reports to be received from the third party. Routine reports may include performance reports, audits, financial reports, security reports, and business resumption testing reports. Management should also consider mandating exception-based reports that would serve as notification of any changes or problems that could affect the nature of the relationship or pose a risk to the financial institution."

monitor the service provider's ongoing operations, including its financial condition, information security, and business resumption and continuity plans.

The importance of the FDIC reviewing financial and audit reports and periodically monitoring the contractor's operations was demonstrated by the FDIC's experience with Blue Canopy's predecessor. In this case, the FDIC terminated the service provider's contract because of the provider's bankruptcy.[32] As a result of the service provider's failure, the FDIC compressed the procurement planning and solicitation and award processes, and Blue Canopy assumed the previous contract and began providing support services to the FDIC in May 2009 – 3 months after the company's failure.[33] In addition to having limited time to find a replacement contractor, the company's distressed financial condition and ultimate bankruptcy could have impaired or compromised the quality of services provided over an extended period of time – as the contractor's senior management and employees focused on their company's financial turmoil at the expense of the services provided. Ultimately, this situation represents an increased operational risk to the FDIC and a potential risk management failure – where the risk has not been identified, measured, monitored and reported, and mitigated.

A CIOO official confirmed that Blue Canopy was not required to submit routine financial and operational reports, as noted above. Nor did the FDIC actively monitor Blue Canopy's financial condition, information security, and business resumption and continuity. However, in order to mitigate the potential risk of a service provider's financial failure, breach of information security protocols, or failure to ensure service continuity, an agency needs to continuously monitor the service provider's financial condition and operations. In the OIG report, *Contract Oversight*

Prior OIG report. The OIG report, *Contract Oversight Management* (EVAL-20-001) (October 2019), noted that some CIOO Oversight Managers lacked the workload capacity to oversee contracts, and certain Oversight Managers were not properly trained or certified.

Within the report, the OIG recommended, in part, that the Deputy to the Chairman and Chief Operating Officer "[d]etermine the appropriate number of oversight managers needed to manage the Division of Information Technology's (DIT) contract workload in conjunction with DIT, and ensure the Oversight Manager workforce is appropriately staffed."

[32] In February 2009, the FDIC's service provider, BearingPoint Inc., a multinational management and technology consulting firm, filed Chapter 11 bankruptcy. The company filed for bankruptcy with approximately $2.23 billion in total debt and approximately $1.76 billion in total assets as of September 2008. The filing included only the company's U.S. operations. According to a CNN news article titled, *BearingPoint files for bankruptcy* (February 2009), "[t]he McLean, Virginia-based company, which began as the consulting arm of KPMG LLP and later struggled with accounting problems and a U.S. Securities and Exchange Commission probe, has been laboring under heavy debt exacerbated by an acquisition spree between 1999 and 2002."

[33] In comparison, the FDIC's procurement planning and solicitation and award processes for contract CORHQ-14-C-0769 took 9 months (from March 2014 to December 2014), and contract CORHQ-14-C-0778 took 12 months (from March 2014 to March 2015).

Management (EVAL-20-001) (October 2019), the OIG reported concerns about CIOO contract oversight.

Best practices recommend that an agency implement heightened contract monitoring for procured Critical Functions, and identify and control risks. For example, the FDIC provides best practice guidance to financial institutions for monitoring contractor risks. The guidance states that "[a]n institution's board of directors and senior management are ultimately responsible for …identifying and controlling risks arising from [third-party] relationships, to the same extent as if the [contracted] activity were handled within the institution."[34] In particular, the FDIC should have routinely reviewed (actively monitored) Blue Canopy's financial condition, information security, and business resumption and continuity testing reports to ensure the security, confidentiality, integrity, and availability of FDIC information. In order to implement heightened management oversight, the FDIC needs to (1) identify the risk in a risk assessment; (2) identify the control(s) needed to oversee the contractor within a management oversight strategy; (3) establish the control(s) and a process for reviewing the control(s) within the contract structure; (4) implement the control(s) during the management oversight process; and (5) periodically review the FDIC and contractor's performance – or, implementation of the control(s).

- **Business Resumption and Contingency Plans.**[35] As part of the procurement risk assessment, or as a separate management oversight strategy, an agency should identify the contract structure and key contract provisions, such as the review and testing of business resumption and contingency plans. The Blue Canopy contracts provided that if the contractor:

  > [I]s determined by the FDIC (at its sole discretion) to provide services essential or critical to the FDIC mission … the contractor shall take immediate and effective measures to ensure the availability or use of back-up or redundant services and/or system(s) support to deal with such emergency.

  In addition, the FDIC's business resumption and contingency plans rely on Blue Canopy's resources being available to continue its services. However, the FDIC

[34] FDIC Financial Institution Letter titled, *Third-Party Risk Guidance for Managing Third-Party Risk (*FIL-44-2008) (June 2008).
[35] The FDIC has warned its regulated institutions to address in its contractual arrangements, the third parties' responsibility for continuation of services and, therefore, the FDIC should do the same in its contracts. According to the FDIC Financial Institution Letter titled, *Third-Party Risk Guidance for Managing Third-Party Risk* (FIL-44-2008) (June 2008), for **business resumption and contingency plans,** "[t]he contract should address the third party's responsibility for continuation of services provided for in the contractual arrangement in the event of an operational failure, including both man-made and natural disasters. The third party should have appropriate protections for backing up information and also maintain disaster recovery and contingency plans with sufficiently detailed operating procedures. Results of testing of these plans should be provided to the financial institution."

did not make the determination that Blue Canopy provided essential or critical services, even though the Agency dedicated more than 38 percent of its IT security budget to Blue Canopy services. In addition, the contract did not stipulate that Blue Canopy should already have had the appropriate protections for backing up information, and maintaining disaster recovery and contingency plans with sufficiently detailed operating procedures. As noted previously, the contract also did not stipulate that Blue Canopy should have periodically tested its plans and provided the results to the FDIC. Nor did the FDIC require periodic joint testing procedures.

A CIOO official stated that Blue Canopy's business resumption and contingency plans were not a concern because Blue Canopy operated within the FDIC's information systems and on the FDIC's premises. However, while Blue Canopy operated within the FDIC's information systems and facilities, the value that Blue Canopy provided was in its human capital. Therefore, the FDIC should have been concerned about Blue Canopy's business resumption and contingency plans in regards to its ability to provide back-up or additional resources during an adverse event. Further, the official stated that Blue Canopy complied with the FDIC's directives governing access to and operations at FDIC offices and facilities. In addition, the CIOO official stated they would have considered and reviewed Blue Canopy's information security reports at the time of the solicitation and award process. However, there was no indication that the CIOO reassessed the reports during the course of the 7-year performance of these contracts. While Blue Canopy personnel were subject to the FDIC's onsite information security protocols, more proactive controls should have been employed to validate that FDIC data had been retained onsite and not transferred to the contractor's facilities or systems.

A CIOO official also stated that the contractor was responsible for ensuring uninterrupted support of services, if the FDIC determined that Blue Canopy provided services essential or critical to the FDIC mission. However, as explained above, the FDIC did not deem Blue Canopy to provide services essential or critical to the FDIC mission so this is a moot point.

Best practices recommend that contractors have business resumption and contingency plans in place and tested. Additionally, according to best practices, the plans and testing reports should be reviewed on a routine, ongoing (proactive) basis, rather than waiting for and reacting to an unexpected event. In particular, having a business continuity plan in place and testing it helps to continuously improve an organization's ability to successfully recover from various scenarios, whether it be a natural disaster, pandemic, or communications failure. In addition, routine reviews ensure that both contractor and agency staff

know their roles and responsibilities in the event of an unexpected incident, and validate the planned response.

As such, Blue Canopy should have had crisis readiness plans in place and should have tested those plans to ensure that it could continue to provide Critical Functions uninterrupted to the FDIC. These plans should have considered the impact of the crisis, for example, on human resources, facilities, hardware, and information security. As noted previously, in October 2019, the FDIC changed its procurement strategy for these Critical Functions from two contracts to two BOAs and included multiple service providers on the BOAs.

Best practices recommend that an agency implement heightened contract monitoring for procured Critical Functions, to the same extent as if the services were performed internally. In particular, the FDIC should have routinely reviewed (on an ongoing and proactive basis) Blue Canopy's business resumption and continuity plans (specific to human capital) to ensure security, confidentiality, integrity, and availability of FDIC information, as well as the continuity of service and performance by Blue Canopy. Since the FDIC relied on Blue Canopy to provide human capital (staffing) in key areas of information security and privacy, the FDIC needed to supervise and manage how Blue Canopy would continue to provide its services in the event that Blue Canopy's human capital was impaired or negatively impacted by significant events. Additionally, the FDIC needed to routinely test, or review the test results of, those plans to ensure continuity of service. Finally, the FDIC needed to assure itself that it was comfortable with the risks posed by Blue Canopy and the procured Critical Functions – especially if Blue Canopy had not demonstrated that it was adequately prepared for business continuity, resumption, or crisis readiness.

Recommendations

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

5) Develop and implement a management oversight strategy for Critical Functions during the procurement planning process, for each contract involving Critical Functions.

6) Determine the contract structure during the solicitation and award process for the procurement of a Critical Function.

7) Revise the management oversight strategy for the procured Critical Functions performed under the BOAs for Managed Security Services Provider and Security and Privacy Professional Services to ensure that the strategy aligns with best practices.

The FDIC Did Not Conduct Periodic Reviews of Controls and Processes for Critical Functions

The FDIC did not conduct periodic reviews of controls and processes for Critical Functions obtained from Blue Canopy during the contract management process, even though the Agency dedicated more than 38 percent of its Information Technology security budget to Blue Canopy services in 2019. These reviews should have included assessments of the contractor and Agency personnel performance, human capital planning, and over-reliance.

Best practices indicate that an agency should perform periodic reviews of its controls and processes to ensure that those controls and processes are adhered to and operating as intended, and that the agency maintains control of its mission and operations. These periodic reviews should be focused on targeted controls or areas of performance (such as personnel performance or human capital planning), and/or performed more broadly (such as a contractor over-reliance assessment). The overall objective of such reviews is to identify, assess, and resolve indications of contractor over-reliance. Without such reviews, an agency may become over-reliant on a service provider if it does not have the capacity (number of Federal employees) and capability (Federal employees with appropriate training, experience, and expertise) to understand the agency's requirements, formulate alternatives, manage the work product, monitor the contractors used to support the Federal workforce, and adequately mitigate the potential impact on mission performance if contractors were to default on their obligations.

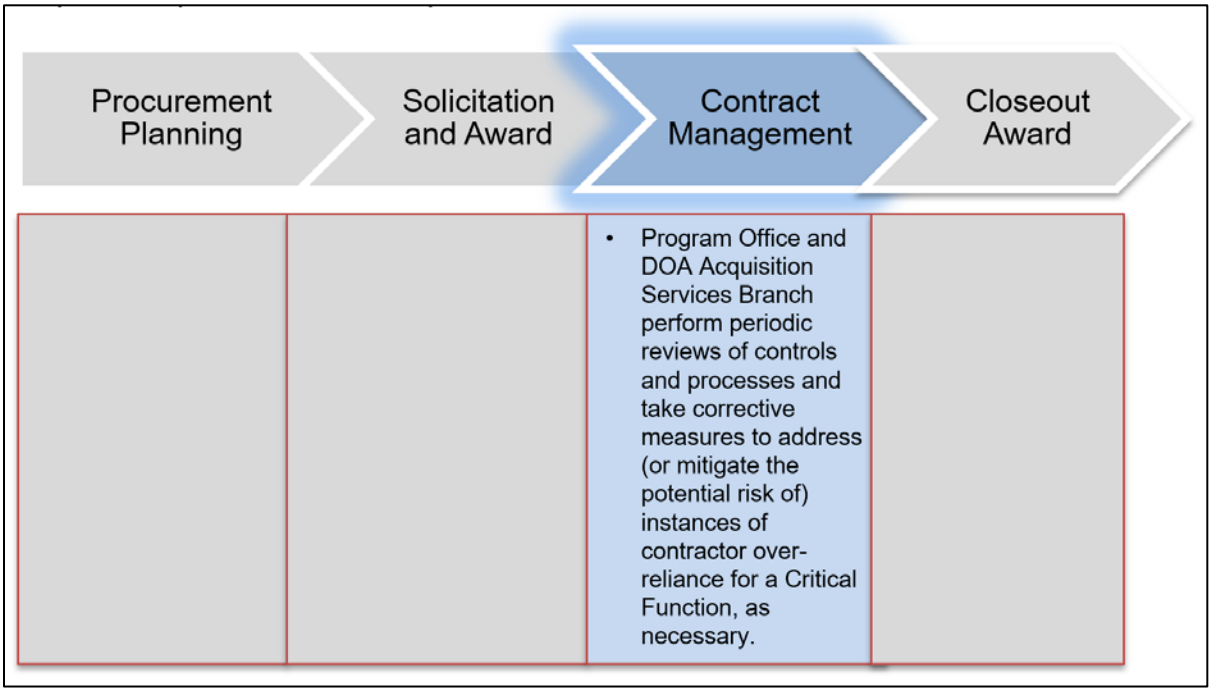
As previously noted, the FDIC and Blue Canopy's contractual arrangement allowed Blue Canopy to assess certain security controls, including configuration management controls. Blue Canopy was also assigned duties related to design and/or execution of these controls. This arrangement lacked independence and represents a failure on the FDIC's part to maintain control of its operations.[36] In addition, the absence of heightened contract monitoring processes, such as a procurement risk assessment and periodic reviews of controls and processes for Critical Functions allowed this internal control weakness to remain undetected.

Since the FDIC did not perform periodic reviews, it did not (1) assess for contractor over-reliance – within individual controls and processes or on an aggregate basis; and (2) identify and implement corrective actions needed during the contract management process related to indicators of potential operational/process failures.

Figure 5 illustrates the best practices for periodic reviews for contractor over-reliance and implementation of corrective measures during the FDIC's acquisition process.

[36] *Security Configuration Management of the Windows Server Operating System* (AUD-19-004) (January 2019).

Figure 5: Best Practices for Conducting Periodic Reviews of Controls and Processes



Source: OIG analysis of identified best practices and the FDIC's policy and procedures.

The FDIC did not identify or implement periodic reviews specific to the risks associated with procured services for Critical Functions. In particular, the FDIC prepared a Contract Management Plan[37] for Blue Canopy to document the joint administrative approach agreed upon by the Contracting Officer and Oversight Manager. The Contract Management Plan addressed general oversight roles and responsibilities, and the evaluation/acceptance of the contractor's performance. However, it did not address how the Contracting Officer and Oversight Manager would assess the FDIC's over-reliance on Blue Canopy or identify and implement corrective actions. These elements are essential components of the heightened review and oversight process for procurements of Critical Functions.

[37] A **Contract Management Plan** is a plan developed by the Contracting Officer and the Oversight Manager that documents the joint administration approach to performing oversight activities for complex contracts for services. The objective of the plan is to ensure that the Contracting Officer, Oversight Manager, and Technical Monitor have a common understanding of both contractor and FDIC obligations under the contract. A Contract Management Plan must be developed for the acquisition of services having a total estimated value of $1 million and greater.

Recommendations

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

8) Identify missing or insufficient controls in the BOAs and task orders for Managed Security Services Provider and Security and Privacy Professional Services, and implement appropriate corrective actions or compensating controls.

9) Implement periodic reviews for procured Critical Functions, including for the BOAs and task orders for Managed Security Services Provider and Security and Privacy Professional Services.

10) Determine when and how to assess for contractor over-reliance as part of the management oversight strategy.

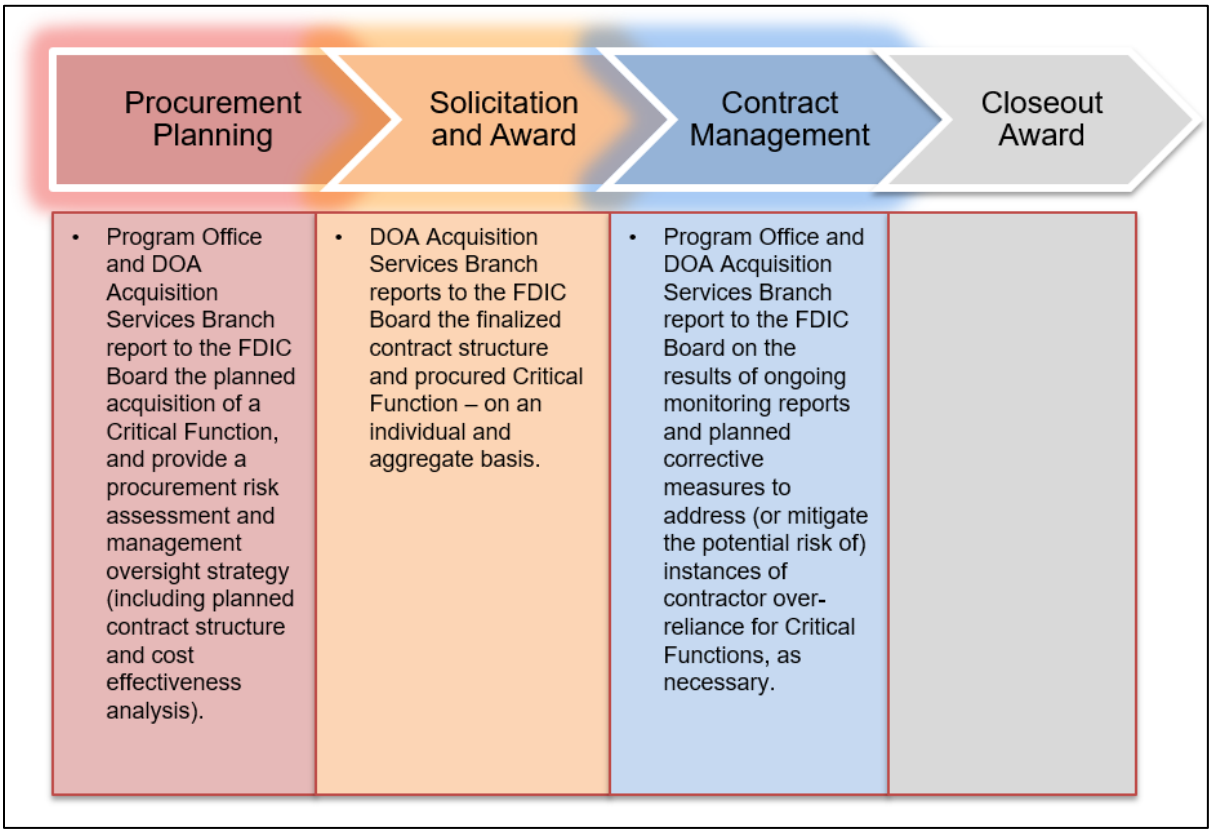
11) Implement corrective actions when the FDIC determines it is over-reliant on a contractor for a procured Critical Function.

The FDIC Did Not Report to Its Board of Directors on Critical Functions

The FDIC did not report to the Board on procured Critical Functions during the procurement planning, solicitation and award, and contract management phases of the acquisition process. Figure 6 illustrates the best practices for Board reporting in the FDIC's acquisition process.

As noted previously, the Board approves the execution of contracts with dollar values over $20 million and contract modifications to contracts previously approved by the Board that increase the award amount or period of performance by more than 15 percent.

Figure 6: Best Practices for FDIC Board Reporting



Source: OIG analysis of identified best practices and the FDIC's policy and procedures.

The FDIC's OCISO and DOA submitted to the Board, through its established procurement process, a Board Case Package and Award Profile Reports.[38] These documents, however, did not identify the procured services that were Critical Functions nor did they present the planned or implemented heightened oversight management activities for the Critical Function procurements. Specifically, the FDIC did not discuss with the Board its procurement risk assessment, management oversight strategy, contract structuring, and ongoing monitoring reports for the procured Critical Functions.

In particular, we found the following:

- **Board Case Package**. The FDIC OCISO and DOA submitted a Board Case Package to the Board that requested approval for the authority to contract for services to support the Information Security and Privacy Program. While the Board Case Package identified the services to be procured, it did not identify or

[38] An **Award Profile Report** is a report that summarizes FDIC contracting activity on a quarterly basis. The report summarizes general contracting-related information and details pending awards and award profiles. In particular, the reports are intended to provide detailed profiles for those awards and award categories with a value of $20 million or more as well as those that require greater oversight due to the nature of the scope of work and risk to the FDIC.

discuss whether the services to be procured were considered to be Critical Functions of the FDIC. Similarly, the Board meeting minutes did not identify the procured services as Critical Functions. Neither the Board Case Package nor the Board meeting minutes reflected that the FDIC discussed with the Board its procurement risk assessment and management oversight strategy, planned contract structuring, and ongoing monitoring controls and reports for the procured Critical Functions.

- **Award Profile Reports.** On a quarterly basis, the FDIC submitted Award Profile Reports to the Board that summarized the FDIC's contracting activities for the quarter. For more than 5 years (from the quarters ended March 2015 to June 2019), DOA submitted a summary status report (an award profile) for only one of the two contracts with Blue Canopy. During the second quarter 2019, DOA provided summary status reports on both contracts after the second contract was modified to increase the contract value above the Board's reporting threshold.

  While the Award Profile Reports described the procured services, assessed contractor performance, tracked fund utilization/allocation, and assessed FDIC contract oversight, the FDIC did not identify Blue Canopy's procured services as Critical Functions. Nor did the reports identify any other procured services as Critical Functions of the FDIC. As a result, the reports did not identify for the Board information on the procurement and oversight of procured Critical Functions on an individual and aggregate contract basis as suggested by best practices.

Prior OIG report. The OIG report, *Contract Oversight Management* (EVAL-20-001) (October 2019), noted that while the information in the Award Profile Report was "important for the Board of Directors to understand the status of higher risk FDIC acquisitions as of a specific point in time, it does not provide the Board or other senior management officials with a portfolio-wide view or the ability to analyze historical contracting trends across the portfolio, identify anomalies, and perform ad hoc analysis to identify risk or plan for future acquisitions."

Within the report, the OIG recommended, in part, that the FDIC "[p]rovide enhanced contract portfolio reports to FDIC executives, senior management, and the Board of Directors."

Recommendations

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

12) Report to the Board about the Procurement Risk Assessments, Management Oversight Strategies, and contract provisions that address identified risks for planned Critical Functions during the procurement planning phase of the acquisition, for its consideration.

13) Report to the Board about the Award Profile Reports and corresponding status reports for procured Critical Functions during the contract management phase of the acquisition process on an individual and aggregate contract basis, for its consideration.

FDIC COMMENTS AND OIG EVALUATION

On March 26, 2021, the FDIC's Deputy to the Chairman, Chief of Staff, and Chief Operating Officer provided a written response to a draft of this report (FDIC Response), which is presented in its entirety in Appendix 5.

In its response, the FDIC stated that it is committed to continually improving its contracting processes and controls. The FDIC acknowledged that it is engaged in efforts to improve its acquisition services and oversight management programs. The FDIC stated that it envisions developing criteria for identifying contracts that support essential functions or that provide services needed in a business continuity event.

The FDIC, however, has expressed reluctance to incorporate the term, "Critical Function," into its process, as that term is used and defined in the OMB Policy Letter 11-01. The definition of essential functions as used by the FDIC is restricted to those functions that impact continuity of operations planning. Critical Functions, on the other hand, are broader and cover all functions that are necessary to the agency being able to effectively perform and maintain control of its mission and operations.

The FDIC asserted that some of the procurement controls contemplated in the OMB Policy Letter may already exist within the FDIC's current acquisition policies and guidance, and we recognize that the FDIC has implemented certain procedures as part of its procurement process. However, in relation to overseeing contractors who perform Critical Functions on behalf of the FDIC, the Agency procedures fell short in several important respects, including with respect to conducting periodic reviews to assess for over-reliance on the contractor. In fact, Blue Canopy services represented nearly 40 percent of the FDIC's annual operating expenses for Information Security ($42.3 million), and the FDIC did not have a sufficient process to identify these Critical Functions and implement heightened monitoring.

As discussed in our report, the FDIC could have done more to identify and oversee procured Critical Functions. The FDIC did not have a process for identifying Critical Functions in procurements at the outset, and this gap created a cascading effect of shortfalls in overseeing Critical Functions. Notably, the FDIC stated in its response

that "if the FDIC determines contract services are essential in the event of an emergency or business continuity event, the statement of work or statement of objectives must include: business continuity requirements, requirements that contractors flow emergency preparedness and continuity requirements to essential subcontracts; and requirements for contractors to have emergency plans for providing services to FDIC in the event of a disruption of normal operations, and participation in FDIC business continuity testing, training, and exercises."

However, as noted in our report, the FDIC did not identify the Blue Canopy contracts as "essential," and, therefore, it did not invoke the additional monitoring and oversight procedures. This example highlights the need for the FDIC to clearly define the terminology related to Critical Functions and incorporate the underlying concepts embodied in Critical Functions, so that it can readily identify Critical Functions in such procurements and take appropriate actions with heightened monitoring and controls.

The FDIC disagreed with the proposition that the Agency's framework did not meet the "third-party risk management principles outlined in the [FDIC's Financial Institution Letter, Guidance for Managing Third-Party Risk]." However, while the framework requires reports for contracts deemed to be essential, the FDIC did not make this determination for the Blue Canopy contracts. Therefore, our report correctly concludes that the Blue Canopy contracts provided limited coverage of the contractor's obligations and responsibilities similar to those recommended in the FDIC's Financial Institution Letter.

The FDIC response further disagreed that the weaknesses identified in our prior OIG report regarding the Security Configuration Management of the Windows Server Operating System "represent[ed] a failure on the FDIC's part to maintain control of its operations." We note that the FDIC previously recognized the problem and took remedial actions to address the independence concern identified in the prior OIG report.

In addition, we maintain that these circumstances represented a failure in the FDIC's controls and procedures. As discussed in this report on Critical Functions, the procedures are not adequate to ensure that periodic reviews are performed to assess the contractor for over-reliance and to identify and implement corrective actions. In addition, it should be noted that the OIG's findings and recommendations on the FDIC's procurement process for Critical Functions cover all such contracts and is not limited to the Blue Canopy contracts.

We understand that the FDIC may consider implementing a process in order to identify Critical Functions and employ heightened monitoring and controls. The FDIC, however, provided no details as to how it plans to do so.

The FDIC concurred with 1 of the 13 recommendations, and plans to complete corrective action by May 31, 2021. The FDIC stated that it partially concurred with the remaining 12 recommendations; however, the FDIC response did not provide specific actions taken or planned. As a result, we consider the remaining 12 recommendations to be unresolved at this time. To resolve these 12 recommendations, we would expect that the FDIC provide a clear indication of the specific actions within the next 6 months, and we will determine whether the recommendations may be converted to being "resolved" at that time, or whether they will remain as "unresolved."

The FDIC response indicated that its planned corrective actions will include surveying recognized practices and procedures associated with contracts supporting essential functions. In order to close these recommendations, we would expect that the FDIC implement a process to assess contractor over-reliance at the Agency and take the following actions:

- Identify contracts requiring heightened monitoring and controls during the procurement planning, award, and contract management phases of the acquisition process;
- Conduct procurement risk assessments for its contracts, including a cost-effectiveness analysis;
- Implement a management oversight strategy for contracts requiring heightened monitoring and controls;
- Implement periodic reviews for contracts requiring heightened monitoring and controls;
- Incorporate enhancements to the FDIC's existing acquisition planning, approval, reporting, and oversight processes;
- Conduct an assessment to determine whether FDIC's current Risk Inventory sufficiently addresses the underlying risks presented in the OIG's report; and
- Report to the Board planned and procured Critical Functions on an individual and aggregate basis.

Upon completion of the corrective actions and before closing the recommendations, we will review the FDIC's actions to ensure that the revised acquisition process includes guidance for identifying planned procurements of Critical Functions and implementing heightened contract monitoring for Critical Functions.

For the 12 unresolved recommendations, the FDIC plans to consider and further study the issues and does not intend to implement corrective actions for another year (between March 31 and June 30, 2022).

We also provided Blue Canopy with a draft copy of the report to review for factual

accuracy. We considered Blue Canopy's informal feedback before finalizing the report.

Objectives

Our evaluation assessed whether:

1. Blue Canopy performed Critical Functions as determined by OMB Policy Letter 11-01 and best practices; and
2. If so, whether the FDIC retained sufficient management oversight of Blue Canopy to maintain control of its mission and operations in accordance with best practices.

According to the FDIC's Legal Division, OMB Policy Letter 11-01 does not directly apply to the Agency but it may be used for guidance. For evaluation purposes, the OIG considers this guidance a best practice.

We performed our work from May 2020 through November 2020 at the FDIC's offices in Arlington, Virginia and Dallas, Texas. We performed our work in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation.

Scope and Methodology

The evaluation's scope included our review of Blue Canopy's two existing contracts[39] with the FDIC's Chief Information Officer Organization to determine if Blue Canopy performed Critical Functions within the FDIC's operations; and, if so, whether the FDIC sufficiently oversaw Blue Canopy to maintain control of the Agency's mission and operations.

To address our objectives, we conducted the following procedures:

- Analyzed Blue Canopy's contracts and contractual services for Critical Functions by comparing and contrasting activities to the following:
  - Industry practices and standards;
  - Other best practices the OIG identified; and
  - The FDIC's Enterprise Risk Management Inventory.

- Analyzed the FDIC's oversight of Blue Canopy to maintain control of the Agency's mission and operations by:
  - Comparing and contrasting management procurement and oversight activities to best practices the OIG identified; and

[39] Contracts CORHQ-14-C-0769 and CORHQ-14-C-0778.

  - Comparing and contrasting DOA, CIOO, and the Legal Division's policy and procedures related to management procurement and oversight activities to best practices the OIG identified.

- Gained an understanding of Federal procurement and oversight control processes by reviewing Federal regulations, government-wide guidance, and best practices, including:
  - Office of Management and Budget Office of Federal Procurement Policy, Policy Letter 11-01, *Performance of Inherently Governmental and Critical Functions* (September 2011);
  - OMB Circular A-76, *Performance of Commercial Activities* (May 2003);
  - Federal Activities Inventory Reform Act of 1998 (October 1998); and
  - Federal Acquisition Regulation (2019).

- Reviewed the FDIC's policy and procedures, including:
  - *FDIC Acquisition Policy Manual* (August 2008);
  - *Acquisition Procedures, Guidance and Information* (January 2020) document; and
  - FDIC Financial Institution Letter: *Third-Party Risk Guidance for Managing Third-Party Risk* (FIL-44-2008) (June 2008).

- Considered the following U.S. Government Accountability Office reports:
  - GAO Report, *DHS Service Contracts: Increased Oversight Needed to Reduce the Risk Associated with Contractors Performing Certain Functions* (GAO-20-417) (May 2020);
  - GAO Report, *Support Service Contracts: NNSA Could Better Manage Potential Risks of Contractors Performing Inherently Governmental Functions* (GAO-19-608) (September 2019);
  - GAO Report, *Human Capital: Additional Steps Needed to Help Determine the Right Size and Composition of DOD's Total Workforce* (GAO-13-470) (May 2013); and
  - GAO Report*, VA Health Care: Additional Guidance, Training, and Oversight Needed to Improve Clinical Contract Monitoring* (GAO-14-54) (October 2013).

- Reviewed the following OIG reports:
  - *Contract Oversight Management* (EVAL-20-001) October 28, 2019;
  - *The FDIC's Receivership Basic Ordering Agreements for Business Process Operations Services* (AUD-14-006) March 31, 2014;
  - *Security Configuration Management of the Windows Server Operating System* (AUD-19-004) January 16, 2019; and
  - *The FDIC's Implementation of Enterprise Risk Management* (EVAL-20-005) July 8, 2020.

- Interviewed FDIC personnel in DOA, CIOO, and the Legal Division who had responsibility for procurement processes related to Critical Functions.

- Interviewed officials at other Federal agencies (independent financial regulatory agencies, other independent agencies, and executive branch agencies) to understand their procurement and oversight contractual arrangements for the performance of Critical Functions.

- Reviewed articles and Congressional Research regarding Federal procurement and oversight control processes.

We applied internal control principles promulgated by the GAO (the Green Book) to guide our work and to supplement and support the best practices that we identified, when appropriate. For example, we considered internal controls standards, and activities, related to (1) the control environment (such as, the organizational structure and assigned responsibility; and, the commitment to recruit, develop, and retain competent individuals); and (2) control activities (such as, documented policies, procedures, techniques, and mechanisms that enforce management directives).

We identified the following commonly acknowledged best practices from selected sources.

Best Practices	OMB	GAO	Industry Standard	Select Federal Agencies
1. Identify planned procurement of Critical Functions.	✓	✓	✓	✓

- **OMB Guidance.** OMB Policy Letter 11-01 advises certain agencies that they should ensure that Federal employees perform and/or manage Critical Functions to the extent necessary for the agency to operate effectively and maintain control of its mission and operations. According to the FDIC's Legal Division, OMB Policy Letter 11-01 does not directly apply to the Agency but it may be used for guidance. In particular, the policy letter states that agencies should determine whether their procurement requirements involve the performance of Inherently Governmental Functions, Functions Closely Associated with Inherently Governmental Functions, or Critical Functions. OMB Policy Letter 11-01 also states that "[d]etermining the criticality of a function requires the exercise of informed judgment by agency officials. The criticality of the function depends on the mission and operations, which will differ between agencies and within agencies over time. In making that determination, the officials shall consider the importance that a function holds for the agency and its mission and operations. The more important the function, the more important that the agency have internal capability to maintain control of its mission and operations."

- **GAO Recommendations.** The GAO report, *Human Capital: Additional Steps Needed to Help Determine the Right Size and Composition of DOD's Total Workforce* (GAO-13-470) (May 2013) found, in part, that the DOD's current policies did not fully reflect federal policy concerning the identification of Critical Functions. OMB Policy Letter 11-01 requires agencies to identify and ensure that they retain control over Critical Functions that are core to the agency's mission, but may be contracted out to the private sector. DOD's policies and procedures predated the publication of this requirement, and consequently contained no reference to it. Ultimately, absent specific policies and procedures on this process, DOD may lack assurance that it retains enough government employees to maintain control over these important functions.

  As a result, the GAO recommended, in part, that the DOD should "revise existing workforce policies and procedures to address the … identification of critical functions."

- **Industry Standard.** According to the FDIC's Financial Institution Letter titled *Third-Party Risk Guidance for Managing Third-Party Risk* (FIL-44-2008) (June 2008), "[a]n institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution." In addition, the guidance "provides a general framework that boards of directors and senior management may use to provide appropriate oversight and risk management of significant third-party relationships." A third-party relationship should be considered significant if, in part, the third party performs critical functions; or, the third party stores, accesses, transmits, or performs transactions on sensitive customer information.

- **Federal Agencies.** Federal agencies have processes to identify, record, monitor, and report on procured Critical Functions. For example, CFPB, DOE, and NASA rely upon their annual inventory of service contracts to identify, monitor, and report on procured Critical Functions. In addition, the GSA and OCC report on procurement actions through the Federal Procurement Data System-Next Generation (FPDS-NG),* which includes those designated as Critical Functions. Conversely, the FRB stated that they do not contract out Critical Functions.

  Based on the agencies we interviewed, 75 percent (6 of 8) of Federal agencies had contracting policies, procedures, and controls that address Critical Functions.

* The **FPDS-NG** is the current central repository of information on Federal contracting. The system contains detailed information on contract actions over $3,000, since fiscal year 2004. According to the GSA, the Federal government uses the reported data to measure and assess the impact of Federal procurement on the nation's economy, learn how awards are made to businesses in various socioeconomic categories, understand the impact of full and open competition on the acquisition process, and address changes to procurement policy. The FPDS-NG system includes reporting fields that capture services designated as Critical Functions.

2. Implement heightened contract monitoring processes for Critical Functions.	✓	–	✓	✓

- **OMB Guidance.** OMB Policy Letter 11-01 advises certain agencies that they should ensure that Federal employees perform and/or manage Critical Functions to the extent necessary for the agency to operate effectively and maintain control of its mission and operations. According to the FDIC's Legal Division, OMB Policy Letter 11-01 does not directly apply to the Agency but it may be used for guidance. In particular, the policy letter states that "[a]gencies shall develop and maintain internal procedures to address the requirements of this guidance." In addition, the policy letter states that agencies should determine the type and level of management attention necessary to ensure that functions that should be reserved for Federal performance are not materially limited by or effectively transferred to contractors and that functions suitable for contractor performance are properly managed.

- **Industry Standard.** According to the FDIC's Financial Institution Letter titled *Third-Party Risk Guidance for Managing Third-Party Risk* (FIL-44-2008) (June 2008), the key to the effective use of a third party in any capacity is for management to appropriately assess, measure, monitor, and control the risks associated with the relationship. One of the risk management process's four main elements is oversight. In particular, "[m]anagement should allocate sufficient qualified staff to monitor significant third-party relationships and provide the necessary oversight… The extent of oversight of a particular third-party relationship will depend upon the potential risks and the scope and magnitude of the arrangement."

- **Federal Agencies.** Federal agencies implemented heightened contract monitoring processes, such as identifying and monitoring for Critical Functions, developing a management oversight strategy, performing cost effectiveness analysis, determining contract structure and key provisions, and performing periodic reviews.

  For example, the following agencies noted heightened contracting monitoring, such as:
  - **Identify and Monitor for Critical Functions.** GSA, NASA, USDA, DOE, OCC, and CFPB have policy and procedures, or follow OMB guidance, related to Critical Functions.
  - **Develop a Management Oversight Strategy.** NASA, USDA, and CFPB performed, or considered it a best practice to perform, strategic human capital planning. In addition, NASA considered internal capability when procuring a Critical Function, and CFPB ensured that Contract Officers have appropriate backgrounds, such as Information Technology expertise for procured Information Technology services.
  - **Perform a Cost Effectiveness Analysis.** NASA, USDA, and DOE performed, or considered it a best practice to perform, a cost effectiveness analysis.
  - **Determine Contract Structure.** USDA, CFPB, and OCC used, or considered it a best practice to have, contract provisions to specify the agency's rights and the contractors obligations and responsibilities surrounding Critical Functions.
  - **Perform Periodic Reviews**. GSA, NASA, USDA, DOE, and OCC have policy and procedures to prevent over-reliance on a contractor, and specific corrective measures to address instances of contractor over-reliance. Although NCUA and CFPB did not have an explicit written policy, they noted the actions/procedures they would take to address an instance of contractor over-reliance. In addition, GSA, NASA, USDA, DOE, OCC, NCUA, and CFPB have procedures to oversee the contractor's performance and their own personnel's oversight of a contractor.

3. Perform a procurement risk assessment.	✓	✓	✓	✓

- **OMB Guidance.** OMB Policy Letter 11-01 advises certain agencies that they should ensure that Federal employees perform and/or manage Critical Functions to the extent necessary for the agency to operate effectively and maintain control of its mission and operations. According to the FDIC's Legal Division, OMB Policy Letter 11-01 does not directly apply to the Agency but it may be used for guidance. In particular, the policy letter states that agencies should determine the type and level of management attention necessary to ensure that functions that should be reserved for Federal performance are not materially limited by or effectively transferred to contractors and that functions suitable for contractor performance are properly managed.

  The OMB policy letter also states that "[w]here a critical function is not inherently governmental, the agency may appropriately consider filling positions dedicated to the function with both Federal employees and contractors. However, to meet its fiduciary responsibility to the taxpayers, the agency must have sufficient internal capability to control its mission and operations… Sufficient internal capability—(i) generally requires that an agency have an adequate number of positions filled by Federal employees with appropriate training, experience, and expertise to understand the agency's requirements, formulate alternatives, take other appropriate actions to properly manage and be accountable for the work product, and continue critical operations with in-house resources, another contractor, or a combination of the two, in the event of contractor default; and (ii) further requires that an agency have the ability and internal expertise to oversee and manage any contractors used to support the Federal workforce… Determinations concerning what constitutes sufficient internal capability must be made on a case-by-case basis taking into account, among other things the: (i) agency's mission; (ii) complexity of the function and the need for specialized skill; (iii) current strength of the agency's in-house expertise; (iv) current size and capability of the agency's acquisition workforce; and (v) effect of contractor default on mission performance." As part of acquisition planning, agencies shall confirm that for the Critical Functions to be procured, the agency has sufficient internal capability to control its mission and operations.

- **GAO Recommendations.** The GAO report, *DHS Service Contracts: Increased Oversight Needed to Reduce the Risk Associated with Contractors Performing Certain Functions* (GAO-20-417) (May 2020), found, in part, that DHS did not consistently plan for the level of Federal oversight needed for certain contracts because there was no guidance on how to document and update the number of Federal personnel needed to conduct oversight. GAO also found that DHS personnel did not identify specific oversight activities they conducted to mitigate the risk of contractors performing functions in a way that could become inherently governmental. DHS also lacked guidance on what these oversight tasks could detail. Ultimately, the GAO concluded that without guidance for documenting and updating the planned Federal oversight personnel needed, and identifying oversight tasks, DHS cannot mitigate the risks associated with service contracts in need of heightened management attention.

  As a result, the GAO recommended that DHS should (1) "develop a risk-based approach for reviewing service requirements … to ensure proposed service requirements are clearly defined and reviewed before planning how they are to be procured…"; (2) "update the Inherently Governmental and Critical Functions Analysis to provide guidance for analyzing, documenting, and updating the federal workforce needed to perform or oversee service contracts requiring heightened management attention..."; and (3) "[develop] guidance identifying oversight tasks or safeguards personnel can perform, when needed, to mitigate the risk associated with contracts containing closely associated with inherently governmental functions, special interest functions, or critical functions."

  The GAO report, *Human Capital: Additional Steps Needed to Help Determine the Right Size and Composition of DOD's Total Workforce* (GAO-13-470) (May 2013), found, in part, that DOD's current policies did not fully reflect federal policy concerning the identification of Critical Functions. OMB Policy Letter 11-01 requires agencies to identify and ensure that they retain control over Critical Functions that are core to the agency's mission but may be contracted out to the private sector. DOD's policies and procedures predated the publication of this requirement, and consequently contained no reference to it. Ultimately, absent specific policies and procedures on this process, DOD may lack assurance that it retains enough government employees to maintain control over these important functions.

  As a result, the GAO recommended, in part, that DOD should "revise existing workforce policies and procedures to address the determination of the appropriate workforce mix..."

- **Industry Standard.** According to the FDIC's Financial Institution Letter titled *Third-Party Risk Guidance for Managing Third-Party Risk* (FIL-44-2008) (June 2008), the key to the effective use of a third party in any capacity is for management to appropriately assess, measure, monitor, and control the risks associated with a contractual relationship. While engaging another entity may assist management and the board in achieving strategic goals, such an arrangement reduces management's direct control and introduces risks. Accordingly, institutions should establish and maintain an effective risk management process for initiating and overseeing outsourced operations.

  An effective third-party risk management process has four elements:
  - Risk assessment,
  - Due diligence in selecting a third-party service provider,
  - Contract structuring and review, and
  - Ongoing monitoring.

  Taken together, these elements compose the financial institution's risk management analysis of the third-party relationship.

- **Federal Agencies.** When procuring Critical Functions, agencies considered strategic human capital planning – analyzing agency staff resources, internal capability and capacity, and cost.

  For example, as noted above, the following agencies noted heightened contracting monitoring, such as:
  - **Develop a Management Oversight Strategy.** NASA, USDA, and CFPB performed, or considered it a best practice to perform, strategic human capital planning. In addition, NASA considered internal capability when procuring a Critical Function, and CFPB ensured that Contract Officers had appropriate backgrounds, such as Information Technology expertise for procured Information Technology services.
  - **Perform a Cost Effectiveness Analysis.** NASA, USDA, and DOE performed, or considered it a best practice to perform, a cost effectiveness analysis.

4. Perform a cost effectiveness analysis.	✓	–	✓	✓

- **OMB Guidance.** OMB Policy Letter 11-01 advises certain agencies that they should ensure that Federal employees perform and/or manage Critical Functions to the extent necessary for the agency to operate effectively and maintain control of its mission and operations. According to the FDIC's Legal Division, OMB Policy Letter 11-01 does not directly apply to the Agency but it may be used for guidance. In particular, the policy letter states that agencies should determine the type and level of management attention necessary to ensure that functions that should be reserved for Federal performance are not materially limited by or effectively transferred to contractors and that functions suitable for contractor performance are properly managed.

  The OMB policy letter also states that "[w]here a critical function is not inherently governmental, the agency may appropriately consider filling positions dedicated to the function with both Federal employees and contractors. However, to meet its fiduciary responsibility to the taxpayers, the agency … must ensure it is cost effective to contract for the services."

- **Industry Standard.** According to the FDIC's Financial Institution Letter titled *Third-Party Risk Guidance for Managing Third-Party Risk* (FIL-44-2008) (June 2008), the key to the effective use of a third party in any capacity is for management to appropriately assess, measure, monitor, and control the risks associated with a contractual relationship. As part of a risk assessment, the institution should analyze the benefits and costs associated with the proposed relationship.

  According to this guidance, a "[r]isk assessment is fundamental to the initial decision of whether or not to enter into a third-party relationship. The first step in the risk assessment process should be to ensure that the proposed relationship is consistent with the institution's strategic planning and overall business strategy. Next, management

should analyze the benefits, costs, legal aspects, and the potential risks associated with the third party under consideration… It is key for management to develop a thorough understanding of what the proposed relationship will accomplish for the institution, and why the use of a third party is in its best interests. A risk/reward analysis should be performed for significant matters, comparing the proposed third-party relationship to other methods of performing the activity or product offering, including the use of other vendors or performing the function in-house. For such matters, the analysis should be considered integral to the bank's overall strategic planning, and should thus be performed by senior management and reviewed by the board or an appropriate committee."

- **Federal Agencies**. When procuring Critical Functions, agencies considered (or, considered as a best practice) cost effectiveness analysis, which included analyzing the appropriate mix of Federal employees and contractors and rebalancing, as needed.

  For example, as noted above, the following agencies noted heightened contracting monitoring, such as:
  - **Perform a Cost Effectiveness Analysis.** NASA, USDA, and DOE performed, or considered it a best practice to perform, a cost effectiveness analysis.

5. Develop a management oversight strategy.	✓	✓	✓	✓

- **OMB Guidance.** OMB Policy Letter 11-01 advises certain agencies that they should ensure that Federal employees perform and/or manage Critical Functions to the extent necessary for the agency to operate effectively and maintain control of its mission and operations. According to the FDIC's Legal Division, OMB Policy Letter 11-01 does not directly apply to the Agency but it may be used for guidance. In particular, the policy letter states that agencies should determine the type and level of management attention necessary to ensure that functions that should be reserved for Federal performance are not materially limited by or effectively transferred to contractors and that functions suitable for contractor performance are properly managed.

  The OMB policy letter also states that "[w]here a critical function is not inherently governmental, the agency may appropriately consider filling positions dedicated to the function with both Federal employees and contractors. However, to meet its fiduciary responsibility to the taxpayers, the agency must have sufficient internal capability to control its mission and operations… Sufficient internal capability—(i) generally requires that an agency have an adequate number of positions filled by Federal employees with appropriate training, experience, and expertise to understand the agency's requirements, formulate alternatives, take other appropriate actions to properly manage and be accountable for the work product, and continue critical operations with in-house resources, another contractor, or a combination of the two, in the event of contractor default; and (ii) further requires that an agency have the ability and internal expertise to oversee and manage any contractors used to support the Federal workforce… Determinations concerning what constitutes sufficient internal capability must be made on a case-by-case basis taking into account, among other things the: (i) agency's mission; (ii) complexity of the function and the need for specialized skill; (iii) current strength of the agency's in-house expertise; (iv) current size and capability of the agency's acquisition workforce; and (v) effect of contractor default on mission performance." As part of acquisition planning, agencies shall confirm that for the Critical Functions to be procured, the agency has sufficient internal capability to control its mission and operations.

- **GAO Recommendations.** The GAO report, *DHS Service Contracts: Increased Oversight Needed to Reduce the Risk Associated with Contractors Performing Certain Functions* (GAO-20-417) (May 2020), found, in part, that DHS did not consistently plan for the level of Federal oversight needed for certain contracts because there was no guidance on how to document and update the number of Federal personnel needed to conduct oversight. GAO also found that DHS personnel did not identify specific oversight activities they conducted to mitigate the risk of contractors performing functions in a way that could become inherently governmental. DHS also lacked guidance on what these oversight tasks could entail. Ultimately, the GAO concluded that without guidance for documenting and updating the planned Federal oversight personnel needed, and identifying oversight tasks, DHS cannot mitigate the risks associated with service contracts in need of heightened management attention.

As a result, the GAO recommended that the DHS should (1) "develop a risk-based approach for reviewing service requirements … to ensure proposed service requirements are clearly defined and reviewed before planning how they are to be procured…"; (2) "update the Inherently Governmental and Critical Functions Analysis to provide guidance for analyzing, documenting, and updating the federal workforce needed to perform or oversee service contracts requiring heightened management attention..."; and (3) "[develop] guidance identifying oversight tasks or safeguards personnel can perform, when needed, to mitigate the risk associated with contracts containing closely associated with inherently governmental functions, special interest functions, or critical functions."

- **Industry Standard.** According to the FDIC's Financial Institution Letter titled *Third-Party Risk Guidance for Managing Third-Party Risk* (FIL-44-2008) (June 2008), the key to the effective use of a third party in any capacity is for management to appropriately assess, measure, monitor, and control the risks associated with a contractual relationship. While engaging another entity may assist management and the board in achieving strategic goals, such an arrangement reduces management's direct control and introduces risks. Accordingly, institutions should establish and maintain an effective risk management process for initiating and overseeing outsourced operations.

  As part of an institution's risk assessment, the institution should also identify performance criteria, internal controls, reporting needs, and contractual requirements that would be critical to the ongoing assessment and control of specific identified risks – in other words, a management oversight strategy that allows for "assessment of performance, as well as mid-course corrections." The guidance also noted that "[a]fter completing the general assessment of risks, particularly relative to the institution's overall strategic plan, management should review its ability to provide adequate oversight and management of the proposed third-party relationship on an ongoing basis. While identifying and understanding the risks associated with the third party is critical at the outset, the long-term management of the relationship is vital to success."

  In addition, the guidance noted that "[t]he extent of oversight of a particular third-party relationship will depend upon the potential risks and the scope and magnitude of the arrangement. An oversight program will generally include monitoring of the third party's quality of service, risk management practices, financial condition, and applicable controls and reports. Results of oversight activities for material third-party arrangements should be periodically reported to the … board of directors or designated committee. Identified weaknesses should be documented and promptly addressed."

- **Federal Agencies.** When procuring Critical Functions, agencies considered strategic human capital planning – analyzing agency staff resources, and internal capability and capacity.

  For example, as noted above, the following agencies noted heightened contracting monitoring, such as:
  - **Develop a Management Oversight Strategy.** NASA, USDA, and CFPB performed, or considered it a best practice to perform, strategic human capital planning. In addition, NASA considered internal capability when procuring a Critical Function, and CFPB ensured that Contract Officers had appropriate backgrounds, such as Information Technology expertise for procured Information Technology services.

6. Determine contract structure.	–	–	✓	✓

- **Industry Standard.** According to the FDIC's Financial Institution Letter titled *Third-Party Risk Guidance for Managing Third-Party Risk* (FIL-44-2008) (June 2008), the key to the effective use of a third party in any capacity is for management to appropriately assess, measure, monitor, and control the risks associated with the relationship. One of the risk management process's four main elements is contract structuring and review. In particular, the guidance states that "[a]fter selecting a third party, management should ensure that the specific expectations and obligations of both the financial institution and the third party are outlined in a written contract prior to entering into the arrangement. Board approval should be obtained prior to entering into any material third-party arrangements… The level of detail in contract provisions will vary with the scope and risks associated with the third-party relationship."

The guidance provides, in part, the following topics that should be considered as a contract is structured, with the applicability of each dependent upon the nature and significance of the third-party relationship: scope (rights/responsibilities of each party), cost/compensation, performance standards, reports (types and frequency of management information), audit (of contractor), confidentiality and security (prohibit contractor from using or disclosing agency's information), customer complaints, business resumption and contingency plans, default and termination (of contractor), dispute resolution, ownership and license, indemnification, and limits on liability.

- **Federal Agencies.** Agencies ensured that statements of work recognize the procurement of Critical Functions, and management considered (or, considered as a best practice) contract provisions that specify the agency's rights and the contractor's obligations and responsibilities, including, but not limited to, provisions that address contractor performance, financial condition, emergency preparedness, corrective measures to regain/maintain control, and transfer/transition to another entity.

  For example, as noted above, the following agencies noted heightened contracting monitoring, such as:
  - **Determine Contract Structure.** USDA, CFPB, and OCC used, or considered it a best practice to have, contract provisions to specify the agency's rights and the contractor's obligations and responsibilities surrounding Critical Functions.

7. Conduct periodic reviews of controls and processes.	✓	–	–	✓

- **OMB Guidance.** OMB Policy Letter 11-01 advises certain agencies that they should ensure that Federal employees perform and/or manage Critical Functions to the extent necessary for the agency to operate effectively and maintain control of its mission and operations. According to the FDIC's Legal Division, OMB Policy Letter 11-01 does not directly apply to the Agency but it may be used for guidance. In particular, the policy letter states that "[a]gencies shall develop and maintain internal procedures to address the requirements of this guidance. Those procedures shall be reviewed by agency management no less than every two years." In addition, agencies "should periodically evaluate the effectiveness of their internal management controls for reserving work for Federal employees and identify any material weaknesses…"

  The OMB policy letter also states that "[a]gencies should review, on an ongoing basis, the functions being performed by their contractors, paying particular attention to the way in which contractors are performing, and agency personnel are managing, contracts involving … critical functions… These reviews should be conducted in connection with the development and analysis of inventories of service contracts."

  In addition, the OMB policy letter states that "if the agency determines that internal control of its mission and operations is at risk due to over-reliance on contractors to perform critical functions, requiring activities should work with their human capital office to develop and execute a hiring and/or development plan. Requiring activities should also work with the acquisition office to address the handling of ongoing contracts and the budget and finance offices to secure the necessary funding to support the needed in-house capacity…"

- **Federal Agencies.** Agencies performed (or, considered as a best practice) periodic reviews of contractor and agency personnel performance, human capital planning, personnel training, risk management strategy, contract requirements, budget/cost justification, attribution of contractor vs. agency work, and over-reliance assessments.

  In addition, agencies developed an exit strategy from the contractual arrangement and/or described that they would take the following actions if it was determined that the agency was over reliant on contractors to perform Critical Functions: (1) review and adjust what the contractor accomplishes for the agency, (2) reassess human capital needs (staff and funding) and make Full Time Employee adjustments; (3) in-source the function; (4) review the contracting process from beginning to end to understand how the agency lost control (retrospective review of the contracting process); (5) reestablish controls over contractor responsibilities (by strengthening oversight, insourcing the work

through the timely development and execution of hiring plans, refraining from exercising options under the contract, or terminating all or part of the contract).

For example, as noted above, the following agencies noted heightened contracting monitoring, such as:

- **Perform Periodic Reviews**. GSA, NASA, USDA, DOE, and OCC have policy and procedures to prevent over-reliance on a contractor, and specific corrective measures to address instances of contractor over-reliance. Although NCUA and CFPB did not have an explicit written policy, they noted the actions/procedures they would take to address an instance of contractor over-reliance. In addition, GSA, NASA, USDA, DOE, OCC, NCUA, and CFPB have procedures to oversee the contractor's performance and their own personnel's oversight of a contractor.

8. Report to the Board procured Critical Functions.	–	–	✓	–

- **Industry Standard.** According to the FDIC's Financial Institution Letter titled *Third-Party Risk Guidance for Managing Third-Party Risk* (FIL-44-2008) (June 2008), the key to the effective use of a third party in any capacity is for management to appropriately assess, measure, monitor, and control the risks associated with a contractual relationship. In particular, the board should be involved in the following stages of an effective third-party risk management program – for procured critical functions:

  - **Risk assessment.** "It is key for management to develop a thorough understanding of what the proposed relationship will accomplish for the institution, and why the use of a third party is in its best interests. A risk/reward analysis should be performed for significant matters, comparing the proposed third-party relationship to other methods of performing the activity or product offering, including the use of other vendors or performing the function in-house. For such matters, the analysis should be considered integral to the bank's overall strategic planning, and should thus be performed by senior management and reviewed by the board or an appropriate committee."
  - **Contract structuring and review.** "Board approval should be obtained prior to entering into any material third-party arrangements. Appropriate legal counsel should also review significant contracts prior to finalization."
    Ongoing monitoring. "Results of oversight activities for material third-party arrangements should be periodically reported to the financial institution's board of directors or designated committee."

Source: OIG analysis of OMB guidance, GAO reports, Industry guidance, and interview statements from Federal agencies.
Legend: ✓ The source identified this item. | – The source did not mention this item.

Table 2 illustrates the services performed by Blue Canopy that we identified as Critical Functions based on National Institute of Standards and Technology Special Publication 800-53, Revision 5 (NIST S.P. 800-53).

NIST S.P. 800-53 provides "a comprehensive set of security and privacy safeguarding measures for all types of computing platforms…Safeguarding measures include both security and privacy controls to protect the critical and essential operations and assets of organizations and the privacy of individuals." The publication also states, "[t]he controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines."[40]

Table 2: Procured Blue Canopy Services Deemed to Be Critical Functions of the FDIC

Procured Function	National Institute of Standards and Technology Guidance	Identified as a Critical Function (Yes/No)
Contract CORHQ-14-C-0778		
Security Operations Center	• Incident Response (IR)-4 Incident Handling • IR-7 Incident Response Assistance • System and Information Integrity (SI)-4 System Monitoring	Yes
Computer Security Incident Response Team	• Incident Response (IR)-4 Incident Handling • IR-5 Incident Monitoring • IR-6 Incident Reporting • Risk Assessment (RA)-1 Policy and Procedures • RA-3 Risk Assessment • RA-5 Vulnerability Monitoring and Scanning • Assessment, Authorization, and Monitoring (CA)-5 Plan of Action and Milestones • Program Management (PM)-4 Plan of Action and Milestones Process • PM-6 Information Security Measures of Performance • PM-9 Risk Management Strategy	Yes
Contract CORHQ-14-C-0769		
Technical Security Assessment	• RA-5 Vulnerability Monitoring and Scanning	Yes
Vulnerability Management	• RA-5 Vulnerability Monitoring and Scanning	Yes
Continuous Controls Assessment Program	• CA-2 Control Assessments • Configuration Management (CM)-4 Impact Analyses	Yes
Privacy Program	• Program Management (PM)-18 Privacy Program Plan	Yes
Testing of Internal Controls	• CA-2 Control Assessments	Yes

[40] *NIST Special Publication 800-53, Revision 5*, *Security and Privacy Controls for Information Systems and Organizations,* (September 2020).

Source: OIG analysis of FDIC's procured services from Blue Canopy against NIST guidance.
*NIST S.P. 800-53 organized security and privacy controls into 20 families. "Each family contains controls that are related to the specific topic of the family. An [alphabetical] two-character identifier uniquely identifies each control family"[41] (e.g., IR for Incident Response). The controls and control enhancements within each family are in numerical order (e.g., IR-4 Incident Handling).

[41] *NIST Special Publication 800-53, Revision 5*, (September 2020).

ASB	Acquisition Services Branch
BOA	Basic Ordering Agreement
CFPB	Consumer Financial Protection Bureau
CFR	Code of Federal Regulations
CIOO	Chief Information Officer Organization
C-SIRT	Computer Security Incident Response Team
DHS	Department of Homeland Security
DOA	Division of Administration
DOD	Department of Defense
DOE	U.S. Department of Energy
DRR	Division of Resolutions and Receiverships
ERM	Enterprise Risk Management
FAIR Act	Federal Activities Inventory Reform Act
FAR	Federal Acquisition Regulation
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Modernization Act
FPDS-NG	Federal Procurement Data System-Next Generation
FRB	Federal Reserve Board
GAO	U.S. Government Accountability Office
GSA	General Services Administration
IGCE	Independent Government Cost Estimate
IT	Information Technology
NASA	National Aeronautics and Space Administration
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OCISO	Office of the Chief Information Security Officer
OMB	Office of Management and Budget
SOC	Security Operations Center
U.S.C.	United States Code
USDA	U.S. Department of Agriculture

Federal Deposit Insurance Corporation

MEMO

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

FROM: Brandon L. Milhorn BRANDON MILHORN Digitally signed by BRANDON MILHORN Date: 2021.03.26 11:41:26 -04'00'
Deputy to the Chairman, Chief of Staff and Chief Operating Officer

CC: Sylvia W. Burns, CIO
E. Marshall Gentry, CRO

DATE: March 26, 2021

RE: Management Response to OIG Draft Audit Report, Critical Functions in FDIC Contracts (No. 2020-005)

The FDIC provides the following response to the Office of Inspector General's (OIG) draft evaluation report titled, *Critical Functions in FDIC Contracts*, dated March 3, 2021. The OIG evaluated two FDIC procurements with Blue Canopy Group, LLC (Blue Canopy) against provisions of OMB Policy Letter 11-01, *Performance of Inherently Governmental and Critical Functions*, September 12, 2011. The OIG found that the FDIC implemented its established procurement process with respect to the two procurements, including reporting to the FDIC Board of Directors. However, the OIG concluded that the FDIC did not have policies and procedures for identifying "critical functions" in its contracts and did not implement heightened monitoring activities for the Blue Canopy contracts consistent with the requirements of OMB Policy Letter 11-01.

The OIG made 13 recommendations aimed at having the FDIC incorporate provisions of OMB Policy Letter 11-01 into the FDIC's policies and procedures, identify "critical functions" during the procurement process, and implement heightened contract monitoring for "critical functions."

While OMB Policy Letter 11-01 is inapplicable to the FDIC as a matter of law, the FDIC's risk-based[1] acquisition procedures address virtually all of the control factors listed in the Policy Letter and many of these controls were in place for the Blue Canopy contracts. The FDIC's acquisition procedures and practices are also consistent with the FDIC Financial Institution Letter (FIL), *Guidance for Managing Third-Party Risk* (FIL-44-2008), which the OIG also used as criteria for the evaluation. The FDIC is committed to continually improving its processes and controls and will: (1) survey recognized practices and procedures associated with contracts supporting essential functions or those involving services necessary in a business continuity event, particularly when those contracts are performed by a single vendor; and (2) incorporate enhancements to our existing acquisition planning, approval, reporting, and oversight processes, as warranted by our unique operational needs and management structure. As such, we have concurred or partially concurred with all of the OIG recommendations.

[1] The FDIC's acquisition procedures are scalable based on the risk and complexity of the procurement and require increased planning, oversight, and monitoring commensurate with a procurement's risk and importance. The FDIC's procedures do not separately designate certain contracts as related to "critical functions."

FDIC Consideration of the OMB Policy Letter and Certain OIG-Identified Practices

The FDIC takes seriously its responsibility to maintain control of its operations and to ensure that it has sufficient and knowledgeable federal staff to oversee contractors, particularly those performing services essential to the FDIC's mission. The FDIC has established risk-based processes and procedures to identify, monitor the performance of, and oversee all contracts, and is committed to improving performance in these areas.

As the OIG acknowledged in its draft report, OMB Policy Letter 11-01 does not apply to the FDIC. The FDIC Legal Division concluded in October 2011 that the OMB Policy Letter did not apply because: (1) the FDIC did not fall within the definition of "executive agency" in the Office of Federal Procurement Policy Act and (2) the FDIC was not funded by congressional appropriations. As an independent agency, the FDIC routinely looks to the practices of agencies governed by the Federal Acquisition Regulation (FAR), other (non-FAR-based) independent agencies, and private business to inform its acquisition policies. Consistent with that approach, the FDIC will continue to adopt those portions of the OMB Policy Letter that support its unique operations, while the Policy Letter overall continues to be inapplicable by operation of law.

There is no uniform set of "best practices"[2] that public and private organizations have agreed upon in the subject area of the OIG's report. As the report demonstrates, no public or private organization follows all of the processes or practices the OIG identified. As noted above, when formulating its policies, the FDIC considers what has worked exceptionally well and improved performance and efficiency at FAR-based agencies, other independent agencies, and private organizations. The FDIC incorporates those processes or practices that support its unique circumstances, recognizing that what has worked well elsewhere or what other organizations have implemented may not work well for the FDIC or might be counterproductive to performance and efficiency – the goal of best business practices. With this approach in mind, the FDIC will consider the processes, practices, and systems that the OIG identified – among others – to enhance our existing policies.

Existing Acquisition Procedures for Contract Planning, Oversight, and Reporting

Many of the procurement controls contemplated in the OMB Policy Letter exist within the FDIC's current acquisition policies and guidance, without the specific designation of "critical functions." Under the FDIC's Acquisition Policy Manual (APM), certain functions are so essential to the performance of government responsibilities that they may not be outsourced, namely the performance of inherently governmental functions.[3] When contracted services fall short of inherently governmental functions but are closely aligned with them, the FDIC is responsible for building in enhanced controls and management oversight in the design and administration of relevant support contracts.[4] In applying acquisition policies and guidance, the FDIC takes a risk-based approach that may apportion greater responsibility to contractors when requirements are well understood, less sensitive, or less likely to change over time. This risk-based approach to activities that are closely aligned with inherently governmental functions is consistent with the intent of OMB Policy Letter 11-01.

The FDIC's acquisition procedures are also consistent with the FDIC's *Guidance for Managing Third-Party Risk* (FIL-44-2008). This guidance document recommends that FDIC-supervised institutions take a risk-based approach to ensuring that appropriate controls, acquisition planning, and oversight are in place to manage services provided by third parties. The FIL does not separately detail specific procedures applicable to "critical functions,"[5] but rather provides a general framework to provide appropriate oversight and risk management of

[2] GAO reported that "[b]est business practices refer to the processes, practices, and systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas."
[3] *See* APM § 1.405(a).
[4] *See* id. § 1.405(b).
[5] The term "critical functions" only appears once in the Introduction section of the guidance.

MEMO 2

significant third-party relationships, including those in which a third party performs "critical functions." The FIL recommends increasing levels of control for more complex or higher-risk activities. The FIL clearly explains that the guidance "should not be considered as a set of required procedures." The FDIC disagrees with any suggestion that the agency's existing comprehensive, risk-based procurement framework does not meet the third-party risk management principles outlined in the FIL. As discussed in detail below, FDIC acquisition policy requires robust acquisition planning that includes consideration of costs, risks, alternatives, contract type, oversight structure, business continuity, security, performance reporting, Board reporting, and, in some instances, Board approval of contracting actions.

Inherently Governmental and Critical Functions. The APM includes a discussion and guidance for avoiding performance by contractors of inherently governmental functions. As recommended in OMB Policy Letter 11-01, the APM details pre- and post-award responsibilities to avoid contracts for inherently governmental functions.[6] The APM emphasizes the importance of being fully aware of contract terms, contractor performance, and contract administration to ensure that appropriate FDIC control is preserved. The APM and implementing Acquisition Procedures, Guidance, and Information (PGI) address planning considerations for contracts considered essential in the event of an emergency or business continuity event and delineates risks associated with such procurements. These planning discussions should consider the resources and the expertise required to perform the functions and manage the procurement.

Market Research and Competition. The APM requires FDIC program offices and the contracting officer to work together to conduct market research to support all acquisition planning. The APM also requires program offices to use competition in acquisitions to the maximum extent possible. Through competition, the FDIC is able to compare the value of competing technical proposals and prices in order to determine which proposal affords the best value. Reasonable competition also means soliciting a sufficient number of sources to obtain an adequate market response and to analyze the fairness and reasonableness of individual offers.

Contract Planning. The APM and PGI require acquisition planning for contracts exceeding $1 million and require consideration and discussion of:

- feasible acquisition alternatives, the impact of prior acquisitions, and any related in-house effort;
- risks associated with the procurement, including technical, cost, and schedule risks and efforts planned or underway to reduce risk and consequences;
- how the oversight manager and technical monitor will oversee the project after contract award, including any reporting requirements;
- the level of business continuity planning necessary for the acquisition, including whether the contractor's services will be necessary in time of emergency and the level of service that will be required, any maintenance and testing requirement specific to business continuity, and any requirement that the contractor participate with FDIC in joint disaster planning exercises; and
- how the contract is to be administered, including how inspection and acceptance corresponding to the statement of work or statement of objectives performance criteria is to be enforced.

In addition, if the FDIC determines contract services are essential in the event of an emergency or business continuity event, the statement of work or statement of objectives must include:

[6] The APM includes a descriptive list of "inherently governmental functions" and services and actions that are not "inherently governmental functions." This list of "inherently governmental functions" is derived from the FAR (48 C.F.R. § 7.503), and the examples in Appendix A in OMB 11-01.

- business continuity requirements;
- requirements that contractors flow emergency preparedness and continuity requirements to essential subcontracts; and
- requirements for contractors to have emergency plans for providing services to FDIC in the event of a disruption of normal operations, and participation in FDIC business continuity testing, training, and exercises.

As it relates to contract structure, the APM states that the contracting officer must select the type of contract and pricing arrangement that represents the most prudent and reasonable relationship with the contractor and minimizes cost and other risks to the FDIC. The contracting officer may use any combination of contract type and pricing arrangement suitable to the procurement. The objective is to select a contract type and pricing arrangement that results in reasonable contractor risk and provides the contractor with the greatest incentive for efficient and economical performance.

Finally, when evaluating quotations from firms, cost is not the only factor that the FDIC considers. The FDIC, instead, uses a best value method – especially for acquisitions requiring innovative solutions or a high level of technical expertise – that allows for the evaluation of technical factors in addition to price and past performance.

Contract Oversight. The FDIC develops a management oversight strategy for contracts and assigns responsibility to FDIC contracting officers, oversight managers, and technical monitors to oversee contractors based on the risk and complexity of the contract. The PGI requires the oversight manager, together with the contracting officer, to determine the level of oversight that is necessary to ensure the contractor makes satisfactory progress toward the successful completion of the terms of the contract. To assist in performing oversight activities for complex contracts for services, the oversight manager must work with the contracting officer to develop a contract management plan. The oversight manager ensures that the contractor delivers the required goods or performs the work according to the contract and the delivery schedule, monitors the expenditure of funds, and approves invoices.

Contracting officers and oversight managers are also responsible for evaluating contractor performance. Contractor performance evaluations must be completed annually for each award, regardless of dollar value, and at the end of the contract.

Contract Reporting. The FDIC develops detailed board cases for individual procurements exceeding $20 million that discuss procurement costs, benefits, alternatives considered, management oversight strategy, and other information. The Board of Directors must approve all contract actions over $20 million. Each quarter, the FDIC provides a contract-specific report to the Board of Directors for complex contracts over $5 million and for all contracts over $20 million.

Acquisition Initiatives to Improve Competition, Oversight, and Performance

The FDIC has also recently implemented new acquisition initiatives to further improve vendor management, contract oversight, and to reduce the number of non-competitive awards. These initiatives focus on awarding competitive, multiple-award basic ordering agreements (BOAs) and smaller, more competitive task orders. Such an approach reduces the chances of the FDIC being overly reliant on an individual vendor. FDIC is also placing a greater focus on upfront acquisition planning to make sure contracts are properly structured and have meaningful service level agreements (SLAs), appropriate incentive/disincentive structures, and performance metrics.

The Chief Information Officer Organization (CIOO) recently issued an Acquisition Planning Guide that outlines the contracting process from start to finish for customers in need of IT goods and services, and provides clear and consistent expectations for stakeholders. The Guide provides tools for implementing the IT acquisition life cycle,

with objectives to:

- develop scalable solutions that promote competition;
- deliver fast, reliable, responsive, and innovative services;
- drive acquisition agility; and
- optimize vendor engagement.

The FDIC has also established a 2021 corporate performance goal and interdivisional work team to strengthen our contract oversight management program by increasing the independence and professionalism of our oversight managers and technical monitors.

FDIC's Execution and Oversight of the Blue Canopy Contracts

The OIG notes in its report that the FDIC followed its normal contract policies and procedures for the two Blue Canopy contracts. While not discussed in detail in the report, we note that the policies and procedures the FDIC followed with respect to the Blue Canopy contracts provided a sound basis for vendor oversight and performance management. The FDIC provided detailed information on the acquisition to the Board of Directors in advance of the procurement and quarterly throughout the period of performance. These actions, based on existing FDIC acquisition policies and procedures, were consistent with the spirit of OMB Policy Letter 11-01 and the FDIC's *Guidance for Managing Third-Party Risk*.

- Due to the dollar value of these procurements, the FDIC submitted and briefed a Board Case to the FDIC Board of Directors to receive authority to award the contracts.
- The FDIC acknowledged the importance of the procured function in the Board Case, contract statement of work, and acquisition plans—the latter stating that services were "critical to ensuring the security and protection of FDIC's IT infrastructure and data."
- In planning this procurement, the CIO assessed whether FDIC staff or contractors should perform the work. The recommendation was to contract for the services due to the available experience of the private sector and its ability to scale resources more quickly than the FDIC.
- The FDIC awarded both procurements competitively utilizing a best value approach.
- The contracts contained SLAs that required the contractor to meet FDIC-defined standards.
- The contracts included a number of key performance indicators (KPIs) and operational performance indicators (OPIs), including KPIs related to providing, backfilling, and retaining human resources and key personnel; incident response; root cause analysis; and report delivery.
- An FDIC team, including oversight managers, technical monitors, and contract specialists, provided oversight of both contracts. The FDIC also completed annual performance reports on Blue Canopy.
- The FDIC reported procurement information to the FDIC Board of Directors quarterly.

The contractor successfully performed all required tasks under both contracts, and received "excellent" and "outstanding" ratings in annual performance reviews, with the exception of one "good" rating on one contract for one rating period.

FDIC Actions Taken to Address Prior OIG Concerns Regarding Blue Canopy Contracts

The FDIC took action to address OIG concerns about Blue Canopy's independence. A prior OIG report, *Security Configuration Management of the Windows Server Operating System*, (AUD-19-004) (January 2019), found that the FDIC tasked Blue Canopy with both designing security controls and assessing their effectiveness, which impaired the firm's ability to conduct an impartial assessment. The OIG also concluded the FDIC needed a formal process for reviewing security control assessment reports to ensure that Blue Canopy performed sufficient security control testing. The FDIC took prompt action to address the OIG's recommendations regarding the lack of independent assessments of Blue Canopy's services, and the OIG closed those recommendations in 2019.

Separate from the prior OIG review, the FDIC also made a management determination to reduce our reliance on a single contractor for information security and privacy services. To increase competition and diversity of firms providing information security and privacy services, reduce the FDIC's reliance on a single vendor for these services, and improve contract oversight and vendor management, the FDIC sought and received Board approval in October 2019 to initiate two contract actions to replace the existing Blue Canopy contracts with new BOAs and task orders. The solicitations for the new contracts occurred in November 2019 and April 2020. In July 2020, the FDIC awarded a competitive BOA to one vendor to provide managed support services for all aspects of the Security Operations Center (SOC) under a fixed-price arrangement. In October 2020, the FDIC awarded BOAs to 10 vendors for Security and Privacy Professional Services (SPPS). FDIC recently competitively awarded seven task orders under the SPPS BOAs resulting in awards to five different vendors. These task orders will transfer work from the Blue Canopy contract in the first and second quarters of 2021. This contracting approach will increase competition and reduce FDIC's reliance on one contractor in these areas. The contracts include performance criteria, reporting, and contractual requirements to facilitate ongoing assessment and mitigation of risk.

Both the Managed Security Services Provider (MSSP) and SPPS BOAs include incentives for vendors to provide superior performance. The MSSP BOA includes provisions which carry monetary penalties should the vendor default against an SLA and incentives to extend the period of performance by demonstrating sustained excellent performance in meeting all SLAs. The SPPS BOA also includes SLAs, which carry monetary penalties when the vendor defaults and include an incentive for the vendor to earn a contract extension by successfully proposing a conversion of their time-and-material work to firm-fixed-priced. In the first 18 months of contract performance, if the initial vendor is not successfully performing, both the MSSP and SPPS BOAs permit a quick transition to another vendor on the contract without a recompetition. Combined with the SLAs, performance metrics, incentives, and penalties, the FDIC has also assigned an experienced oversight manager and a team of technical monitors that have the capacity and capability to oversee these vendors properly and mitigate any risk to FDIC operations associated with inadequate vendor performance.

Given the existing contractual controls in the Blue Canopy contracts (such as SLAs and other performance metrics), remedial actions taken to address the independence concern identified by the OIG, and the subsequent revision of the acquisition strategy associated with the services previously procured under the Blue Canopy contracts, the FDIC disagrees with the OIG's determination that the contract "represent[ed] a failure on the FDIC's part to maintain control of its operations." Blue Canopy's performance under the contracts, which included detailed performance metrics, was regularly reviewed and received high marks from the FDIC. The FDIC took prompt action to address security control testing sufficiency before OIG issued the January 2019 audit report. Moreover, the FDIC determined, in advance of the 2019 contract modifications to increase the contract ceiling on both Blue Canopy contracts, that a new competitive, multi-vendor acquisition strategy should be put in place for the services. The new acquisition strategy was presented to and approved by the Board in October 2019. This ongoing oversight of the Blue Canopy contracts and the reconsideration of the underlying acquisition strategy for the services are key components of the procedures highlighted as "best practices" by the OIG in its audit and demonstrate the control asserted and maintained by the FDIC over these services.

MEMO 6

Management Response to Recommendations

Ongoing efforts to improve the FDIC's acquisition services and oversight management programs will incorporate additional structure and discipline around certain contracts that support essential functions or involve services needed in a business continuity event, consistent with the recommendations in the OIG report. While the FDIC does not plan to explicitly adopt the "critical functions" framework from OMB Policy Letter 11-01 or each of the compiled practices set out by the OIG in its report, the FDIC will conduct a survey to identify cost-effective, risk-based controls appropriate for the FDIC's unique mission and statutory responsibilities related to essential functions or for services necessary in a business continuity event, particularly when the services may be provided by a single vendor.

Recommendation 1: Incorporate the provisions of OMB Policy Letter 11-01 guidance into the FDIC Acquisition Policy Manual (August 2008) and Acquisition Procedures, Guidance and Information document (January 2020).

Management Decision: Partially Concur

Corrective Action: The FDIC's existing acquisition policy, as a comprehensive framework, incorporates many of the risk management principles referenced by the OIG in its audit and incorporated in OMB Policy Letter 11-01. The FDIC will consider each of the OIG's recommendations and further study the need for additional risk-based controls for essential procurements. While OMB Policy Letter 11-01 does not apply to FDIC procurements as a matter of law, the FDIC envisions developing (as an added component of our existing risk-based system) criteria for identifying a subset of contracts supporting essential FDIC functions or those that provide services in a business continuity event that will further enhance FDIC contract management consistent with the spirit the Policy Letter. Those designated contracts would then be subject to a risk assessment process to ensure the FDIC maintains control over the function for which services are being procured, has an appropriate contract oversight structure, and includes contract provisions commensurate with risks. DOA will revise the APM and PGI to reflect any resulting process and control enhancements.

Division and office directors are responsible for determining their human resource needs, using contractors appropriately, and maintaining control of their respective mission and operational responsibilities. In addition to existing requirements for oversight management, the FDIC remains committed to the use of SLAs and other controls to manage vendor performance and is considering additional controls to ensure the independence, training, and professionalism of oversight managers. FDIC will consider and further study potential methodologies for assessing contractor overreliance, including how other agencies make such determinations. Based on our study, we will provide guidance to divisions and offices for assessing the potential for contractor overreliance and maintaining federal control of essential functions or those necessary during a business continuity event.

Estimated Completion Date: March 31, 2022

Recommendation 2: Identify Critical Functions during the procurement planning, award, and contract management phases of the acquisition process.

Management Decision: Partially Concur

Corrective Action: In addition to current practices, the FDIC plans to further address this recommendation through the study and actions described in our response to Recommendation 1.

Estimated Completion Date: March 31, 2022

Recommendation 3: Assess whether the FDIC's Enterprise Risk Management program should identify the impact of procured Critical Functions, and procurement risk related to contractors performing Critical Functions, within the FDIC's Risk Inventory.

MEMO 7

Management Decision: Concur

Corrective Action: The FDIC Risk Inventory identifies risks to the FDIC achieving its mission, goals, and objectives and risks to agency operations. Specific relevant items within the risk inventory currently include risks related to cybersecurity, privacy, protection of sensitive information, potential cyberattacks, management and oversight of contracts, adequacy of staffing, and succession planning—which involves having a sufficient number of the right people with the right skills to meet mission responsibilities. The Risk Inventory does not identify "procured critical functions" as a separate and distinct risk. Nevertheless, the comprehensive nature of the risk management framework includes many FDIC functions that might be classified as "critical." In response to this recommendation, the FDIC will review its risk inventory and conduct an assessment to determine if the current risk inventory sufficiently addresses the underlying risks presented in the OIG's report, irrespective of the specific use of the term "critical function."

Estimated Completion Date: May 31, 2021

Recommendation 4: Conduct a procurement risk assessment for Critical Functions during the procurement planning process, for each contract involving Critical Functions. As part of the procurement risk assessment, include a cost effectiveness analysis.

Management Decision: Partially Concur

Corrective Action: Existing acquisition planning procedures require consideration and discussion of risks associated with all procurements. In addition to current practices, the FDIC plans to further address this recommendation through the study and actions described in our response to Recommendation 1.

Estimated Completion Date: March 31, 2022

Recommendation 5: Develop and implement a management oversight strategy for Critical Functions during the procurement planning process, for each contract involving Critical Functions.

Management Decision: Partially Concur

Corrective Actions: The FDIC currently develops a management oversight strategy to oversee all contractors based on the risk and complexity of the contract. In addition to current practices, the FDIC plans to further address this recommendation through the study and actions described in our response to Recommendation 1.

Estimated Completion Date: March 31, 2022

Recommendation 6: Determine the contract structure during the solicitation and award process for the procurement of a Critical Function.

Management Response: Partially Concur

Corrective Action: The FDIC currently considers the appropriate contract structure based on the goods or services being procured and any associated risks for all contracts during acquisition planning. In addition to current practices, the FDIC plans to further address this recommendation through the study and actions described in our response to Recommendation 1.

Estimated Completion Date: March 31, 2022

Recommendation 7: Revise the management oversight strategy for the procured Critical Functions performed under the BOAs for Managed Security Services Provider and Security and Privacy Professional Services to ensure that the strategy aligns with best practices.

MEMO 8

Management Response: Partially Concur

Corrective Action: The existing management oversight strategy for the subject BOAs and task orders includes performance criteria, internal controls, reporting, and contractual requirements that were established during acquisition planning and are detailed in statement of work documents. Following the FDIC's study discussed in response to recommendation 1, the CIOO will assess whether any additional enhancements to the management oversight strategy for the MSSP and SPPS BOAs and task orders are needed beyond those already incorporated.

Estimated Completion Date: June 30, 2022

Recommendation 8: Identify missing or insufficient controls in the BOAs and task orders for Managed Security Services Provider and Security and Privacy Professional Services, and implement appropriate corrective actions or compensating controls.

Management Response: Partially Concur

Corrective Actions: The CIOO and the Acquisition Services Branch considered both internal controls and contractual requirements during acquisition planning for the subject BOAs and task orders and included them in the statement of work documents. Following the study discussed in response to Recommendation 1, the CIOO will assess whether any additional enhancements are needed for the MSSP and SPPS BOAs and task orders beyond those already incorporated.

Estimated Completion Date: June 30, 2022

Recommendation 9: Implement periodic reviews for procured Critical Functions, including for the BOAs and task orders for Managed Security Services Provider and Security and Privacy Professional Services.

Management Response: Partially Concur

Corrective Action: In addition to current practices, the FDIC plans to address this recommendation through the study and actions described in our response to Recommendation 1, and based on such actions, will assess the need for additional periodic reviews.

With respect to the MSSP and SPPS contracts, FDIC contract officers, oversight managers, and technical monitors assigned to the BOAs and task orders will ensure that contractors comply with contract terms and meet performance expectations. The FDIC will also complete an annual performance review of MSSP and SPPS contractors. Following the FDIC's study and actions in response to Recommendation 1, the CIOO will assess the need for additional periodic reviews of such contracts and whether additional enhancements are required beyond the controls already incorporated.

Estimated Completion Date: June 30, 2022

Recommendation 10: Determine when and how to assess for contractor over-reliance as part of the management oversight strategy.

Management Response: Partially Concur.

Corrective Action: In addition to current practices, the FDIC plans to address this recommendation through the study and actions described in our response to Recommendation 1.

Estimated Completion Date: March 31, 2022

Recommendation 11: Implement corrective actions when the FDIC determines it is over-reliant on a contractor

for a procured Critical Function.

Management Response: Partially Concur

Corrective Actions: Existing acquisition processes and procedures help limit the likelihood of such an occurrence; however, the FDIC will examine whether additional controls are necessary in conjunction with the study and actions described in our response to Recommendation 1.

Estimated Completion Date: March 31, 2022

Recommendation 12: Report to the Board about the Procurement Risk Assessments, Management Oversight Strategies and contract provisions that address identified risks for planned Critical Functions during the procurement planning phase of the acquisition, for its consideration.

Management Response: Partially Concur

Corrective Action: The FDIC includes significant information regarding acquisition strategy, contract oversight and performance measures, and other controls in current board cases for contracts or BOAs over $20 million. Additional information on contract and contractor performance is provided in quarterly reports to the FDIC Board. The FDIC will consider additional reporting requirements related to contracts for essential functions or for services necessary during a business continuity event, including where such functions are performed by a single vendor, in conjunction with the study and actions described in response to Recommendation 1.

Estimated Completion Date: March 31, 2022

Recommendation 13: Report to the Board about the Award Profile Reports and corresponding status reports for procured Critical Functions during the contract management phase of the acquisition process on an individual and aggregate contract basis, for its consideration.

Management Response: Partially Concur.

Corrective Action: See response to Recommendation 12.

Estimated Completion Date: March 31, 2022

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

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The FDIC will consider each of the OIG's recommendations and further study the need for additional risk based controls for essential procurements. DOA will revise the APM and PGI to reflect any resulting process and control enhancements. In addition, the FDIC will consider and further study potential methodologies for assessing contractor overreliance, including how other agencies make such determinations. Based on its study, the FDIC will provide guidance to divisions and offices for assessing the potential for contractor overreliance and maintaining federal control of essential functions or those necessary during a business continuity event.	March 31, 2022	$0	No	Open
2	The FDIC plans to further address this recommendation through the study and actions described in its response to Recommendation 1.	March 31, 2022	$0	No	Open
3	The FDIC will review its risk inventory and conduct an assessment to determine if the current risk inventory sufficiently addresses the underlying risks presented in the OIG's report, irrespective of the specific use of the term "Critical Function."	May 31, 2021	$0	Yes	Open
4	The FDIC plans to further address this recommendation through the study and actions described in its response to Recommendation 1.	March 31, 2022	$0	No	Open
5	The FDIC plans to further address this recommendation through the study and actions described in its response to Recommendation 1.	March 31, 2022	$0	No	Open
6	The FDIC plans to further address this recommendation through the study and actions described in its response to Recommendation 1.	March 31, 2022	$0	No	Open

7	Following the FDIC's study discussed in response to Recommendation 1, the CIOO will assess whether any additional enhancements to the management oversight strategy for the Managed Security Services Provider and Security and Privacy Professional Services BOAs and task orders are needed beyond those already incorporated.	June 30, 2022	$0	No	Open
8	Following the FDIC's study discussed in response to Recommendation 1, the CIOO will assess whether any additional enhancements to the management oversight strategy for the Managed Security Services Provider and Security and Privacy Professional Services BOAs and task orders are needed beyond those already incorporated.	June 30, 2022	$0	No	Open
9	The FDIC will complete an annual performance review of the Managed Security Services Provider and Security and Privacy Professional Services contractors. In addition, following the FDIC's study and actions in response to Recommendation 1, the CIOO will assess the need for additional periodic reviews of such contracts and whether additional enhancements are required beyond the controls already incorporated.	June 30, 2022	$0	No	Open
10	The FDIC plans to address this recommendation through the study and actions described in its response to Recommendation 1.	March 31, 2022	$0	No	Open
11	The FDIC will examine whether additional controls are necessary in conjunction with the study and actions described in its response to Recommendation 1.	March 31, 2022	$0	No	Open
12	The FDIC will consider additional reporting requirements related to contracts for "essential functions" or for services necessary during a business continuity event, including where such functions are performed by a single vendor, in conjunction with the study and actions described in response to Recommendation 1.	March 31, 2022	$0	No	Open

13	The FDIC will consider additional reporting requirements related to contracts for "essential functions" or for services necessary during a business continuity event, including where such functions are performed by a single vendor, in conjunction with the study and actions described in response to Recommendation 1.	March 31, 2022	$0	No	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; or
2. Management does not concur with the recommendation, but alternative action meets the intent of the recommendation; or
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.