Evaluation Report

SBA's Cloud Migration and Oversight

APRIL 9, 2019

REPORT NUMBER 19-10

Executive Summary

SBA's Cloud Migration and Oversight

Report
No. 19-10

April 9, 2019

What OIG Reviewed

This evaluation report summarizes the results of our review of the Small Business Administration's (SBA's) cloud migration and oversight.

In fiscal year (FY) 2017, SBA undertook a headquarters data center consolidation project, which resulted in the decommissioning of nearly 200 servers and network equipment and reduced power consumption for the headquarters data center. SBA's Office of the Chief Information Officer (OCIO) made the decision that no new hardware, including servers or storage arrays, would be purchased or installed in the data center as part of the Agency's move to the cloud.

This initiative was codified as a strategic goal in SBA's FY 2018–2022 Strategic Plan. Furthermore, SBA's FY 2019 Congressional Budget Justification and FY 2017 Annual Performance Report set a performance goal to increase IT cost savings/avoidance through the streamlining of contracting, category management, and cloud computing to $10.8 million in FY 2019.

Our evaluation's objective was to determine whether SBA's cloud migration efforts followed applicable federal guidance and standards. Our scope included SBA's cloud systems inventory, as well as SBA's cloud migration efforts and oversight from FY 2017 through FY 2018.

What OIG Found

SBA needs to improve its cloud migration and oversight controls in risk management, security, data mobility, and IT investments to meet federal guidance and standards. During the time of our review, SBA was taking steps to improve the accuracy of the system it uses to monitor its cloud system inventory. These efforts will help ensure the appropriate controls are in place to protect its systems and data.

Effective deployment of identity and access management, contingency planning, risk management, and configuration management controls are critical to SBA having an effective information security program that achieves its mission/business needs. In addition, SBA needs to adopt standards to ensure it can efficiently move data among cloud platforms. These mobility controls accelerate the development and use of cloud computing standards and allow data migration to occur with minimal disruption.

OIG Recommendations

We provided eight recommendations to improve SBA's cloud migration and oversight efforts. The recommendations address needed improvements in the following areas: cloud inventory and monitoring controls, data ownership portability and interoperability, and improved documentation of cloud cost savings and service level requirements.

Agency Response

SBA management fully agreed with four recommendations and partially agreed with four recommendations. We found that the planned corrective actions resolved each of the eight recommendations. These responses are summarized in the Analysis of Agency Response section.

U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL
WASHINGTON, D.C. 20416

Final Report Transmittal
Report Number 19-10

DATE: April 9, 2019

TO: Linda E. McMahon
Administrator

FROM: Hannibal “Mike” Ware
Inspector General

SUBJECT: SBA’s Cloud Migration and Oversight

This evaluation report summarizes the results of our review of the Small Business Administration’s (SBA’s) cloud migration and oversight. Our evaluation’s objective was to determine whether SBA’s cloud migration efforts followed applicable federal guidance and standards.

We identified that SBA needs to improve its cloud migration and oversight controls in risk management, security, data mobility, and IT investments. SBA’s planned corrective actions resolved all eight recommendations. The Office of Inspector General will keep the eight recommendations open until we receive documentation demonstrating that final actions were implemented.

We appreciate the courtesies and cooperation extended to us during this evaluation. If you have any questions, please contact me at (202) 205-6586 or Andrea Deadwyler, Assistant Inspector General for Audits, at (202) 205-6616.

cc: Pradeep Belur, Chief of Staff and Chief Operating Officer
Patricia Gibson, Senior Advisor
Maria A. Roat, Chief Information Officer
Timothy E. Gribben, Chief Financial Officer and Associate Administrator for Performance Management
Chris Pilkerton, General Counsel
Martin Conrey, Attorney Advisor, Legislation and Appropriation
LaNae Twite, Director, Office of Internal Controls

Table of Contents

Introduction

The Office of Management and Budget (OMB) requires agencies, when evaluating options for new information technology (IT) deployments, to default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. Cloud computing allows users to access and use shared data and computing services. The cloud also provides users access to resources without agencies having to build additions to their infrastructure. The National Institute of Standards and Technology (NIST) provides an overview of cloud service management in Appendix II.

NIST provides guidance on cloud migration and states that to maximize effectiveness and minimize costs, security and privacy must be considered throughout the system lifecycle, from the initial planning stage forward. NIST guidance also states that with any outsourcing of IT services, security and privacy must be considered. Furthermore, all cloud systems must comply with the Federal Information Security Modernization Act of 2014 (FISMA). The Federal Risk and Authorization Management Program was designed to assist agencies in meeting FISMA requirements for cloud systems. Moreover, OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, states if the process provided by the third-party service organization is significant to an agency's internal control objectives, then the agency is responsible for establishing supplemental controls. Management still retains overall responsibility and accountability for all controls related to the processes.

Another critical issue centers on the risks associated with moving data from within the confines of the agency to cloud service provider(s). Depending on the nature of the migrated system, the organization needs to clearly identify which resources, responsibilities, and controls previously under the organization's control are transferred to cloud service provider(s). Prior to migrating data and systems to a cloud environment, federal agencies must follow applicable laws and regulations to mitigate risks associated with cloud migration and oversight. Attempting to address security and privacy issues after implementation and deployment exposes the organization to unnecessary risk to data, such as breach of confidentiality, loss of integrity, and inaccessibility. In addition, remediation efforts may be difficult and expensive.

Background

In fiscal year (FY) 2017, SBA undertook a headquarters data center consolidation project, which resulted in the decommissioning of servers and network equipment and reduced power consumption for the headquarters data center. SBA's Office of the Chief Information Officer (OCIO) made the decision that no new hardware, including servers or storage arrays, would be purchased or installed in the data center as part of the Agency's move to the cloud. As a result, certain resources, responsibilities, and controls were transferred to the cloud service providers through data center consolidation and cloud migration projects.

This initiative was codified as a strategic goal in SBA's FY 2018–2022 Strategic Plan. Furthermore, SBA's FY 2019 Congressional Budget Justification and FY 2017 Annual Performance Report set a performance goal to increase IT cost savings/avoidance through the streamlining of contracting, category management, and cloud computing to $10.8 million in FY 2019.

Prior Work

In FY 2016, OIG issued a report that identified weaknesses during SBA's Office 365 cloud migration.[1] In addition, our FY 2016 and 2017 FISMA reviews of SBA systems identified migration and trusted internet connection issues with SBA's cloud environment.[2]

Objective

Our evaluation's objective was to determine whether SBA's cloud migration efforts followed applicable federal guidance and standards. Our scope included SBA's cloud systems inventory, as well as SBA's cloud migration efforts and oversight from FY 2017 through FY 2018.

Results

SBA needs to improve its cloud migration and oversight controls in risk management, security, data mobility, and IT investments to meet federal guidance and standards. During the time of our review, SBA was taking steps to improve the accuracy of the inventory system it uses to monitor its cloud system inventory. These efforts will help ensure the appropriate controls are in place to protect its systems and data.

Effective deployment of identity and access management, contingency planning, risk management, and configuration management controls are critical to SBA having an effective information security program that achieves its mission/business needs. In addition, SBA needs to adopt standards to ensure it can efficiently move data among cloud platforms. These mobility controls accelerate the development and use of cloud computing standards and allow data migration to occur with minimal disruption.

[1] Report 16-16, Weakness Identified During SBA's Office 365 Cloud Email Migration.

[2] Report 18-14, Weaknesses Identified During the FY 2017 Federal Information Security Modernization Act Review.

Finding 1: SBA Needs to Update and Monitor Its Cloud Information System Inventory to Ensure Risk Management and Security Controls Are in Place to Protect Systems and Data

SBA did not consistently update and monitor its cloud system inventory to ensure system vulnerabilities are tracked and resolved. The lack of a complete and accurate cloud inventory prevents the Agency from knowing the extent to which its data resides outside its information system boundaries and is subject to the inherent risks of cloud systems. These potential risks may include exposing sensitive data and users ineffectively deleting or removing data at the end of a cloud contract. These risks could expose the Agency's data to unauthorized parties and potentially compromise program objectives. From April to August 2018, our review identified that OCIO was enhancing the accuracy of their system inventory program. However, our review identified that prior to their updates, their inventory records and document repository functions were not consistently updated for all cloud systems. In its recently updated security policies, SBA identified Cyber Security Assessment and Management (CSAM) as its primary tool to manage its information system inventory, including its cloud systems. However, in our tests and followup interviews, we identified that the functionality of CSAM has yet to be fully utilized to manage cloud inventory, including verifying system completeness of artifacts and the tracking vulnerabilities. According to OCIO, prior to 2018, their office relied solely on program offices and their system security officers to update CSAM.

OCIO's implementation procedures stipulate that CSAM serves as a vehicle to assist security managers in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in Agency programs and systems. However, our review of CSAM and interviews with system and security officials identified outdated and inaccurate records caused primarily by program offices' inconsistent implementation of CSAM procedures. NIST SP 800-53 R4, Security and Privacy Controls, requires agencies to develop and document an inventory of information system components that accurately reflects the current information system. OCIO implementation procedures for risk management require OCIO to coordinate with the applicable program office and to register IT systems in CSAM, and both OCIO and system owners are responsible to ensure data in the system is reliable and up-to-date. Our initial review of CSAM records identified 57 independent systems. However, at the time of our review, approximately 35 percent, or 20, of these systems records could not be accessed. OCIO stated they were in the process of correcting or consolidating these records, because they represented components of other systems or inactive systems.

Our review identified additional information within CSAM that was inaccurate or missing. Initially, OCIO reported that they had 11 cloud systems in operation or under development for 2018. However, during our review of the OCIO Security Operations Center, we were informed that an additional system was migrated to the cloud in 2018. Furthermore, our review identified five systems indicated by their systems security plans as using a cloud system as a component. The cloud systems identified in the system security plans were not included in SBA's cloud inventory. Our team followed up with OCIO to resolve the discrepancy. OCIO stated that the system security plans were outdated and that the components were routed through SBA's cloud or through a non-cloud system. Inaccurate and incomplete records hinder SBA's ability to monitor and control its cloud inventory.

In 2018, OCIO stated their office assumed responsibility for updating CSAM. However, at the time of our review, OCIO's vulnerability and baseline scanning teams informed us their testing processes do not include use of CSAM. Furthermore, the teams informed us they do not use their test results to update the system security plans in CSAM. This process is contradictory to NIST SP 800-37 R1, Risk Management Framework, which states that updates to security plans may be triggered by vulnerability scans. As a result, the Agency may not have effective oversight of its cloud data. For example, the security plans in CSAM may not be up-to-date, and critical vulnerabilities may go unresolved, which could result in unauthorized access, destruction, disclosure, and/or modification of information, as well as possible denial of service.

Recommendations

We recommend that the Administrator direct the Office of the Chief Information Officer to:

1. Enhance its cloud inventory controls through periodic updates and reconciliation of Cyber Security Assessment and Management with the current environment in accordance with SBA's IT Security Policy.

2. Instruct the vulnerability and baseline scanning teams to use Cyber Security Assessment and Management to update security plans, in accordance with NIST guidance.

Finding 2: SBA Needs to Improve Its Assessment and Monitoring of Cloud Service Providers to Address System Component Weaknesses and Identify Vulnerabilities

As SBA migrates its systems to the cloud, it will need to enhance its oversight processes to include monitoring cloud service providers' controls against SBA security requirements. Our FY 2018 FISMA review included testing of three SBA cloud systems that were included in the scope of this evaluation.[3] All three SBA cloud systems tested had findings related to identity and access management and contingency planning. One of the three cloud systems had findings in risk management, and another had findings in configuration management.

Identity and access management. Implementation of policies and procedures to ensure that only authorized users can access SBA resources. One system had not complied with SBA's IT Security Policy regarding session activity timeouts due to the settings having been inherited from the third-party vendor. By not complying with SBA's session inactivity timeout policy, there is a greater risk of unauthorized usage of the information system and the data within. The system owners for the two other cloud systems were unable to provide evidence of audit logging policies and procedures over the audit logging controls. In addition, one of the system owners was unable to provide evidence that appropriate access was authorized and granted for a selection of new users added. By not providing the appropriate evidence, there is a greater chance that potential vulnerabilities go unidentified within the audit logging processes for both systems.

Contingency planning. Establishment of processes to facilitate the recovery and restoration of an IT system following a disruption. Two of the three cloud systems could not document their ability to implement their information system contingency planning strategies. Neither system could provide tests or lessons learned documentation. One of the two systems could not provide a business impact analysis or a signed, approved contingency plan. Without a fully implemented contingency plan, system owners are unable to address system component weaknesses. The third cloud system owner could not provide evidence that backup schedules were performed by their cloud service provider that mitigates the loss of SBA data.

Risk management. Implementation of policies and procedures to safeguard SBA's ability to perform its mission and protect its assets. Risk management includes assessing and monitoring risk and should include oversight of contractor systems. For one cloud system, SBA did not enforce contractual requirements for the cloud service provider to provide information security posture reporting. Furthermore, SBA did not perform internal assessments to determine if whether the provider's security controls were designed, implemented, and operating effectively in accordance with SBA security requirements. Without oversight of contractor systems, SBA may not be aware of the actual security posture of the Agency's information systems and risks may not be identified and sufficiently mitigated.

Configuration management. Establishment and implementation of procedures to ensure the integrity of IT products and information systems. The system owner for one cloud system could not provide evidence that configuration management controls had been defined and implemented. A Configuration Management Plan or a Service Organization Controls report is required to satisfy this

[3] We incorporated finding elements identified during our FY 2018 FISMA review. To determine SBA's compliance with FISMA, OIG contracted with KPMG to perform review procedures relating to FISMA. KPMG interviewed SBA personnel, inspected documentation, and tested the effectiveness of SBA's IT security controls. OIG monitored KPMG's work and reported SBA's compliance with FISMA in the CyberScope submission to the U.S. Department of Homeland Security in October 2018.

requirement. Without formal, documented configuration management policies and procedures, baseline configurations for operating systems, databases, and network devices could be at risk to outside threats.

In all of the systems reviewed, vulnerabilities surfaced in access and identity management and contingency planning. In lieu of relying on the cloud service providers' security controls, the Agency retains overall responsibility and accountability for security. These responsibilities include establishing supplemental controls to meet its security and privacy requirements. Effective cloud system oversight processes, as required by NIST and OMB A-123 are essential to SBA in maintaining the integrity of information systems.

Recommendation

We recommend that the Administrator direct the Office of the Chief Information Officer to:

3. Ensure its existing cloud service provider security processes include FISMA monitoring controls in identity and access management, contingency planning, risk management, and configuration management.

Finding 3: SBA Needs to Adopt Standards to Ensure It Can Efficiently Move Data Among Cloud Platforms

SBA did not ensure that its cloud system contracts contained enabling language to facilitate efficient data movement among cloud providers, as outlined in NIST SP 500-291, Version 2, Cloud Computing Standards Roadmap, and recommended in best practices in acquiring IT as a service. Moreover, our review of SBA's standard operating procedures (SOP) found that controls over interoperability, portability, and data ownership were not documented.

NIST guidance states cost-effective and seamless migration requires interoperability, portability, and data ownership standards. Also, a lack of interoperability affects the availability of data and complicates the portability of data between cloud providers.[4] Furthermore, without interoperability and portability standards, SBA cannot ensure that mission-critical requirements are met, and they increase the risk that sizable investments may become obsolete. NIST guidelines on security and privacy state that ownership rights over data must be firmly established in service contracts to secure the privacy of data. NIST guidance, while dynamic and changing, would provide SBA confidence that its data and related applications will operate on multiple cloud environments. NIST guidance also promotes a level playing field among cloud service providers, which would provide SBA more marketplace options.

While interoperability is considered for new investments in the SBA Business Technology Investment Council's oversight of IT investments in SOP 90 82, Procedure for Managing SBA IT Investments, our review of SBA's policies and procedures did not identify controls, i.e., standards, to ensure interoperability, portability, and data ownership.[5] In addition, through our review of documentation for 11 cloud systems and interviews with designated system owners, we identified only one system where documentation relating to data movement protocols was provided by the system owner.[6]

Recommendations

We recommend that the Administrator direct the Office of the Chief Information Officer to:

4. Develop and implement policies and procedures to formalize systems and data interoperability, portability, and data ownership in migrating systems to the cloud, as specified in NIST SP 500-291, Cloud Computing Standards Roadmap.

5. Coordinate with system owners and contracting officers to ensure reviewed contracts with cloud service providers specify data and system interoperability, portability, and data ownership as specified in NIST SP 500-291, Cloud Computing Standards Roadmap.

[4] Cloud interoperability means that data can be processed by different services on different cloud systems through common specifications. Cloud portability means that data can be moved from one cloud system to another.
[5] In addition to SOP 90 82, we also reviewed SOP 20 21, Government Acquisitions Program; SOP 90 47 4, IT Security Policy; SOP 90 52, IT Investment Policy; SBA's systems development methodology; and OCIO implementation procedures.
[6] Our review included contracts, statements of work/objectives, and configuration management plans.

Finding 4: SBA Needs to Improve Its Ability to Document Cloud Cost Savings and Service Level Requirements to Monitor Performance and Costs

SBA's management system did not allow the Agency to accurately measure whether cloud migration improvements occurred, whether cost avoidance and savings were within projections, and whether appropriate service level agreements (SLAs) had been defined within contracts. [7] [8] The federal government initiated its 'cloud first' policy in December 2010. However, at the time of our review, SBA's cloud migration strategy was still in draft. This draft strategy stated there is no doubt that deploying SBA applications in the cloud can lower infrastructure costs, increase business agility, and remove the undifferentiated "heavy lifting" within the enterprise.

As required by OMB Circular A-11, our review identified a need for a process to capture estimated cost savings and/or cost avoidance from cloud migration and data center consolidation. However, OCIO could not fully support its performance goal of $10.8 million in cost savings and cost avoidance for data center consolidation and cloud migration.[9] We requested the documentation SBA used to generate its performance goal, and we also requested SBA's cloud migration strategy and policies. The cost documentation SBA provided totaled approximately $8 million. Without adequate support justification, stakeholders cannot rely on SBA's cost savings and cost avoidance data for strategic planning and budgeting.

Since 2017, SBA has made improvements in its oversight of IT investments in accordance with the requirements of Federal Information Technology Acquisition Reform Act.[10] However, we found that SBA could not provide the initial business cases for four cloud-based major IT investments.[11] Without documentation of initial business cases for cloud IT investments, SBA cannot ensure that these investments align with strategic plans, budget goals, and procurement requirements, as required by OMB Circular A-11. SBA provided revisions to project investments cases but could not provide the original business cases that would provide a basis to accurately measure progress and cost effectiveness of cloud activities against a baseline, as required by the Procedure for Managing SBA IT Investments. Business cases were also not provided for four other cloud investments, and documentation provided and followup interviews did not show evidence of review and authorization by SBA's investment and architecture review boards.[12] These omissions occurred because OCIO had not implemented a process to document the use and retention of business cases for IT investments.

SBA needs a process to strengthen oversight of cloud service provider performance through SLAs. SBA's IT and acquisition policies and procedures do not provide specific guidance on SLAs. To

[7] OMB Circular A-11 states that if an agency makes an advanced technology investment to achieve certain cost savings and quality improvements, the management system should permit the agency to measure whether these improvements occurred and whether operations and maintenance costs are within projections.

[8] SLAs define performance with clear terms and definitions, demonstrate how performance is being measured, and delineate what enforcement mechanisms are in place to ensure SLAs are met.

[9] SBA's FY 2019 Congressional Budget Justification and FY 2017 Annual Performance Report stated that SBA could save/avoid $10.8 million in data center consolidation and cloud migration. This estimate was part of a strategic objective performance goal for enterprise-wide information system modernization and cost-effective technology.

[10] Examples of improvements include requiring program offices to engage with SBA's investment review board.

[11] Business cases provide the baseline data from which progress is measured and project goals are verified.

[12] SBA developed the Business Technology Investment Council (BTIC) to serve as SBA's investment review board. To support the BTIC, SBA revised its Architecture Review Board to oversee IT technical assessments and support the IT acquisitions process.

ensure the reliability of SBA's cloud systems, we reviewed contract documentation to assess SLAs. System owners did not provide evidence that service levels were incorporated into contracts for five cloud systems. OMB Circular A-123 states that agencies must have a process for monitoring the service organization's performance in relation to various metrics, as typically defined in an SLA. Most of these metrics must be tailored to specific operations. For example, agencies regularly review the security, availability, and processing integrity of SLAs.[13] The NIST Cloud Computing Standards Roadmap further states that agencies using cloud services should be careful to include suitable performance, monitoring, and emergency metrics and conditions into the cloud service master agreement and associated SLAs. These elements, reflecting the agency's given mission and goals, will help to ensure that each agency will pay only for needed services. According to the federal guide on best practices for acquiring IT as a service, cloud consumers should ensure that their service provider's performance is clearly specified in all SLAs, and that all such agreements are fully incorporated into the contract. Without SLAs, SBA cannot fully measure and hold cloud service providers accountable for performance.

Recommendations

We recommend that the Administrator direct the Office of the Chief Information Officer to:

6. Develop a process for capturing performance goal estimates and actual cost savings and cost avoidance for IT initiatives, such as cloud migration and data center consolidation, as required by OMB Circular A-11.

7. Follow SBA IT investment guidance by documenting cloud migration decisions through approval of applicable business cases from the Business Technology Investment Council and Architecture Review Board.

8. Ensure Agency contracts and related oversight controls with cloud service providers, such as cloud service master agreements and associated service level agreements clearly define roles and responsibilities, performance metrics, and remediation plans for noncompliance in accordance with OMB Circular No. A-123 and NIST SP 500-291, Version 2.

[13] OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control.

Analysis of Agency Response

SBA management fully agreed with four recommendations and partially agreed with four recommendations. We found that SBA's planned corrective actions resolved each of the eight recommendations.

Summary of Actions Needed to Close the Recommendations

The following provides the status of recommendations and the actions necessary to close them.

1. **Resolved.** SBA management agreed to our recommendation. By April 30, 2019, OCIO will update its CSAM tool to align with the Agency FISMA inventory, to include cloud service providers currently in use. This recommendation can be closed once SBA provides evidence that CSAM cloud inventory controls are periodically enhanced and updated to reflect the current environment in accordance with SBA's IT Security Policy.

2. **Resolved.** SBA management agreed to our recommendation. By April 30, 2019, OCIO will ensure that the CSAM tool reflects results from vulnerability and configuration scan results, as applicable. This recommendation can be closed once SBA provides evidence that vulnerability and baseline scanning teams are using CSAM to update security plans in accordance with NIST guidance on risk management.

3. **Resolved.** SBA management agreed to our recommendation. By April 30, 2019, OCIO will improve its process for the monitoring of controls provided by leveraged cloud service providers. This recommendation can be closed once SBA provides evidence that it has improved the process for monitoring cloud service provider controls in identity and access management, contingency planning, risk management, and configuration management.

4. **Resolved.** SBA management partially agreed with our recommendation. However, SBA's planned corrective action resolved the recommendation. By September 30, 2019, OCIO will develop guidance that formalizes the use of published system design principles, contract clauses, standards, and ongoing IT projects. IT project teams will be instructed to incorporate this guidance into their development lifecycle process. To comply with NIST SP 500-291, Version 2, NIST Cloud Computing Standards Roadmap, OCIO will establish a specific principle to ensure only authorized FedRAMP services are consumed. This recommendation can be closed once SBA provides evidence that data ownership, portability, and interoperability policies have been developed and implemented for cloud systems, as specified by NIST.

5. **Resolved.** SBA management partially agreed with our recommendation. However, SBA's planned corrective action resolved the recommendation. By September 30, 2019, the Architecture Review Board will meet with program office representatives to ensure that project teams are aware of the required system design principles, contract clauses, standards, and ongoing IT projects. Communication of this information will be tracked in meeting minutes published within the OCIO Enterprise Architecture website. This recommendation can be closed once SBA provides evidence that data ownership, portability, and interoperability are incorporated into existing cloud service provider contracts, as specified by NIST and required by OMB Circular A-123.

6. **Resolved.** SBA management partially agreed with our recommendation. However, SBA's planned corrective action resolved the recommendation. The target date for final action is

September 30, 2019. OCIO is currently tracking both cost savings and avoidance. In the future, OCIO is planning to improve its ability to establish and measure performance goals and estimates. This recommendation can be closed once SBA provides evidence that a process for capturing performance estimates and actual cost savings and avoidance for IT initiatives has been established, as required by OMB Circular A-11.

7. **Resolved.** SBA management agreed to our recommendation. By September 30, 2019, the OCIO Enterprise Architecture team will develop clear criteria for the Architecture Review Board (ARB) process that ensures all new cloud-based technologies are directed to the Architecture Review Board Assessment workflow. This recommendation can be closed once SBA provides evidence that cloud migration decisions are being approved by the Business Technology Investment Council and the ARB, as required by SBA's Procedure for Managing SBA IT Investments and ARB guidance.

8. **Resolved.** SBA management partially agreed with our recommendation. However, SBA's planned corrective action resolved the recommendation. By September 30, 2019, OCIO will establish basic guidance for cloud service provider master agreements that ensures roles and responsibilities, performance metrics, and remediation plans conform to the guidance as described in NIST SP 500-291, Version 2, NIST Cloud Computing Standards Roadmap. This recommendation can be closed once SBA provides evidence that contracts and related controls with cloud service providers, such as cloud service master agreements and associated service level agreements are updated to clearly define roles and responsibilities, performance metrics and remediation plans in accordance with OMB Circular No. A-123 and NIST SP 500-291, Version 2.

Appendix I: Objective, Scope, and Methodology

Our evaluation's objective was to determine whether SBA's cloud migration efforts followed applicable federal guidance and standards. Our scope included SBA's cloud systems inventory, as well as SBA's cloud migration efforts and oversight from FY 2017 through FY 2018.[14]

To answer our objective, we reviewed federal guidance and standards, and we assessed SBA policies and procedures. During the planning and survey phases of this evaluation, we primarily requested and reviewed documentation from OCIO and interviewed OCIO officials. We reviewed system inventories, business cases, system security plans, and contracts. During the fieldwork phase of this evaluation, we followed up with document requests to system owners and a contracting specialist, and we interviewed the system owners and program officials. We reconciled information gathered from OCIO officials to the information gathered from the system owners, and we assessed the results.

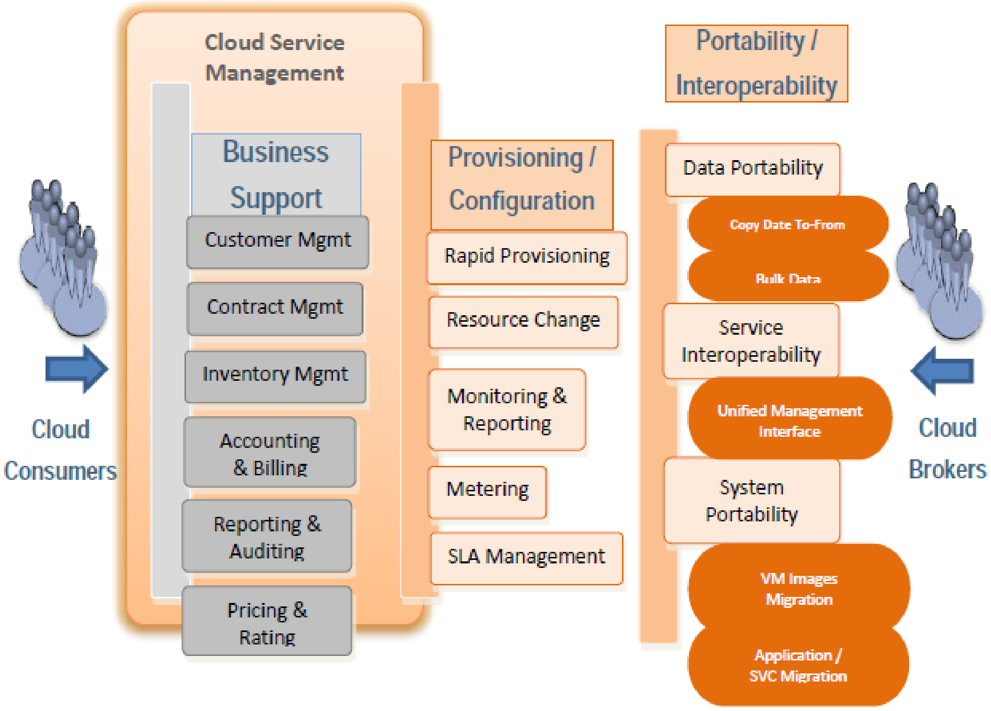
We also incorporated finding elements identified during our FY 2018 FISMA review. To determine SBA's compliance with FISMA, OIG contracted with KPMG to perform review procedures relating to FISMA. KPMG interviewed SBA personnel, inspected documentation, and tested the effectiveness of SBA's IT security controls. OIG monitored KPMG's work and reported SBA's compliance with FISMA in the CyberScope submission to DHS in October 2018.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's quality standards for inspection and evaluation. Those standards require that we adequately plan and perform the evaluation to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objective. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our objective.

[14] The cloud system TeamMate was excluded from testing because it is an OIG system.

Appendix II: Cloud Service Management

NIST SP 500-291, Version 2, NIST Cloud Computing Standards Roadmap, states cloud service management includes all the service-related functions that are necessary for the management and operation of those services required by or proposed to cloud consumers. As illustrated in our report and in the NIST diagram below, cloud service management can be described from the perspectives of business support, provisioning and configuration, and portability and interoperability requirements.



Appendix III: Agency Comments

U.S. Small Business Administration

DATE: April 3, 2019

TO: Hannibal "Mike" Ware
Inspector General

FROM: Maria Roat
Chief Information Officer

MARIA ROAT Digitally signed by MARIA ROAT
Date: 2019.04.04 15:19:35 -04'00'

SUBJECT: OIG Project 18005, *SBA's Cloud Migration and Oversight*

Thank you for providing the U. S. Small Business Administration (SBA) with a copy of the draft report titled "SBA's Cloud Migration and Oversight", OIG Project 18005. The draft report analyzes whether SBA's cloud migration efforts followed applicable federal guidance and standards. The scope included SBA's cloud systems inventory and SBA's cloud migration efforts and oversight from FY 2017 through FY 2018. OIG provided eight recommendations in the following areas: cloud inventory and monitoring controls, data ownership portability and interoperability, and improved documentation of cloud cost savings and service level requirements.

SBA Office of the Chief Information Officer (OCIO) agrees with recommendations one, two, three and seven, and partially agrees with recommendations four, five, six and eight. While we generally agree with the recommendations, several of the recommendations related to services that were in the process of being implemented, or were undergoing transition with an expected completion date by the end of this month.

Additionally, OCIO would like to provide full context to SBA's significant progress in moving the agency's information technology, cloud computing services, and cybersecurity functions forward. The audit was conducted during modernization and mid-stream of migrating its data center and applications to the cloud. OCIO has been and will continue to track and report cost savings and avoidance to the Office of Management and Budget. Additionally, OCIO will continue to leverage, and align with, the Federal Risk and Authorization Management Program (FedRAMP) standards for security assessments, authorizations, and continuous monitoring for cloud products and services, and the FAR 46.202-1 for Service Level Agreements.

Thank you for the opportunity to comment on this draft report. Specific responses to each recommendation were provided under separate cover. SBA appreciates OIG's consideration of our comments prior to publishing the final report.