Cloud Service Provider Governance Performance Audit

PUBLIC RELEASE

OFFICE OF INSPECTOR GENERAL

LIBRARY

LIBRARY OF CONGRESS

2020-IT-103
January 2022
This page left blank intentionally
Date      January 26, 2022
To        Dr. Carla Hayden
          Librarian of Congress
From      Kimberly Byrd
          Acting Inspector General
Subject   Cloud Service Provider Governance Performance Audit—Audit No.
          2020-IT-103

This transmits our final report for the Office of the Inspector General’s audit of the
Library of Congress’s Cloud Service Provider Governance performance.

The report contains 21 recommendations intended to improve management and
operational efficiencies, in addition to managing risks at acceptable levels, as the Library
continues to integrate cloud infrastructure and services.

Based on management's written responses to the draft report, we consider all of the
recommendations resolved. Your responses provided an action plan for implementing the
recommendations in accordance with LCR 9-160, Rights and Responsibilities of
Employees to the Inspector General, §6.A.

We appreciate the cooperation and courtesies extended by the Library during this audit.

cc       Principal Deputy Librarian
         Chief Information Officer
         Chief Financial Officer
         General Counsel
Table of Contents

OIG Appendix: Cotton & Company Audit Report ........................................................................2
OIG Appendix: Cotton & Company Audit Report
LIBRARY OF CONGRESS
CLOUD SERVICE PROVIDER GOVERNANCE PERFORMANCE AUDIT
AUDIT REPORT

January 24, 2022

Cotton & Company LLP
333 John Carlyle Street
Suite 500
Alexandria, Virginia 22314
703.836.6701
www.cottoncpa.com
Loren Schwartz, CPA, CISA, CISSP, Partner
lschwartz@cottoncpa.com
# TABLE OF CONTENTS

I. EXECUTIVE SUMMARY .................................................................................................................. 1  
   SUMMARY OF RESULTS .............................................................................................................. 1

II. BACKGROUND ............................................................................................................................... 5 
   DEFINING CLOUD COMPUTING .................................................................................................. 5  
   BENEFITS OF CLOUD COMPUTING ......................................................................................... 6  
   RISKS OF CLOUD COMPUTING ............................................................................................... 7  
   FedRAMP ..................................................................................................................................... 7  
   KEY LIBRARY ORGANIZATIONS WE ENGAGED ......................................................................... 9

III. AUDIT RESULTS ........................................................................................................................... 10 
   FINDING 1: THE LIBRARY IS UNABLE TO IDENTIFY CURRENT-STATE CLOUD SERVICES IN A RELIABLE AND EFFECTIVE MANNER. .... 10  
   FINDING 2: THE LIBRARY DOES NOT HAVE AN ACTIONABLE CLOUD STRATEGY. ................. 13  
   FINDING 3: THE LIBRARY HAS NOT DEVELOPED A SYSTEM ADMINISTRATION MANUAL FOR THE OGS. .............................................. 15  
   FINDING 4: THE LIBRARY HAS NOT PERFORMED A GAP ANALYSIS AS PART OF ITS CLOUD STRATEGY WORKFORCE DEVELOPMENT AND PLANNING COMPONENT. ........................................................................................................... 17  
   FINDING 5: THE LIBRARY’S CLOUD CONTRACTS LACK DETAILED SERVICE-LEVEL INFORMATION REGARDING DATA PRESERVATION AND MIGRATION. ............................................................................................................................... 19  
   FINDING 6: THE LIBRARY DOES NOT CONSISTENTLY APPLY THE RISK MANAGEMENT FRAMEWORK TO ITS CLOUD APPLICATIONS. .......... 23  
   FINDING 7: THE LIBRARY DOES NOT CONSISTENTLY IMPLEMENT ITS COST ESTIMATION AND MONITORING REQUIREMENTS FOR CLOUD MIGRATIONS. ......................................................................................................................... 28

APPENDIX A – OBJECTIVE, SCOPE, AND METHODOLOGY .......................................................... 33  
APPENDIX B – MANAGEMENT RESPONSE .................................................................................... 36
Ms. Kimberly Byrd  
Acting Inspector General  
Office of Inspector General  
U.S. Library of Congress  

Dear Ms. Byrd,

Cotton & Company LLP is pleased to submit the attached audit report detailing the results of our performance audit of the Library of Congress’ cloud strategy, governance, technical planning, and procedures. The Library Office of Inspector General engaged Cotton & Company to conduct this performance audit pursuant to Contract Number LCOIG20D0004. Cotton & Company performed the work from September 2020 through January 2022.

Cotton & Company conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Sincerely,

Cotton & Company LLP

Loren Schwartz CPA, CISA, CISSP  
Partner
I. EXECUTIVE SUMMARY

Cloud computing refers to an emerging information technology (IT) delivery model in which computing resources (e.g., networks, servers, storage, applications, services) are accessible over the Internet. Through this model, a provider of these computing services—called a cloud service provider (CSP)—allows customers to rent its computing resources and increase or decrease their usage as needed with minimal effort. This differs significantly from the traditional on-premises model, in which an organization is fully responsible for planning and implementing its own computing infrastructure.

Over the last decade, federal government agencies have increasingly adopted cloud computing technology, moving their applications from on-premises data centers to the cloud. In response to this trend, components of the federal government have attempted to standardize the cloud adoption process. In 2011, the Federal Chief Information Officer (CIO)\(^1\) developed a cloud strategy called Cloud First that gave agencies broad authority to increase their reliance on cloud technology. In 2018, the Federal CIO updated this strategy to Cloud Smart, which includes actionable recommendations for federal agencies that are adopting cloud services.

Consistent with the government-wide trend toward cloud technology, the Library of Congress (Library) has migrated systems in its inventory from its legacy primary on-premises data center to a new computing architecture. This process included establishing a new data center and network infrastructure and increasing its cloud utilization. The Library Office of the Chief Information Officer (OCIO) began planning for this Data Center Transformation (DCT) project in 2016, and the Library obtained congressional funding for the project beginning in 2017. According to the Library OCIO’s 2021–2024 Directional Plan, the Library intends to support its systems with a hybrid environment consisting of a combination of modernized data centers and purchased cloud services. The Library Office of the Inspector General (OIG) engaged Cotton & Company to conduct a performance audit of the Library’s cloud practices. Our objective was to determine whether the Library has implemented adequate governance controls to ensure that its cloud services are secure, operationally suitable, and cost-beneficial.

To achieve this objective, Cotton & Company performed a combination of inquiries, inspections of policies and procedures, and assessments of a sample of cloud implementations to test the Library’s current organizational practices against the guidance within the federal Cloud Smart strategy, relevant criteria from National Institute of Standards and Technology (NIST) and the Government Accountability Office (GAO), and other best practices.

Summary of Results

We found that the Library made partial progress regarding all three elements of the Cloud Smart strategy: security, procurement, and workforce.

\(^{1}\) The Federal CIO is a member of the Office of Management and Budget (OMB) and oversees federal IT policy and strategic planning for all federal IT Investments.
• The Library’s Assessment and Authorization (A&A) Guidance includes requirements for authorizing systems, including those running on a cloud platform, in accordance with NIST frameworks and the Federal Risk and Authorization Management Program (FedRAMP).2

• The Library of Congress Federal Acquisition Regulation documents include standard processes for soliciting services.

• The Library recognized the necessity of training certain personnel in cloud technology and developed a Cloud Integrated Product Team (IPT) in response.

However, despite these positive achievements, Cotton & Company noted the following deficiencies:

**The Library is unable to identify current-state cloud services in a reliable and effective manner.**

The Library is transitioning to a more cloud-centric environment; however, the Library cannot easily track its progress with regard to the transition, as it was unable to consistently provide an effective list of current-state cloud services as of the end of our fieldwork. Specifically, the Library uses the Archer application as its system of record for all IT systems currently in use. For each system, Archer includes information about the accreditation status, system categorization, and implementation of each control. Archer is also able to identify whether the system is hosted by the Library or by a contractor. However, Archer only provides more detailed information regarding the system-hosting environment, such as the type of cloud-hosting environment or service provider, through a “System Environment” text box that the Library cannot use for filtering results or sorting a custom system list.

**The Library does not have an actionable cloud strategy.**

Library personnel spoke to us regarding the Library’s future plans related to the cloud; however, the Library’s documented cloud strategy—which was under development during the course of our audit—primarily provided high-level principles and omitted details regarding key considerations identified in the federal Cloud Smart strategy, including:

• Intended outcomes and capabilities of the Library’s cloud-specific security program, including considerations of continuous data protection and awareness.

• Cloud-specific IT security requirements for contracts.

• A workforce development and planning component with a tailored transformation and training approach.

---

2 FedRAMP is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies.
The Library plans to draft a more detailed cloud implementation plan to support its cloud strategy by the second quarter (Q2) of 2021. As of November 2021, the Library updated its forecast to publish the cloud implementation plan by the end of the first quarter (Q1) of 2022.

The Library has not developed a system administration manual for the OCIO Google Services (OGS).
The Library plans to implement multiple applications on the OGS, including one application that the Library released into production in December 2020; however, the Library has not developed an operations manual for its OGS implementations, as it did for its Amazon Web Services (AWS) implementations. The AWS operations manual includes detailed information regarding account creation, system roles within the platform, and audit logging responsibilities. Without a similar operations manual for OGS, Library personnel may not be aware of their responsibilities for administering accounts on this platform. As of November 2021, the Library has demonstrated progress on a draft OGS System Administration Manual and provided an updated forecast completion of Q1 2022.

The Library has not performed a gap analysis as part of its cloud strategy workforce development and planning component.
The Library began procuring cloud services in fiscal year (FY) 2017, as part of the DCT program. This effort required the Library to transform its workforce, including hiring individuals with cloud experience to facilitate effective cloud adoption within the Library. The Library established the Cloud IPT, a group comprising several groups within the OCIO, and made cloud training available to the individuals within this group. However, the OCIO has not performed a cloud skills gap assessment for all members of the Cloud IPT that:

- Maps current IT workforce resources to future skill and position requirements.
- Identifies both technical and non-technical skill and position gaps.

Completing a skills gap assessment and creating a workforce development and planning component for its cloud strategy will better equip the Library to manage cloud-related security, privacy, and procurement issues as they arise.

The Library’s cloud contracts lack detailed service-level information regarding data preservation and migration.
In 2016, the Library procured a multiple-award Indefinite Delivery-Indefinite Quantity (IDIQ) contract for cloud services from AWS and the OGS (Contract No. LCNLS16C0070). The IDIQ contract was accompanied by a Service Level Agreement (SLA) that listed metrics for availability, performance, and communication attributes. However, the SLA requirements were missing language describing how the service provider will transition Library data back to the Library in the event of contract exit/termination, as recommended by NIST Special Publication (SP) 800-144, Guidelines on Security and Privacy in Public Cloud Computing, Section 5, and GAO-16-325, Cloud Computing – Agencies Need to Incorporate Key Practices to Ensure Effective Performance. Without this language in place in its contracts, the Library may not be able to successfully preserve agency data in the event of a cloud contract termination scenario.
The Library does not consistently apply the risk management framework to its cloud applications.


1. **Prepare** to execute the RMF from an organization and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
2. **Categorize** the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.
3. **Select** an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.
4. **Implement** the controls and describe how the controls are employed within the system and its environment of operation.
5. **Assess** the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
6. **Authorize** the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.
7. **Monitor** the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

We assessed RMF compliance for a selection of Library cloud systems and noted the following discrepancies in the Library’s A&A implementation:

1. The Library significantly reduced the control baseline for its Low Impact Externally Hosted (LIEH) systems compared to the established NIST baselines without documenting either its rationale for doing so or its acceptance of risk for excluding individual controls.
2. The Library’s System Security Plans (SSPs) do not consistently provide details regarding why some of its system controls are listed as “Inherited” or “Not Applicable,” such as identifying the system from which the control is inherited or why the control was not applicable.
3. The Library does not consistently remediate system risks documented in its Plan of Action & Milestones (POA&Ms) in accordance with Library-defined timeframes.
4. The Library does not consistently design and implement each system’s continuous monitoring (CM) strategy in accordance with its continuous monitoring requirements. These inconsistencies included:
a. Not assessing all applicable controls at the Library-defined frequency.
b. Not including all required controls, as defined by the system baseline, within the system’s continuous monitoring plan.

**The Library does not consistently implement its cost estimation and monitoring requirements for cloud migrations.**

Cloud computing offers potentially significant cost savings for customers. However, not all applications are suitable for the cloud, due to factors such as regulatory requirements, application design, and technical architecture; as a result, these applications may cost more to migrate into a cloud environment. The Council of CIO’s *Application Rationalization Playbook, An Agency Guide to Portfolio Management* advises that agencies assess Total Cost of Ownership (TCO) information of its existing applications, score its applications based on the TCO, business value, and technical fit, and use the score to assess hosting options and alternatives for its applications. Organizations therefore should not approve cloud implementation for an application unless they have performed an analysis demonstrating that cloud computing has the lowest TCO compared to other alternatives. Organizations should also track cloud implementation costs during operation to ensure that the organization can quantify any resulting savings and cost avoidances. Our team was unable to obtain evidence supporting that the Library performed an independent cost estimate for the migration of 10 selected applications to the cloud, rather than continuing to host the 10 applications on-premises. Additionally, the Library does not have mechanisms in place to track cost savings and cost avoidances for two selected applications for which an on-premises option was available.

**II. BACKGROUND**

**Defining Cloud Computing**

NIST SP 800-145, *The NIST Definition of Cloud Computing*, defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The publication goes on to identify five essential characteristics of cloud computing:

- **On-Demand Self-Service**: A consumer can unilaterally provision computing capabilities as needed, automatically, without requiring human interaction from the service provider.
- **Broad Network Access**: Capabilities are available over the network and accessed through standard mechanisms (e.g., mobile phones, tablets, laptops, workstations).
- **Resource Pooling**: The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- **Rapid Elasticity**: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the
consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

- **Measured Service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active user accounts). Resource usage can be monitored, controlled, and reported.

A CSP allows customers to rent its computing resources. These computing resources can include networks, servers, storage, applications, and services.

NIST SP 800-145 identifies three cloud service models that encompass the different cloud customer use cases, as shown in the table below:

<table>
<thead>
<tr>
<th>Service Model</th>
<th>Primary Use Case</th>
<th>Customer Manages</th>
<th>CSP Manages</th>
</tr>
</thead>
</table>
| Infrastructure as a Service (IaaS) | Organizations seeking to minimize the complexity of capacity planning | • Data  
• Applications  
• Middleware  
• Operating System | • Storage capacity  
• Networks  
• Servers |
| Platform as a Service (PaaS)  | Developers using the tools provided by a PaaS to create cloud-based applications | • Data  
• Applications | • Middleware  
• Operating System  
• Storage capacity  
• Networks  
• Servers |
| Software as a Service (SaaS)  | Customers in need of a specific software solution | | • Applications  
• Middleware  
• Operating System  
• Storage capacity  
• Networks  
• Servers  
• Data |

**Source**: NIST SP 800-145: The NIST Definition of Cloud Computing, Description of Service Models on RedHat website.³

**Benefits of Cloud Computing**

Regardless of the cloud service model used, transitioning to a cloud model provides potential benefits. NIST SP 800-146, Cloud Computing Synopsis and Recommendations, lists specific examples, including:

- **Savings in Up-Front Costs**: A customer does not need to expend the high costs required to provision and configure their own IT infrastructure to run an application, instead they can rent space on a CSP’s existing infrastructure and pay a recurring usage fee.

- **Rapid Scalability**: Cloud customers are able to increase or decrease their usage of cloud resources on demand. This allows customers to respond quickly to changing business

needs, rather than under-utilizing or exceeding the more static capacity of an on-premises infrastructure.

- **Decreased Administrative Burden**: The CSP will assume significant IT responsibilities to operate the customer’s application environment, decreasing the day-to-day IT responsibilities for the customer.

### Risks of Cloud Computing

According to NIST SP 800-146, migrating from on-premises IT solutions to cloud-based solutions introduces several new cross-organizational risks. First, although the customer retains ultimate responsibility for its data in a cloud environment, it loses some ability to enforce controls over that data. Specifically, when supporting its own IT operations, an organization will implement a combination of administrative, physical, and technical controls to protect the confidentiality, integrity, and availability of its data in accordance with its own policies and procedures and applicable laws and regulations. Organizations have less ability to implement and monitor these controls when their data is hosted on a CSP’s environment. The customer must obtain sufficient assurance that the CSP’s controls align with its needs and gain an understanding of its own control responsibilities. A cloud customer must also consider the increased exposure inherent to a cloud environment.

The customer must also carefully consider the performance and legal implications of transferring data responsibility to a CSP. Potential considerations include availability of the cloud service, remedies for failure to perform, and restrictions on the use of customer data. Contracts and SLAs documenting these considerations must be clear and detailed to protect the customer.

There are significant indirect costs associated with migrating a system to—or initiating a system as—a cloud environment. These include costs related to:

- Ensuring cloud compliance with organization policies.
- Training and recruiting a cloud-ready workforce.
- Reengineering an application, if necessary, to be suitable for a cloud environment.
- If necessary, migrating out of a cloud environment in the event of performance or business continuity issues.

Without adequate consideration of the TCO for a cloud implementation, a customer may not realize cost savings from moving to the cloud.

**FedRAMP**

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
FedRAMP empowers agencies to use modern cloud technologies with emphasis on security and protection of federal information, as well as helps accelerate the adoption of secure cloud solutions.⁴

According to FedRAMP documents, the program includes objectives to:

- Ensure cloud systems used by government entities have adequate safeguards.
- Eliminate duplication of effort and reduce risk management costs.
- Enable rapid and cost-effective government procurement of information systems/services.

There are two types of FedRAMP authorizations: a Provisional Authority to Operate (P-ATO) from the FedRAMP Joint Authorization Board (JAB) and an Agency Authority to Operate (ATO).⁵

For either authorization, the FedRAMP program requires the CSP to be accredited under the FedRAMP process before the federal government may procure the CSP’s services. CSPs expend a tremendous amount of resources to have their services authorized through FedRAMP.⁶ Specifically, FedRAMP requires CSPs’ systems to undergo a Security Assessment Framework (SAF), which is a modified version of the NIST RMF.⁷ Under the SAF, the CSP must categorize each of its systems in accordance with Federal Information Processing Standards (FIPS) 199,⁸ select security controls based on that categorization, and implement those security controls.

The CSP must detail these controls in an SSP. Subsequently, the CSP must engage an organization called a Third-Party Assessment Organization (3PAO)⁹ to assess the controls. This assessment results in the creation of a FedRAMP package, which includes, at a minimum, the following documents:

- **SSP:** Contains details regarding how the CSP has implemented each required security control.
- **Security Assessment Plan (SAP):** Developed by the 3PAO. The SAP documents the scope and testing methodology of the assessment.

---

⁴ [https://www.gsa.gov/technology/government-it-initiatives/fedramp](https://www.gsa.gov/technology/government-it-initiatives/fedramp)
⁵ [https://www.fedramp.gov/jab-authorization/#jab-authorization-process](https://www.fedramp.gov/jab-authorization/#jab-authorization-process)
⁶ According to the FedRAMP Cloud Service Provider Process Description.
⁷ According to NIST SP 800-37, Rev 2, the RMF provides a process to integrate security and risk management activities into the system development life cycle (SDLC).
⁸ FIPS 199 defines a system categorization as low, moderate, or high based on the potential impact of a system’s breach of data confidentiality, integrity, and availability.
⁹ According to FedRAMP ([https://www.fedramp.gov/assessors/](https://www.fedramp.gov/assessors/)), a 3PAO is an independent organization that is approved by the FedRAMP program to perform initial and periodic security assessments of cloud systems.
- **Security Assessment Report (SAR):** Documents the results of the 3PAO’s assessment. The SAR contains information about vulnerabilities, threats, and risks discovered during the testing process.

- **POA&Ms:** Developed by the CSP in response to the vulnerabilities identified in the SAR. The POA&M demonstrates that the CSP has a plan in place—complete with staffing, resources, and a schedule—for correcting each security weakness identified.

The CSP delivers these and other supporting documents collectively as a package to an agency authorizing official (AO) or the JAB for authorization review. Once the AO or the JAB approves the package, the CSP is included on the list of authorized CSPs on the FedRAMP website. As of September 29, 2021, there are 238 FedRAMP-authorized products in the FedRAMP marketplace.

In addition to the approval process, authorized FedRAMP services must undergo both monthly and annual continuous monitoring processes to enable timely risk management decisions. These processes result in recurring updates to the SSP, SAR, and POA&Ms.

After a CSP system has been approved through FedRAMP, agencies may use the CSP’s service offerings and leverage the documentation within the FedRAMP authorization package. The agency does so by formally requesting FedRAMP packages from the FedRAMP Program Management Office, which limits access to only those seeking to grant a security authorization. The agency must still issue its own ATO, as the Federal Information Security Modernization Act of 2014 (FISMA) requires agencies to individually accept the risk of use of any IT system. However, using an existing FedRAMP package decreases the FISMA compliance costs for the agency, as it lessens the need for the agency to assess a CSP’s controls as part of its own authorization process.

FedRAMP is explicitly required for executive departments and agencies, but it is not mandatory for legislative-branch agencies such as the Library. However, the Library OCIO recommends leveraging FedRAMP-compliant packages when possible. When it is not possible to leverage a FedRAMP-compliant package, the Library must perform a full assessment of the CSP’s security controls.

### Key Library Organizations We Engaged
The Library is headed by the Librarian of Congress, who is supported by multiple service units. Our audit procedures were primarily directed to the OCIO service unit, which is responsible for

---

10 According to NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*, an ATO is a formal decision made by an organization-designated official to operate an information system and accept the risks of doing so. This authorization is not indefinite and must be re-performed periodically.


12 According to the FedRAMP Policy Memorandum, dated December 8, 2011
IT project management, IT security, data management, and IT operations at the Library. The OCIO consists of directorates that are responsible for different aspects of IT. Below are the directorates that we directly engaged during testing:

- **IT Service Operations (ITSO):** Responsible for data center selection and management, including server management, storage management, and capacity planning.
- **IT Governance (ITGOV):** Develops and maintains Library policies, procedures, and standards on IT management across the Library; responsible for organizational risk management and IT strategic planning.
- **IT Financial Management (ITFM):** Maintains oversight of the financial management of IT investments at the Library; facilitates the requisitioning of agency non-personnel IT resources and services.
- **IT Design & Development (ITDD):** Supports all aspects of design and development for mission critical business applications, including integration, quality assurance, and maintenance, as well as content/data distribution, maintenance, and management.
- **IT Security (ITSEC):** Ensures compliance of IT systems and IT systems security staff with established IT security policy and guidance.

We also performed audit procedures over Contract and Grants Directorate (CGD) cloud procurement related activities. Within the Chief Operating Officer organization, the CGD is responsible for awarding and administering contracts and grants within the Library.

### III. Audit Results

We identified the following findings during the audit:

**Finding 1: The Library is unable to identify current-state cloud services in a reliable and effective manner.**

**Background**

The Library is increasingly adopting cloud computing services as it moves to a cloud-enabled hybrid hosting model.\(^{13}\) Depending on its business needs and data protection requirements, the Library will run applications strictly on-premises, solely in the cloud, or using a combination of both hosting types.

The OCIO stated that the Library uses the Archer Governance, Risk, and Compliance tool as its system of record for all IT systems currently in use. Archer maintains a list of authorization packages across the Library and includes risk summary, security, authorization, controls, and

\(^{13}\) NIST SP 800-145 defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”
boundary data for each package. A specific system’s record may include additional information regarding the system’s hosting environment in the system environment text box; this information may include the type of external hosting (e.g. SaaS, IaaS, and PaaS) and any system dependencies.

During our audit, Cotton & Company submitted multiple requests to obtain a copy of the Library’s inventory of cloud and SaaS systems. The information provided was not sufficient to enable us to ascertain a precise cloud inventory, and we were required to conduct follow-up meetings to reconcile the varying data the Library provided in response to our requests. In preparing its responses to our requests, the Library used exported data from Archer, which required Library personnel to perform additional research and make updates to ensure the completeness and accuracy of the information.

**Condition**
The Library does not maintain sufficient records of the current state of its cloud transition, including the number of systems it has transitioned to the cloud and the hosting provider responsible for each cloud implementation. Although information about each system’s hosting environment appears to be available in a text box within the Library’s system of record (i.e., Archer), the Library cannot filter or sort the data within Archer using that text box, which limits the Library’s ability to identify whether systems are cloud-based and the nature of the cloud service (i.e., IaaS, PaaS, or SaaS). The Library was ultimately able to provide an inventory identifying which of its systems are hosted in a cloud environment; however, to prepare this listing, Library personnel were required to manually research and interpret the data in Archer.

**Criteria**
Library of Congress Regulation (LCR) 5-210, *Enterprise Architecture (EA)*, states:

> Chief Architect. The Chief Architect is responsible for:
> Providing outcomes that meet the requirements and expressed priorities of the Library by:
> Collecting, validating, managing, and making available current state content driven by priorities from the Library to support IT governance and ITIM.

*NIST SP 800-145, The NIST Definition of Cloud Computing*, lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. It also lists three service models (software, platform, and infrastructure), and four deployment models (private, community, public, and hybrid) that together categorize ways to deliver cloud services.

*NIST Cybersecurity Framework (CSF) 1.1, Identify Core Function* states:

> The goal of the Identify function is to develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

CSF ID.Asset Management (AM)-2 includes “Software platforms and applications within the organization are inventoried” as a cybersecurity risk management activity.

CSF ID.AM-4 includes “External information systems are catalogued” as a cybersecurity risk management activity.

**Cause**
The Library does not include identification of a system’s hosting or service model as a standard attribute in its system inventory records within Archer. The Library explicitly referenced cloud services using the NIST definition of cloud (see Criteria section above) during a preliminary findings discussion on January 25, 2021; however, the OCIO has not explicitly defined cloud as an attribute within its system of record, instead opting to identify the specific nature of the hosting environment in the freeform narrative within the “System Environment” text box.

**Effect**
The Library’s inability to effectively generate an automated overview of its current-state cloud implementation and key service providers may hinder the OCIO from obtaining a current and comprehensive understanding of the status of the Library’s cloud implementation. As a result, the OCIO may not be able to effectively determine the magnitude of the risks posed by its external service providers and track the Library’s progress toward its planned future state. Further, not having readily available records of the current cloud environment may hinder the Library in responding to its business needs, including those related to risks and contract efficiencies.

**Recommendations**
We recommend that the Library:

1.1 Develop a process to ensure that it is able to identify its cloud-hosted systems, as defined by NIST SP 800-145 and CSF ID.AM-4.

1.2 Enhance and document its capabilities to ensure that the OCIO can automatically track and report on the Library’s current-state cloud systems at a level of granularity that can support EA and OCIO reporting of cloud migration metrics and track the Library’s progress toward a planned future state.
Finding 2: The Library does not have an actionable cloud strategy.

**Background**
In 2011, the Government released its Cloud First strategy, which asserted the potential benefits of cloud computing. In 2018, the Federal CIO developed and released Cloud Smart, a new strategy to accelerate the adoption of cloud computing by providing actionable information and recommendations. Cloud Smart attempts to focus on how agencies will use applications to meet their mission and what it will take to truly modernize their IT capabilities. According to the Cloud Smart federal strategy, government agencies should create cloud adoption strategies that are founded on an interdisciplinary approach that considers three key pillars: security, procurement, and workforce.

In March 2013, the Library OIG issued Report No. 2013-IT-101, *The Library has an Opportunity to be More Proactive in Adopting More Efficient Computing Technologies*. This report emphasized the need for the Library to “develop an enterprise-wide plan to evaluate possible use of cloud computing and achievable cost savings.”

In 2016, the Library purchased cloud IaaS units to support its operations. Subsequently, in 2018, the Library initiated the DCT project to migrate systems within its inventory from its primary, on-premises data center to a hybrid environment consisting of a combination of modernized data centers and cloud services.

**Condition**
In December 2020, the Library finalized its initial two-page cloud strategy, which included an overview of cloud technology, the OCIO’s principles regarding the cloud, and a discussion of the benefits of cloud technology. However, the strategy did not detail the core components of cloud adoption as described within Cloud Smart, including specific consideration of continuous data protection and awareness (security), SLA requirements (procurement), and a workforce development plan (workforce).

**Criteria**
The Library is a legislative-branch agency and is therefore not required to follow executive-branch directives, standards, and publications; however, the Library has chosen to selectively adopt directives and standards that it deems suitable. The Library Cloud Strategy, dated December 2020, states:

> The Library of Congress’ OCIO is adopting a “cloud smart” strategy to support the Library’s technical and business operations. Adopting Cloud Smart, the successor to the federal government’s Cloud First strategy, enables the Library to leverage cloud-based processing and storage solutions while recognizing that a cloud-only solution may not be the best or most economical solution for every need.

The Federal Cloud Smart Strategy states:
Taking a risk-based approach to securing cloud environments... requires that agencies place an emphasis on protections at the data layer in addition to the network and physical infrastructure layers, transitioning to a multi-layer defense strategy, otherwise known as defense-in-depth.

Generally, agencies’ cloud strategies and policies should also include a workforce development and planning component that tailors a transformation and training approach to that agency.

Standardizing cloud contract SLAs will provide more effective, efficient, and secure cloud procurement outcomes for agencies, while also enabling enhanced management of risk across the Federal enterprise through greater consistency and transparency in negotiations with commercial suppliers.

Although the Library has not formally adopted NIST SP 500-293, we consider the following to be a best practice for government entities:


> Organizations need to review, revise, and develop policy in the context of the global business and technical model enabled by cloud computing and other enabling technologies.

**Cause**

The Library is aware of the need for a cloud strategy and developed a strategy document during the course of our audit. However, the effort is still incomplete, as the Library’s cloud strategy is supported by a cloud implementation plan, which the Library has not yet finalized.

**Effect**

Without a detailed, documented cloud strategy that lays out cloud transition criteria and roadmaps, the Library may not be able to successfully execute commercial and functional plans that adequately consider performance factors such as security, procurement, and workforce. This may create security and compliance risks, increase both financial and administrative costs, and limit the benefits of adopting cloud technologies.

**Recommendations**

We recommend that the Library:

2.1 Update its cloud strategy and cloud implementation plan to fully align with the federal Cloud Smart strategy.

2.2 Disseminate the updated documents to management-level OCIO personnel and individuals within CGD to ensure organization-wide awareness and alignment.
Finding 3: The Library has not developed a system administration manual for the OGS.

**Background**
In 2016, the Library contracted with a cloud reseller to purchase cloud infrastructure units from both AWS and the OGS. The two cloud infrastructure platforms contributed to the Library’s strategy to adopt a hybrid hosting model that consists of a combination of the Library’s own data centers and purchased cloud units.

During our audit, Library personnel provided us with a Library implementation document entitled *System Administration Manual (SAM) for Office of the Chief Information Officer (OCIO) Amazon Services (OAS)*. The SAM includes detailed information addressing account creation, roles, and audit logging responsibilities within AWS.

As of December 2020, the Library had identified multiple applications for implementation on the OGS, including one application that the Library already released into production in December 2020.

**Condition**
The Library has not developed a SAM detailing its administration procedures for applications hosted on the OGS, including procedures for creating and monitoring user accounts, as well as audit logging responsibilities.

**Criteria**

*The LC IT Security Program provides a baseline of policies, procedures, standards, and guidelines for Library service units...*

*Specific implementation information can often be found in National Institute for Standards and Technology (NIST) publications, such as NIST Special Publication (SP) 800-53, Rev.4, Security and Privacy Controls for Federal Information Systems and Organizations.*

NIST SP 800-53, Control AC-1 states:

*The organization:*

a. *Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:*

   1. *An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and*
2. Procedures to facilitate the implementation of the access control policy and associated access controls

NIST SP 800-53, Control AU-1 states:

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Cause
Because the Library did not have a detailed cloud strategy and implementation plan in place that comprehensively describes steps to enforce Library security controls, the Library was not obligated to create a SAM to address access management and audit logging for the OGS. The Library is in the process of creating cloud implementation guidance that would formalize the obligations supporting an effective cloud administration program.

Effect
Without a documented operations manual for the OGS, the Library may not be able to successfully and consistently implement the user controls that are necessary for secure and effective use of the cloud service. This increases the risk to the confidentiality, integrity, and availability of Library data.

Recommendations
We recommend that the Library:

3.1 Develop account management and auditing procedures to support the implementation of the OGS.
3.2 Provide training to relevant personnel so they can execute the responsibilities documented within the new procedures.
3.3 Ensure the most current SAMs are available/accessible as needed to enable Library personnel to perform their duties.
Finding 4: The Library has not performed a gap analysis as part of its cloud strategy workforce development and planning component.

**Background**

In 2011 the Government released its Cloud First strategy, which asserted the potential benefits of cloud computing. In 2018, the Federal CIO developed and released Cloud Smart, a new strategy to accelerate the adoption of cloud computing by providing actionable information and recommendations. According to the Cloud Smart federal strategy, one of the three pillars for government agencies’ successful adoption of the cloud is the federal IT workforce. The strategy notes that government agencies should conduct their own enterprise-wide skill gap analyses and identify potential skill gaps.

In 2016, the Library purchased cloud infrastructure units\(^\text{14}\) to support its IaaS platforms from AWS and Google Cloud, and it continues to migrate systems in its inventory onto these platforms. The Library performed additional system and application migrations as part of its DCT project.

The OCIO provided cloud technology training on the new environment and the migration of applications to ITSO through Technical Exchange Meetings and CSP in-person training. In May 2019, the OCIO established the Cloud IPT, which provides IT engineering and IT security framework and vision for the implementation of the OCIO cloud environment. The Cloud IPT includes OCIO staff within ITSEC, Business Continuity & Disaster Recovery, ITSO, and ITDD. In June 2019, ITSO issued a data call to validate any cloud-related training courses that ITSO personnel had completed. In addition to its in-person training, the OCIO offered online training on a platform called *A Cloud Guru* to ensure staff had access to relevant IT training that supports individual development. Cloud IPT members are not required to participate in the online and in-person training; however, they are strongly encouraged to do so.

Additionally, the OCIO is working with the Human Capital Directorate to update existing OCIO IT position descriptions to include new technologies, including cloud computing skillsets.

**Condition**

The Library’s current cloud strategy does not include a workforce development and planning component that incorporates a tailored cloud-related training program.

Although the ITSO division of the Cloud IPT issued a data call to assess cloud-related training courses its personnel had taken, the OCIO has not performed an OCIO-wide gap assessment of cloud-related skills for all members of the Cloud IPT that:

- Maps current IT workforce resources to future skill and position requirements.
- Identifies both technical and non-technical skill and position gaps.

\(^{14}\) One unit of cloud computing capability is defined as a set quantity of instance hours, networking, and persistent storage.
Criteria
The Library is a legislative-branch agency and is therefore not required to follow executive-branch directives, standards, and publications. However, the Library has chosen to selectively adopt directives and standards that it deems suitable, including the federal government’s Cloud Smart strategy.

The Federal Cloud Smart Strategy, published June 24, 2019, Section IV. Workforce states:

As agencies adopt and migrate to cloud platforms, the impact that these migrations have on the Federal workforce needs to be examined. Specifically, agencies should identify potential skills gaps that emerge as a result of a transition to cloud-based services, and, where needed, equip their existing staff with additional skills and knowledge to keep up with the ever-expanding list of technology options available to procure and deploy.

Generally, agencies’ cloud strategies and policies should also include a workforce development and planning component that tailors a transformation and training approach to that agency. Additionally, in the event that an impact to the existing workforce has been identified, this approach should include a cross-walk of new skills and occupational categories with legacy occupational categories to foster clarity and ease of transition.

Successful adoption of cloud solutions requires a workforce that understands how to manage the complexities of a migration as well as how to support a cloud environment once fully deployed. Agency CIOs, Chief Human Capital Officers (CHCOs), and Senior Agency Official for Privacy (SAOPs) should collaboratively conduct a skills gap analysis that maps current IT workforce resources to future skill and position requirements. Agencies are strongly encouraged to leverage industry projections to help predict future workforce skill and position requirements, especially for IT roles.

While Federal agencies should continue to comply with the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework to help standardize government-wide cybersecurity workforce gap assessments, they are encouraged to conduct their own enterprise-wide skills gap analysis to ensure inclusion of all current and future IT skills and positions specific to their workforce requirements.

Current employees may lack the skills or knowledge required to facilitate a cloud migration or to maintain the environment once migrated. Therefore, agencies must conduct their skills gap analysis to identify both technical and non-technical skill and position gaps so that leadership may determine which deficiencies are the most significant and/or represent a critical mission need.
Cause
The Library’s cloud strategy is incomplete and does not include a workforce development and planning component. As a result, the OCIO has not conducted a gap assessment of cloud-related skills for all members of the Cloud IPT. Such an analysis would enable the OCIO to identify future technical and non-technical positions that it may need to fill, as well as existing positions that it may not require in the future.

Effect
Without a gap assessment of technical and non-technical skills for all members of the Cloud IPT, the Library will be unable to ensure that Cloud IPT personnel are equipped to manage cloud-related security, privacy, and procurement issues. Such skill gaps could cause the Library to procure unsuitable cloud solutions or cause delays in identifying and addressing issues, which may result in an increase in threats to the confidentiality, integrity, and availability of Library data.

Recommendations
We recommend that the Library:

4.1 Update the Library’s cloud strategy to include a workforce development and planning component.

4.2 Perform an OCIO-wide skills gap assessment in support of the Library cloud strategy.

4.3 Based on the results of the OCIO-wide skills gap assessment, implement any necessary corrective actions.

Finding 5: The Library’s cloud contracts lack detailed service-level information regarding data preservation and migration.

Background
In 2016, the Librarian of Congress directed the Library to move from using a decentralized technology governance model to centrally coordinating all technology activities through the OCIO in an effort to modernize the Library’s IT infrastructure. This included requiring all cloud procurements to undergo OCIO review and approval.

In 2016, the Library procured a multiple-award IDIQ contract for cloud services from AWS and OGS (Contract No. LCNLS16C0070). The IDIQ contract provides detailed descriptions of cloud service procurements and references an SLA spreadsheet that lists metrics for availability, performance, and communication attributes and how the Library measures these attributes. As of January 5, 2021, the Library had multiple applications running on AWS and OGS.

Cloud policies and procedures provide guidelines under which organizations are willing to operate in the cloud. Organizations implement these policies and procedures to ensure the integrity and privacy of their information. Cloud policies and procedures should include a statement regarding what data the organization is willing to maintain in the cloud, as well as information regarding how the organization selects CSPs and expected performance levels in key areas such as response times, incident reporting, and security.
**Condition**
The Library has drafted procurement policies regarding cloud computing services and IT products and services; however, it has not finalized these policies. We reviewed two Library contracts and the associated SLA requirements and noted that both contracts were missing language describing how the CSP will transition Library data back to the Library in the event of contract exit/termination.

**Criteria**

NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing, Section 5. Public Cloud Outsourcing*, states:

5.2 Preliminary Activities (p. 53)

*Establishing an exit strategy is an important part of the planning process and should be factored into the requirements analysis. It also relates to the organization’s contingency and continuity planning activities. The exit strategy should cover a normal termination, such as that at expiration of the service agreement, and also an unexpected termination, such as that due to service provider bankruptcy or poor performance. The ability to export all of the organization’s data in a usable format through a secure, reliable, and efficient means, and in a timely manner, is a vital aspect of an exit strategy. Other aspects include addressing application dependencies on proprietary programming interfaces, system calls, and database technologies, as well as the recovery of useful metadata that may have accumulated within the cloud environment.*

5.4 Concluding Activities (p. 60-61)

At the end of a project, when transitioning to another cloud provider, or for other reasons, the organization can decide to enter the final stage of outsourcing and terminate use of the public cloud services and close out the contract. Organizations should perform the following activities preceding the termination of an outsourcing contract:

- **Recover Organizational Resources and Data.** The organization should ensure that any resources of the organization made available to the cloud provider under the terms of the service agreement, such as software, equipment, documentation, are returned or recovered in a usable form, as well as any data, programs, scripts, etc. owned by the organization and held by the cloud provider. If the terms of service require the cloud provider to purge data, programs, backup copies, and other cloud consumer content from its environment, evidence such as system reports or logs should be obtained and verified to ensure that the information has been properly
expunged. These activities should be carried out in compliance with an agency’s records management policy.

Having an exit strategy established early in the planning stage, and periodically reviewing and updating its contents, can minimize the problems encountered with the termination of a service agreement, and the effort required to transition applications to another service provider or return them to the organization’s data center.

Although the Library has not formally adopted NIST SP 800-146, we consider the following to be a cloud-related best practice for government entities:

NIST SP 800-146, Cloud Computing Synopsis and Recommendations, states:

Section 3. Typical Commercial Terms of Service, 3.1 Promises (p. 16):

Generally, providers make four key promises to consumers:

- **Data Preservation.** If a consumer’s access to cloud services is terminated “for cause,” i.e., because the consumer has violated the clouds’ acceptable use policies or for nonpayment, most providers state that they have no obligation to preserve any consumer data remaining in cloud storage. Further, after a consumer voluntarily stops using a cloud, providers generally state that they will not intentionally erase the consumer’s data for a period of 30 days. Some providers preserve only a snapshot of consumer data, or recommend that consumers: (1) backup their data outside that provider’s cloud inside another provider’s cloud, or (2) back it up locally.

Section 9. Recommendations, 9.1 Management (p. 66):

- **Migrating Data to and from Clouds.** Consumers should identify the specific resources that are suitable for migrating data into and out of clouds. Resources could be services such as: (1) email, (2) data repositories such as shared documents, or (3) systems that run in virtualized environments. Consumers should develop a plan for both migrating the data to and from the cloud, and for interacting with the data once it is resident in the cloud. Consumers should plan also for an eventual termination of a provider’s service during the procurement phase of the contract, and should clarify how assets are to be returned to consumers. Consumers should also plan for migration between clouds.

Although the Library has not formally adopted GAO report GAO-16-325, Cloud Computing – Agencies Need to Incorporate Key Practices to Ensure Effective Performance, we advise that the Library consider this report, which contains best practices for government procurement of cloud services. Specifically:

GAO-16-325 identified 10 key practices that agencies should include in an SLA, such as identifying the roles and responsibilities of major stakeholders, defining performance
objectives, and specifying security metrics. These key practices, if properly implemented, can help agencies ensure services are performed effectively, efficiently, and securely.

GAO-16-325, Key Practice 4, states:

Specify how and when the agency has access to its own data and networks. This includes how data and networks are to be managed and maintained throughout the duration of the SLA and transitioned back to the agency in case of exit/termination of service.

**Cause**
The Library had not finalized its directives for the procurement of cloud services. The Library stated that it has drafted two documents:

1. LC Directive 5-110.4: Procurement of Cloud Computing Services
2. LC Directive 5-110.2: Procurement of Information Technology Products and Services

However, the Library did not prioritize the creation, approval, and publication of these cloud procurement policies and procedures before the actual execution of cloud procurements.

**Effect**
Without including detailed information and criteria in its cloud contracts and SLA requirements to clarify how the CSP will transition Library data back to the Library in the event of exit/termination, the Library may not be able to successfully preserve its data. This increases the risk to the security and preservation of Library data within the cloud infrastructure.

**Recommendations**
We recommend that the Library:

5.1 Finalize and implement the procurement policies for cloud computing services and IT products and services.

5.2 Ensure that the procurement policies take into consideration the guidelines and recommendations for cloud procurement contained in NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, and NIST SP 800-146, *Cloud Computing Synopsis and Recommendations*.

5.3 Ensure that SSPs or other system-specific documents for current cloud-based systems address data preservation and the migration of data to and from the cloud, as outlined in NIST SP 800-146, *Cloud Computing Synopsis and Recommendations*, sections 3 and 9, respectively.
Finding 6: The Library does not consistently apply the risk management framework to its cloud applications.

Background
The Library’s OCIO has established Security A&A Guidance, which contains a standard approach for conducting A&A tasks for information systems. This guidance is based on NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, and covers all Library systems (including systems that process data on behalf of the Library) to ensure that the Library and its service providers select, implement, assess, and monitor appropriate security and privacy controls on an ongoing basis.

The RMF provides a structured approach that enhances the system development life cycle (SDLC) by providing information security and risk management activities. The Library uses this framework to manage the security posture of information systems through various tasks that support the secure implementation of controls and ongoing management of risks.

The seven steps of RMF are as follows:15

1. **Prepare** to execute the RMF from an organization and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
2. **Categorize** the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.
3. **Select** an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.
4. **Implement** the controls and describe how the controls are employed within the system and its environment of operation.
5. **Assess** the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
6. **Authorize** the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.
7. **Monitor** the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

The Library’s A&A Guidance states that the Library must conduct this process for all new information systems, and these systems must continue to meet the security requirements defined in the Library’s SSPs. The RMF states that previous authorization decisions can be rescinded when there is a violation of federal or organizational policies, directives, regulations, standards, or guidance; or a violation of the terms and conditions of the authorization. Failure to maintain an effective continuous monitoring program may be grounds for rescinding an authorization decision.

We selected a sample of eight externally hosted systems in use at the Library and inspected related documentation—including ATO memoranda, SSPs, Security Assessment Reports (SARs), continuous monitoring plans, and POA&Ms—to determine whether the service providers followed the RMF activities detailed in the A&A Guidance. The eight systems included:

<table>
<thead>
<tr>
<th>System</th>
<th>Library System Number</th>
<th>Hosted On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Analytics</td>
<td>LIB-235</td>
<td>Adobe – Adobe Analytics</td>
</tr>
<tr>
<td>Braille Certification Learning Management System</td>
<td>LIB-371</td>
<td>Gyrus</td>
</tr>
<tr>
<td>iCohere Collaboration Platform</td>
<td>LIB-145</td>
<td>Cogeco-Peer 1</td>
</tr>
<tr>
<td>Legislative Branch Financial Management System (LBFS) Momentum Cloud</td>
<td>LIB-105</td>
<td>CGI Federal – CGI IaaS cloud</td>
</tr>
<tr>
<td>LC Human Capital Management System</td>
<td>LIB-408</td>
<td>AWS GovCloud</td>
</tr>
<tr>
<td>LOC Learning Management System</td>
<td>LIB-387</td>
<td>Skillsoft – Private Cloud</td>
</tr>
<tr>
<td>Qualys*</td>
<td>LIB-241</td>
<td>Qualys Cloud Platform</td>
</tr>
<tr>
<td>ServiceNow Platform</td>
<td>LIB-336</td>
<td>ServiceNow – Government Community Cloud</td>
</tr>
</tbody>
</table>

* Qualys is part of a Security Tool Suite (STS) major system, in which the Library combines multiple systems into a single authorization package and security plan.

**Condition**

The Library has not consistently implemented the Select, Implement, Assess, and Monitor steps from the RMF framework in accordance with its policies and procedures. Specifically, for a selection of eight externally hosted systems, we noted the following:

1. **Select.** The Library has significantly reduced the control baseline for its LIEH systems from the established NIST baselines without documenting either its rationale for doing so or its acceptance of the associated risk. Specifically, we noted that the Library classified 56 total controls as LIEH security controls, while NIST SP 800-53, Revision 4 contains a baseline of 115 low-impact controls. The Library has defined criteria in place for classifying applications as LIEH (e.g., FIPS categorization of “Low,” no sensitive data or personally identifiable information [PII], externally hosted); however, the Library has not documented its rationale for excluding individual controls from the LIEH baseline. The Library had applied this reduced baseline to two systems in our sample: Adobe Analytics and the iCohere Collaboration Platform.

---

16 NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations, Page 146.
2. **Implement.** The Library’s SSPs did not consistently contain detailed implementation information describing why the Library had designated some system/application controls as “Inherited” or “Not Applicable.” Specifically, for five of the eight externally hosted systems in our sample, we noted that the SSP contained controls listed as “Inherited” or “Not Applicable” but did not include detailed information regarding the system from which the control was inherited or why the control was not applicable. Below, we provide information regarding the number of insufficiently detailed control descriptions for each sampled system.

- Momentum Cloud: 18 “Inherited” controls
- Adobe Analytics: 3 “Inherited” controls, 99 “Not Applicable” controls
- LOC Learning Management System: 2 “Not Applicable” controls
- Braille Certification Learning Management System: 7 “Not Applicable” controls
- STS: 18 “Inherited” controls, 16 “Not Applicable” controls
  - Note: A sub-system of STS, Qualys, was decommissioned prior to the conclusion of the audit reporting period.

3. **Assess.** The Library did not consistently remediate system risks within its Library-defined timeframes. Specifically, we noted overdue POA&Ms for four of the eight externally hosted systems in our sample. In total, we identified 11 overdue POA&Ms in the report generated on January 14, 2021, with estimated completion dates ranging from August 2020 through November 2020. The Library closed all 11 identified POA&Ms prior to the conclusion of the audit reporting period.

4. **Monitor.** The Library did not consistently document, implement, and execute a continuous monitoring strategy for its cloud systems, as follows:

- The Library’s continuous monitoring plan for the Adobe Analytics system omitted NIST SP 800-53 controls that were applicable to the system, such as AC-02 and CM-01.
- The Library did not consistently assess NIST SP 800-53 control AC-07 for the Momentum system in accordance with the organization-defined frequency in the system’s continuous monitoring plan. The Library defined this control’s assessment frequency as 90 days; however, we reviewed the SAR generated on January 14, 2021, and noted that it stated that the Library last assessed this control on June 17, 2020 (i.e., 211 days prior). **Note:** As of November 2021, AC-07’s assessment frequency is 1 year and was last assessed in April 2021. Therefore, this item is considered remediated.
- The Library tailored its continuous monitoring plan for the Learning Management System based on a “Low” FIPS 199 security categorization; however, the Library had categorized the Learning Management System as “Moderate.”
Criteria

The LC IT Security Program provides a baseline of policies, procedures, standards, and guidelines for Library service units... Specific implementation information can often be found in National Institute for Standards and Technology (NIST) publications, such as NIST Special Publication (SP) 800-53, Rev.4, Security and Privacy Controls for Federal Information Systems and Organizations... and NIST Federal Information Processing Standards (FIPS) 200 Minimum Security Requirements for Federal Information and Information Systems.

NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, page 13 states:

An agency has the flexibility to tailor the security control baseline in accordance with the terms and conditions set forth in the standard. Tailoring activities include: (i) the application of scoping guidance; (ii) the specification of compensating controls; and (iii) the specification of agency-defined parameters in the security controls, where allowed. The system security plan should document all tailoring activities.

System security plans should clearly identify which security controls employed scoping guidance and include a description of the type of considerations that were made.

NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, page 31 states:

Tailoring decisions regarding security controls should be defensible based on mission/business needs and accompanied by explicit risk-based determinations. Tailoring decisions, including the specific rationale for those decisions, are documented in the security plans for organizational information systems. Every security control from the applicable security control baseline is accounted for either by the organization (e.g., common control provider) or by the information system owner. If certain security controls are tailored out, then the associated rationale is recorded in security plans (or references/pointers to other relevant documentation are provided) for the information systems and approved.


All high risk POA&Ms must be mitigated within 30 days (3.15.m-10); All moderate risk POA&Ms must be mitigated within six months (3.15.n-1); and all low risk POA&Ms must be mitigated within one year (3.15.o-1).
Library of Congress Security Assessment and Authorization (A&A) Guidance, dated August 24, 2020, Section 5.3.7 states:

…the ISSO is responsible for scheduling an assessment of information system specific controls in accordance with Library policy by an independent assessor.

A&A Guidance, Section 3.3 states:

An information system-specific information security continuous monitoring (ISCM) plan should be established in the initiation phase of the SDLC and Step 3 of the RMF. The ISCM plan requires the ISBO, ISSO, and/or Common Control Provider to determine the security controls to be monitored and frequency in which to assess the selected controls.

FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, states:

For low-impact information systems, organizations must, as a minimum, employ appropriately tailored security controls from the low baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the low baseline are satisfied.

Cause
The OCIO stated that the continuous monitoring plans were non-compliant due to human error, and that it would update the plans by the end of Q2 FY 2021. Note: As of November 2021, the Adobe Analytics plan was updated to include the missing controls. The Library continues to work on an updated CM plan for the Learning Management System, with a scheduled completion date of Q1 2022. The OCIO further noted that the missing implementation details in some SSPs were the result of a technical error in its A&A tool that prevented implementation statements for inherited controls from appearing in the associated sections for inheriting systems. With regard to the LIEH baselines, the OCIO noted that the Library identified the controls based on cost considerations, without documenting a risk-based approach for the tailoring-out of individual controls. Lastly, the OCIO stated that it had understood that the Library was able to tailor controls based on business needs, including designating controls within the system baseline as not applicable. However, the OCIO did not tailor the Library’s controls based on mission/business needs, accompanied by explicit risk-based determinations.

Effect
Without performing effective risk management activities when selecting, implementing, assessing, and monitoring controls, the Library has reduced assurance over the security posture of its information systems. This may manifest as a weakening of authorization decisions and increase the risk to internally and externally hosted Library data. Without explicitly documented risk-based reasons for excluding controls, the Library will find it difficult to re-assess control decisions based on technology or environment changes. Further, without readily available information regarding control inheritance, an assessor or authorizer may have an incomplete
understanding of the system’s control environment. Most notably, if a system is inheriting deficient controls, it will not be immediately clear to key personnel.

**Recommendations**

We recommend that the Library:

6.1 Evaluate the alignment of its established LIEH control baselines with NIST control baselines and document and justify any deviations (i.e., tailoring), with a rationale or an acceptance of the related risk.

6.2 Refine its POA&M management process to ensure that it reviews reports of overdue POA&Ms in a timely manner and to require justification for any delays or extensions for POA&Ms.

6.3 Review cloud system continuous monitoring plans to ensure that the control scopes and assessment frequencies are commensurate with the systems’ control baselines. Monitor performance of control assessments accordingly.

6.4 Review the SSPs in Archer to determine the scope of the technical error related to inherited controls. Coordinate with the vendor to identify and implement a solution.

6.5 Conduct an analysis to determine if SSPs for other systems have insufficient tailoring or inheritance statements and create a plan to address any identified gaps.

**Finding 7: The Library does not consistently implement its cost estimation and monitoring requirements for cloud migrations.**

**Background**

The Library is increasingly adopting cloud computing services as it moves to a hybrid hosting model. Depending on its business needs and data protection requirements, the Library will run the applications strictly on-premises, solely in the cloud, or using a combination of both hosting types.

Investments in federal IT have the potential to make agencies more efficient in fulfilling their missions by reducing costs and improving operational efficiencies. GAO reports that each year, the federal government invests approximately $90 billion in IT, with about 75 percent of this amount reportedly spent on operating and maintaining existing systems. However, as GAO has previously testified, federal IT investments have frequently failed or incurred cost overruns and schedule slippages while contributing little to mission-related outcomes.17

In 2013, the OIG survey report entitled *The Library has an Opportunity to be More Proactive in Adopting More Efficient Computing Technologies* recommended that “Information Technology Services (ITS, [currently OCIO]) collect the data to make informed IT assessments of its infrastructure and report to the Deputy Librarian its progress on adopting the

---

recommendations from the consultants’ report.” This report addressed the opportunities for the Library to gain cost efficiencies through the use of virtual machines (VMs) and cloud-based services, specifically including potential reductions in energy expenses. The report advised ITS to capture current cost levels.

The Library captures actual costs for all payments against contract orders and invoices paid in the LBFMS Momentum Cloud. The Treasury Invoice Processing Platform (IPP) system also retains records of invoices and payments.

In 2021, Cotton & Company inquired of Library management to determine whether the Library had developed a TCO for each application in both a cloud-hosted and Library-hosted environment. Such a comparison is necessary to quantify the Library’s determination as to whether a cloud-based or self-hosted model is a more cost-effective choice to host particular applications. However, the Library was unable to provide Library-specific TCO documentation.

Additionally, Cotton & Company selected a sample of eight of the Library’s current externally hosted SaaS implementations18 and performed testing to determine whether: 1) the Library followed its security policies for these implementations, and 2) the Library followed its procurement process when selecting and procuring externally hosted solutions. Our testing included inspecting cost projection and ongoing cost-tracking documentation.

**Condition**

The Library did not perform an independent TCO analysis to compare the estimated cost of transitioning 10 of its applications to the cloud to the cost of continuing to host the applications on-premises, based on the cost the Library incurred to host the applications prior to transitioning them to the cloud.

Additionally, the Library does not have mechanisms in place to track cost savings and cost avoidances for its cloud implementations that have on-premises hosting alternatives. Specifically, the Library is not actively tracking cost savings and avoidances for the following SaaS implementations:

- LBFMS Momentum Cloud
- LC Human Capital Management System

**Criteria**

Library of Congress Regulation 5-130, *Information Technology Investment Management, Section B. Investment Monitoring Phase*, states:

18 The eight SaaS implementations included in our sample do not overlap with the applications the Library identified as having transitioned to the cloud. Although the SaaS implementations are externally hosted, they do not fit the Library’s definition of “cloud,” which reflects the definition included in NIST SP 800-145.
1. **Service units are responsible for:**
   
a. Planning and monitoring implementation of their IT investments in collaboration with OCIO, and completing and submitting quarterly and annual IT investment reports with documentation supported reported status, if necessary.

   ...

3. The ITSC is responsible for conducting quarterly and annual performance reviews of the IT Investment Portfolio, and presenting findings to the EC and the Librarian for review. The ITSC will ensure that all reviews of the IT Investment Portfolio include, but are not limited to, the service unit’s analysis of the following information:

   b. Variances between the anticipated cost of the IT investment and the projected actual cost of the IT investment to date.

Library of Congress Directive 5-130.1, *IT Investment Management*, Section 2.2 states:

*IT Investments are designed to provide the following information:*

...  
- **Estimate of costs and benefits (quantitative and/or qualitative)**  
...

- **Measurements of success.**


- **Identify standard cost modeling to be used, and deliver comprehensive cost estimates**
- **Identify any historical trends driving the forecasts**


*Quarterly reporting is based on the service unit investment owner’s analysis of variances from the proposed schedule of milestones, costs, and risks in the investment proposal during that quarter, and projection of possible variances in the next quarter.*


*Management tracks major entity achievements and compares these to the plans, goals, and objectives set by the entity.*
GAO-19-58, *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked* page 47 states:

> An important aspect to the success of key OMB cloud initiatives, like Cloud Smart and the associated drive for greater agency adoption of cloud services, will be the ability for key stakeholders to access complete information on the savings that agencies are achieving under these efforts.

The following represents optional criteria and guidance for the Library.

The Office of Management and Budget (OMB) memorandum M-19-19, *Update to Data Center Optimization Initiative (DCOI)* states:

> As agencies gain greater IT spending transparency through Capital Planning and Investment Control (CPIC) and Technology Business Management (TBM), the resulting data will support and enable their ability to rationalize their application portfolios to find greater return on investment, in alignment with the 2018 Federal Cloud Computing Strategy (“Cloud Smart”)... Agencies should consider carefully the Total Cost of Ownership (TCO) when making such determinations, not just licensing and hosting costs.

**Cause**

The Library did not subject its cloud migration activities to its cost-benefit estimation policies. In addition, it did not subject its cloud implementations to its policies for reporting cost variances in its IT investments. We were also informed that the Library may be contractually required to obtain cloud hosting for its SaaS applications, despite the availability of on-premises hosting.

**Effect**

Without adequate cost comparisons and cost-tracking mechanisms for its cloud implementations, the Library may not be able to accurately quantify the costs or benefits of transitioning to and using cloud services. This may prevent the Library from maximizing the benefits from its investments and potentially cause it to overspend on cloud hosting in situations where self-hosted options are more economical. Further, by not monitoring its costs, the Library may miss opportunities to keep original business cases on track for benefit realization (monitoring).

**Recommendations**

We recommend that the Library:

7.1 Establish Library-specific cost models for computing, storage, and network services that the Library can use in performing TCO comparisons and monitoring.

7.2 Ensure the Library’s cloud strategy or implementation plan clearly identifies the need to document and present TCO comparisons when making hosting determinations.
7.3 Plan and monitor the implementation of its cloud IT investments and complete and submit quarterly and annual IT investment reports with documentation supporting the reported status, if necessary.
APPENDIX A – OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of the audit was to assess the effectiveness of the Library’s cloud strategy, governance, technical planning, and procedures. In carrying out this objective, we performed the following steps:

- Determining whether the Library has implemented corrective actions to address prior Library or GAO cloud audit findings.
- Determining whether the Library has prioritized and completed an enterprise-wide cloud strategy in alignment with federal guidance.
- Determining whether the Library’s cloud inventory is accurate, formalized, and managed using automated methods.
- Determining the extent to which the Library has effectively implemented federal standards and requirements, as well as best practices for its existing cloud implementations. This includes:
  - Reviewing Library policies, procedures, and technical guides; NIST publications; and other federal guidance and best practices for determining cloud suitability.
  - Selecting a sample of the existing cloud implementations and identifying and interviewing the personnel responsible for each sampled cloud implementation.
  - Evaluating the cloud suitability process and determining whether it incorporates Library and federal requirements, guidance, and best practices (application rationalization).
  - Evaluating existing cloud contracts for adequate SLAs and security controls.
  - Obtaining and reviewing cost-benefit analyses completed for a sample of in-progress or recently completed cloud considerations to determine any potential cost savings for moving to the cloud. In addition, assess the methodology by which the Library determined the current and future TCO.
  - Evaluating the cloud procurement approval and authorization process.
  - Reviewing and identifying Library policies, procedures, and manuals; NIST publications; and other federal guidance regarding organization cloud approval and procurement. Include activities related to Information Technology Investment Management (ITIM) and Technology Business Management (TBM), in addition to Enterprise Architecture/Service Catalog Requirements.
  - Interviewing Contracts Directorate, Directorate Leadership (Executive Committee), OCIO, Enterprise Services, and Enterprise Architecture personnel.
  - Evaluating the cloud approval and procurement processes and assessing them against relevant guidance and best practices.
  - Obtaining and reviewing actual cost savings for a sample of current cost implementations.
We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted the audit from September 2020 through January 2022.

We assessed internal controls that we deemed to be significant to the audit objective. Specifically, we assessed 10 out of the 17 principles associated within the five components of internal control defined in GAO’s Standards for Internal Control in the Federal Government (September 2014) (Green Book).

The table below summarizes the principles we assessed:

<table>
<thead>
<tr>
<th>Control Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 2: Exercise Oversight Responsibility</td>
</tr>
<tr>
<td>Principle 3: Establish Structure, Responsibility, and Authority</td>
</tr>
<tr>
<td>Principle 4: Demonstrate Commitment to Competence</td>
</tr>
<tr>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Principle 6: Define Objectives and Risk Tolerances</td>
</tr>
<tr>
<td>Principle 7: Identify, Analyze, and Respond to Risks</td>
</tr>
<tr>
<td>Control Activities</td>
</tr>
<tr>
<td>Principle 12: Implement Control Activities</td>
</tr>
<tr>
<td>Information and Communication</td>
</tr>
<tr>
<td>Principle 13: Use Quality Information</td>
</tr>
<tr>
<td>Principle 15: Communicate Externally</td>
</tr>
<tr>
<td>Monitoring</td>
</tr>
<tr>
<td>Principle 16: Perform Monitoring Activities</td>
</tr>
<tr>
<td>Principle 17: Evaluate Issues and RemEDIATE Deficiencies</td>
</tr>
</tbody>
</table>

We assessed the design, implementation, and operating effectiveness of internal controls and identified deficiencies that we believe could affect the Library’s cloud processes.

To address the audit objectives, we:

- Inspected the Library’s cloud strategy.
- Inspected the Library’s regulations and directives around ITIM.
- Inspected the Library’s regulations and directives around procuring cloud services.
- Inspected the Library’s policies and procedures related to authorizing and securing cloud services.
- Inspected the Library’s charter for its cloud workforce development.
- Inspected program documents from the FedRAMP framework.
Inquired of Library personnel and inspected prior-year audit reports on the Library OIG website regarding cloud-relevant findings.

Inquired of Library personnel regarding the following topics:
  - The process for determining the need for new applications and the appropriateness of a cloud implementation.
  - The cloud procurement process.
  - The Library’s efforts to draft a cloud strategy and associated policies and procedures.
  - The Library’s inventory processes to track cloud applications.
  - Ongoing efforts to monitor the costs and performance of the Library’s cloud program.

Inspected the following documents based on a sample of Library cloud implementations:
  - Application rationalization.
  - Procurement documents, including contracts and SLAs.
  - A&A documents, including SARs, ATOs, and SSPs.
  - Cost estimation, including TCO.
  - Cost tracking.
APPENDIX B – MANAGEMENT RESPONSE

We provided Library management with our draft version of this report, and they provided the following responses. We have not audited management’s responses and therefore do not express an opinion on them.
MEMORANDUM

DATE: December 10, 2021

TO: Kim Byrd, Acting Inspector General

FROM: J. Mark Sweeney, Principal Deputy Librarian of Congress

SUBJECT: Management Response to OIG report 2020-IT-103, Cloud Service Provider Governance

Thank you for providing the draft report on the Library of Congress’ activities to develop a more robust hybrid computing environment, which has included increased procurement of cloud services. The Library generally agrees with the recommendations. As we move from the initial rationalization and migration under the hybrid Data Center Transformation project to enrich our cloud first strategy, the information will assist with the evolution of the Library’s policies and development of more comprehensive documentation of the planning and risk assessment being conducted for IT systems.

The Office of the Chief Information Officer (OCIO) has been working diligently to transition the Library’s IT infrastructure to a more modern and efficient computing model. OCIO will continue to collaborate with service units and divisions across the Library to achieve these goals, such as by coordinating with the Financial Services Directorate to develop cost models and data that inform the total cost of ownership and estimates for procurements of cloud services, with the Contracts and Grants Directorate to negotiate applicable terms to safeguard Library data within cloud environments, and with the Human Capital Directorate to perform an OCIO-wide cloud skills gap assessment and implement any necessary corrective actions based on the results of the assessment in support of the Library cloud strategy.

The attached spreadsheet provides responses and target dates for addressing each of the recommendations as related to cloud service provider governance.

cc: Judith Conklin, Chief Information Officer
Edward Jablonski, Chief Operating Officer
Ronald Backes, Director, Contracts and Grants
Mary Klutts, Chief Financial Officer
Elizabeth Pugh, General Counsel
John Rutledge, Deputy CIO
Elizabeth Scheffler, Acting Comptroller
<table>
<thead>
<tr>
<th>Rec#</th>
<th>Recommendation</th>
<th>Resp. Office</th>
<th>Comments</th>
<th>Target completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Develop a process to ensure that it is able to identify its cloud-hosted</td>
<td>OCIO</td>
<td>The Library will develop a process to ensure that it is able to identify its cloud-hosted systems, as defined by NIST 800-145 and CSF ID.AM-4.</td>
<td>Q4 FY2022</td>
</tr>
<tr>
<td>1.2</td>
<td>Enhance and document its capabilities to ensure that the OCIO can automatically</td>
<td>OCIO</td>
<td>The Library will modify Archer's configurations that will allow OCIO to track and report on each system's hosting environment or service model, to include current-state cloud systems. This will support OCIO's reporting of cloud reporting metrics.</td>
<td>Q3 FY2022</td>
</tr>
<tr>
<td>2.1</td>
<td>Update its cloud strategy and cloud implementation plan to fully align with the</td>
<td>OCIO</td>
<td>The Library will update its cloud strategy and cloud implementation plan to fully align with the federal Cloud Smart strategy.</td>
<td>Q4 FY2022</td>
</tr>
<tr>
<td>2.2</td>
<td>Disseminate the updated documents to management-level OCIO personnel and</td>
<td>OCIO in</td>
<td>The Library will disseminate the updated documents to management-level OCIO personnel and individuals within CGD to ensure organization-wide awareness and alignment.</td>
<td>Q4 FY2022</td>
</tr>
<tr>
<td></td>
<td>individuals within CGD to ensure organization-wide awareness and alignment.</td>
<td>collaboration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Develop account management and auditing procedures to support the implementation of the OCIO Google Services.</td>
<td>OCIO</td>
<td>The Library will develop account management and auditing procedures to support the implementation of the OCIO Google Services (OGS).</td>
<td>Q4 FY2022</td>
</tr>
<tr>
<td>3.2</td>
<td>Provide training to relevant personnel so they can execute the responsibilities documented within the new procedures.</td>
<td>OCIO</td>
<td>The Library will provide training to relevant personnel so they can execute the responsibilities documented within the new procedures.</td>
<td>Q4 FY2022</td>
</tr>
<tr>
<td>3.3</td>
<td>Ensure the most current SAMs are available/accessible as needed to enable Library personnel to perform their duties.</td>
<td>OCIO</td>
<td>The Library will ensure the most current SAM for LIB-259 OGS is available/accessible as needed to enable Library personnel to perform their duties.</td>
<td>Q1 FY2022</td>
</tr>
<tr>
<td>4.1</td>
<td>Update the Library's cloud strategy to include a workforce development and planning component.</td>
<td>OCIO</td>
<td>The Library will update the Library's cloud strategy to include a workforce development and planning component.</td>
<td>Q4 FY2022</td>
</tr>
<tr>
<td>4.2</td>
<td>Perform an enterprise-wide skills gap assessment in support of the Library cloud strategy.</td>
<td>OCIO in</td>
<td>The Library will perform an OCIO-wide cloud skills gap assessment in support of the Library cloud strategy.</td>
<td>Q4 FY2023</td>
</tr>
<tr>
<td></td>
<td>collaboration with HCD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rec#</td>
<td>Recommendation</td>
<td>Resp. Office</td>
<td>Comments</td>
<td>Target completion</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>4.3</td>
<td>Based on the results of the enterprise-wide skills gap assessment, implement any necessary corrective actions.</td>
<td>OCIO in collaboration with HCD</td>
<td>The Library will implement any necessary corrective actions based on the results of the OCIO-wide cloud skills gap assessment.</td>
<td>Q1 FY2024</td>
</tr>
<tr>
<td>5.1</td>
<td>Finalize and implement the procurement policies for cloud computing services and IT products and services.</td>
<td>OCIO and CGD</td>
<td>The Library will finalize and implement the procurement policies for cloud computing services and IT products and services.</td>
<td>Q4 FY2022</td>
</tr>
<tr>
<td>5.2</td>
<td>Ensure that the procurement policies take into consideration the guidelines and recommendations for cloud procurement contained in NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, and NIST SP 800-146, Cloud Computing Synopsis and Recommendations.</td>
<td>OCIO and CGD</td>
<td>The Library will ensure that the procurement policies take into consideration applicable guidelines and recommendations for cloud procurement.</td>
<td>Q4 FY2022</td>
</tr>
<tr>
<td>5.3</td>
<td>Ensure that SSPs or other system-specific documents for current cloud-based systems address data preservation and the migration of data to and from the cloud, as outlined in NIST SP 800-146, Cloud Computing Synopsis and Recommendations, sections 3 and 9, respectively.</td>
<td>OCIO</td>
<td>The Library will ensure that the SSPs for cloud hosted systems address data preservation and data migration to and from the cloud.</td>
<td>Q3 FY2022</td>
</tr>
<tr>
<td>6.1</td>
<td>Evaluate the alignment of its established LIEH control baselines with NIST control baselines and document and justify any deviations (i.e., tailoring), with a rationale or an acceptance of the related risk.</td>
<td>OCIO</td>
<td>The Library will review the LIEH process to ensure that any deviations from the NIST Low control baseline are documented and approved.</td>
<td>Q2 FY2022</td>
</tr>
<tr>
<td>6.2</td>
<td>Refine its POA&amp;M management process to ensure that it reviews reports of overdue POA&amp;Ms in a timely manner and to require justification for any delays or extensions for POA&amp;Ms.</td>
<td>OCIO</td>
<td>The Library will refine its POA&amp;M process to ensure management review of reports of overdue POA&amp;Ms and address justification for any delays or extensions.</td>
<td>Q2 FY2022</td>
</tr>
<tr>
<td>6.3</td>
<td>Review cloud system continuous monitoring plans to ensure that the control scopes and assessment frequencies are commensurate with the systems’ control baselines. Monitor performance of control assessments accordingly.</td>
<td>OCIO</td>
<td>The Library will review the continuous monitoring plans to ensure control scopes and assessment frequencies are commensurate with the systems’ control baselines. Monitoring frequencies may be adjusted accordingly.</td>
<td>Q3 FY2022</td>
</tr>
<tr>
<td>6.4</td>
<td>Review the SSPs in Archer to determine the scope of the technical error related to inherited controls. Coordinate with the vendor to identify and implement a solution.</td>
<td>OCIO</td>
<td>The Library will review Archer configurations and address the technical issues related to inherited controls.</td>
<td>Q3 FY2022</td>
</tr>
<tr>
<td>6.5</td>
<td>Conduct an analysis to determine if SSPs for other systems have insufficient tailoring or inheritance statements and create a plan to address any identified gaps.</td>
<td>OCIO</td>
<td>The Library will conduct an analysis of SSPs to verify the tailoring/inheritance is accurately captured and create a plan to address identified gaps.</td>
<td>Q3 FY2022</td>
</tr>
<tr>
<td>7.1</td>
<td>Establish Library-specific cost models for computing, storage, and network services that the Library can use in performing TCO comparisons and monitoring.</td>
<td>OCIO in collaboration with FSD</td>
<td>The Library will establish Library-specific cost models for computing, storage, and network services that the Library can use in performing TCO comparisons and monitoring.</td>
<td>Q4 FY2023</td>
</tr>
<tr>
<td>7.2</td>
<td>Ensure the Library’s cloud strategy or implementation plan clearly identifies the need to document and present TCO comparisons when making hosting determinations.</td>
<td>OCIO</td>
<td>The Library will ensure that either its cloud strategy or implementation plan identifies the need to document and present TCO comparisons when making hosting determinations.</td>
<td>Q4 FY2023</td>
</tr>
<tr>
<td>7.3</td>
<td>Plan and monitor the implementation of its cloud IT investments and complete and submit quarterly and annual IT investment reports with documentation supporting the reported status, if necessary.</td>
<td>OCIO</td>
<td>The Library will monitor cloud IT investments and report on a quarterly basis, with documentation supporting the reported status, if necessary.</td>
<td>Q2 FY2023</td>
</tr>
</tbody>
</table>