MEMO

Date November 17, 2022
To Dr. Carla Hayden
Librarian of Congress
From Kimberly Byrd
Inspector General


The attached report presents the results of the annual audit of the Library of Congress’ (Library) financial statements for fiscal year (FY) 2021.

We contracted with the independent certified public accounting firm of KPMG for the FY 2021 audit. The contract required that KPMG perform the audit in accordance with Government Auditing Standards; the Office of Management and Budget Bulletin 21-04, Audit Requirements for Federal Financial Statements; and the U.S. Government Accountability Office and the Council of the Inspectors General on Integrity and Efficiency’s Financial Audit Manual.

Results of Independent Audit

Financial Statement Opinion

For the twenty-sixth consecutive year, we are pleased to report that the auditors issued an unmodified (clean) opinion on the Library’s financial statements. In its audit, KPMG found that the financial statements were fairly presented, in all material respects, in conformity with U.S. generally accepted accounting principles. Further details are in the Independent Auditor’s Report.

Internal Control over Financial Reporting

KPMG’s consideration of internal control over financial reporting resulted in a material weakness regarding deficiencies in Library’s controls to identify
disclosures for investments. KPMG also identified a significant deficiency regarding deficiencies in the Library’s Legislative Branch Financial Management System. Details for these findings are in Exhibit I and II of the Independent Auditor’s Report.

Compliance with Laws and Regulations

KPMG found no instances of noncompliance with laws and regulations tested.

Office of the Inspector General Oversight of KPMG

In connection with the contract, we reviewed KPMG’s report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with Government Auditing Standards, was not intended to enable us to express, and we do not express, opinions on the Library’s financial statements, conclusions about the effectiveness of internal controls, or conclusions on compliance with laws and regulations. KPMG is responsible for the attached auditor’s report dated November 14, 2022, and the conclusions expressed in the report. However, our review disclosed no instances where KPMG did not comply, in all material respects, with U.S. generally accepted government auditing standards.

cc: J. Mark Sweeney, Principal Deputy Librarian
Edward Jablonski, Chief Operating Officer
Mary Klutts, Chief Financial Officer
Michael Van Deusen, Comptroller
Judith Conklin, Chief Information Officer
John Rutledge, Deputy Chief Information Officer
Meredith Skowronski, Senior Counsel, Audit Liaison
Elizabeth Pugh, General Counsel

Attachments

---

1 A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the Library’s financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis.

2 In accordance with U.S. generally accepted government auditing standards, KPMG’s report is dated as of the last day of its fieldwork. KPMG’s final report was delivered to the Office of the Inspector General on November 14, 2022.
Independent Auditors’ Report

Inspector General of the Library of Congress
Librarian of Congress:

Report on the Financial Statements
We have audited the accompanying consolidated financial statements of the Library of Congress (Library), which comprise the consolidated balance sheet as of September 30, 2021, and the related consolidated statements of net cost and changes in net position, and combined statement of budgetary resources for the year then ended, and the related notes to the consolidated financial statements.

Management’s Responsibility for the Financial Statements
Management is responsible for the preparation and fair presentation of these consolidated financial statements in accordance with U.S. generally accepted accounting principles; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of consolidated financial statements that are free from material misstatement, whether due to fraud or error.

Auditors’ Responsibility
Our responsibility is to express an opinion on these consolidated financial statements based on our audit. We conducted our audit in accordance with auditing standards generally accepted in the United States of America, in accordance with the standards applicable to financial audits contained in Government Auditing Standards issued by the Comptroller General of the United States, and in accordance with Office of Management and Budget (OMB) Bulletin No. 21-04, Audit Requirements for Federal Financial Statements. Those standards and OMB Bulletin No. 21-04 require that we plan and perform the audit to obtain reasonable assurance about whether the consolidated financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the consolidated financial statements. The procedures selected depend on the auditors’ judgment, including the assessment of the risks of material misstatement of the consolidated financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity’s preparation and fair presentation of the consolidated financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity’s internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the consolidated financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion
In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the Library of Congress as of September 30, 2021, and its net costs, changes in net position, and budgetary resources for the year then ended in accordance with U.S. generally accepted accounting principles.
Other Matters

Financial Statements as of and for the Year Ended September 30, 2020

The accompanying financial statements of the Library as of September 30, 2020 and for the year then ended were audited by other auditors whose report thereon dated May 14, 2021, expressed an unmodified opinion on those financial statements, before the adjustment to correct the error described in Note 3 to the consolidated financial statements. The other auditors’ report included other matter paragraphs that described the required supplementary information presented to supplement the financial statements and the other information presented for purposes of additional analysis, and that the other auditor did not express an opinion or provide any assurance on such information.

As part of our audit of the 2021 consolidated financial statements, we also audited the adjustments described in Note 3 that were applied to the 2020 consolidated financial statements. In our opinion, such adjustments are appropriate and have been properly applied. We were not engaged to audit, review, or apply any procedures to the 2020 consolidated financial statements of the Library other than with respect to the adjustments and, accordingly, we do not express an opinion or any other form of assurance on the 2020 consolidated financial statements as a whole.

Interactive Data

Management has elected to reference to information on websites or other forms of interactive data outside the financial report to provide additional information for the users of its consolidated financial statements. Such information is not a required part of the basic consolidated financial statements or supplementary information required by the Federal Accounting Standards Advisory Board. The information on these websites or the other interactive data has not been subjected to any of our auditing procedures, and accordingly we do not express an opinion or provide any assurance on it.

Required Supplementary Information

U.S. generally accepted accounting principles require that the information in the Management’s Discussion and Analysis and Assessment of Condition of Heritage Assets sections (hereinafter referred to as the “required supplementary information”) be presented to supplement the basic consolidated financial statements. Such information, although not a required part of the basic consolidated financial statements, is required by the Federal Accounting Standards Advisory Board who considers it to be an essential part of financial reporting for placing the basic consolidated financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management’s responses to our inquiries, the basic consolidated financial statements, and other knowledge we obtained during our audit of the basic consolidated financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Other Information

Our audit was conducted for the purpose of forming an opinion on the basic consolidated financial statements as a whole. The Table of Contents and Results of the Library of Congress Financial Statement Audit are presented for purposes of additional analysis and are not a required part of the basic consolidated financial statements. Such information has not been subjected to the auditing procedures applied in the audit of the basic consolidated financial statements, and accordingly, we do not express an opinion or provide any assurance on it.
Other Reporting Required by Government Auditing Standards

Internal Control over Financial Reporting

In planning and performing our audit of the consolidated financial statements as of and for the year ended September 30, 2021, we considered the Library’s internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Library’s internal control. Accordingly, we do not express an opinion on the effectiveness of the Library’s internal control. We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers’ Financial Integrity Act of 1982.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that have not been identified. However, as described in the accompanying Schedule of Findings, we did identify certain deficiencies in internal control that we consider to be material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity’s financial statements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiencies described in the accompanying Schedule of Findings as item Exhibit I to be a material weakness.

Library management did not report the material weakness in Exhibit I in its Internal Control Program, Systems Controls, and Legal Compliance section included in the Management’s Discussion and Analysis section of the accompanying Financial Statements Report.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiencies described in the accompanying Schedule of Findings as item Exhibit II to be a significant deficiency.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Library’s consolidated financial statements as of and for the year ended September 30, 2021 are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the consolidated financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under Government Auditing Standards or OMB Bulletin No. 21-04.

Management’s Responses to Findings

The Library’s responses to the findings identified in our audit are described in the Management Response to Independent Auditor’s Report on the Library of Congress FY 2021 Financial Statements following the accompanying Schedule of Findings. The Library’s responses were not subjected to the auditing procedures applied in the audit of the consolidated financial statements and, accordingly, we express no opinion on the responses.

Purpose of the Other Reporting Required by Government Auditing Standards

The purpose of the communication described in the Other Reporting Required by Government Auditing Standards section is solely to describe the scope of our testing of internal control and compliance and the
results of that testing, and not to provide an opinion on the effectiveness of the Library’s internal control or compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

Washington, D.C.
November 14, 2022
Independent Auditors’ Report
Exhibit I – Material Weakness

Schedule of Findings – Material Weakness
The weakness in internal control described in this Exhibit existed during the year ended September 30, 2021. The determination of which control deficiencies rise to the level of a material weakness or a significant deficiency is based on an evaluation of the impact of control deficiencies identified, considered individually and in the aggregate, on the Library of Congress (Library) consolidated financial statements as of and for the year ended September 30, 2021. The associated entity level controls, as defined by the Standards for Internal Control in the Federal Government issued by the Comptroller General of the United States (Green Book), are also identified in relation to the control activities in the corresponding areas of this Exhibit.

Deficiencies in Library of Congress’ Controls to Identify Disclosures for Investments

Background:
As a Legislative Branch agency of the Federal Government, the Library is not required to comply with the requirements of the Chief Financial Officers Act of 1990. However, for purposes of financial management and reporting, the Library has issued Library of Congress Regulation (LCR) 6-110, Financial Management, which states: “The Financial Services Directorate (FSD) will establish and maintain procedures to ensure that all of the Library’s financial activities are conducted in a manner consistent with a legislative branch agency, are in accordance with applicable laws and regulations, follow generally accepted accounting and internal control principles, and are managed with integrity and reliability.” The Library conforms to the standards prescribed by the Federal Accounting Standards Advisory Board (FASAB) as its basis for Generally Accepted Accounting Principles (GAAP), and as a result, the Library is required to follow FASAB’s GAAP Hierarchy to ensure all relevant disclosures are included in its financial statements.

Conditions:
The Library did not design and implement controls to assess that all items that require disclosure are completely and accurately included in the Library’s financial statement notes, as required by Green Book Principle 10. Specifically, the Library’s financial reporting process was not designed to identify the need to use Other Accounting Literature as a source of disclosure requirements related to non-federal investments.

Cause:
This deficiency is a result of insufficient entity level controls as follows:

The Library lacked the documented procedures and training related to the comprehensive review of financial statement disclosures, to validate that all required elements had been disclosed, as required by Green Book Principle 4. Without documented procedures and appropriate training, it is difficult for FSD staff to perform the proper validations, making the review of the financial statements less effective.

Effects:
Omitting a required disclosure from the notes to the financial statements resulted in incomplete financial information in the Library’s Financial Statements Report for FY2020 and FY2021, which the Library has corrected in the FY2021 Financial Statements Report. Specifically, the Investments note to the financial statements did not include the elements related to other investments held with the public required by the Financial Accounting Standards Board. These required elements include the fair value measurement and hierarchy within which the fair value measurements for non-federal investments are classified.
Recommendations:

We recommend that Library management:

1. Perform an annual review to identify all financial reporting requirements related to disclosures and design and implement internal controls to document the review.

2. Develop and document appropriate procedures for and train applicable FSD accounting staff on the review of draft financial statements to validate that all required financial statement disclosures have been included in compliance with GAAP.
Independent Auditors’ Report
Exhibit II – Significant Deficiency

Schedule of Findings - Significant Deficiency

The weakness in internal control described in this Exhibit existed during the year ended September 30, 2021. The determination of which control deficiencies rise to the level of a material weakness or a significant deficiency is based on an evaluation of the impact of control deficiencies identified, considered individually and in the aggregate, on the Library of Congress (Library) consolidated financial statements as of and for the year ended September 30, 2021. The associated entity level controls, as defined by the Standards for Internal Control in the Federal Government issued by the Comptroller General of the United States (Green Book), are also identified in relation to the control activities in the corresponding areas of this Exhibit.

Deficiencies in Library of Congress’ Legislative Branch Financial Management System

Background:
As part of the Library’s Fiscal Year (FY) 2021 financial statement audit, we tested key information technology (IT) controls, including monitoring controls placed on third-party service organizations, to determine if relevant access controls, change management controls, computer operations and program development controls were designed and operating effectively. The service organization provides hosting services for Legislative Branch Financial Management System’s (LBFMS) physical servers and executes access and change management controls for the application’s production operating system (OS) and database (DB). Service organization employees perform development activities and are responsible for deploying configuration changes to the application. As part of our test procedures, we evaluated the implementation of the change management process.

On May 24, 2021, the Library’s service organization migrated the physical servers to a new hosting environment. The Library received the service organization’s single-user Statements on Standards for Attestation Engagements 18 (SSAE 18) System and Organization Controls (SOC) 1, Type 2, Report on Controls Placed in Operation and Tests of Operating Effectiveness for Services Provided to the Library of Congress for the Period of August 1, 2020 to July 31, 2021.

Conditions:
The Library did not design and implement appropriate types of control activities in the entity’s information system for coverage of information processing objectives for operational processes, as required by Green Book Principle 11, Design of Appropriate Types of Control Activities. Specifically, the Library did not:

- Effectively implement its control to monitor financially relevant controls designed and implemented by the Library’s service organization, as follows:
  - The Library inappropriately relied on the evaluation of hosting controls for the LBFMS application included in the FY 2021 SOC 1 report despite the exclusion of the new hosting environment and controls in place after the migration of the production OS and DB on May 24, 2021.
  - The Library did not coordinate with the service organization to ensure that the scope and subject matter of the SOC 1 report aligned with the complete service offerings performed by the service organization on behalf of the Library. Specifically, the Library did not ensure that the following controls were included and tested by the service organization auditor:
    - Application configuration management controls;
    - Batch/Interface configuration controls; and
    - Application privileged user access controls.
The Library did not coordinate with the service organization to ensure that preventative or detective access controls were designed and implemented to enforce segregation of duties between LBFMS developers and individuals who deploy changes to the production environment.

- Effectively design and implement its controls over the periodic review and recertification of LBFMS privileged application, DB, and OS users’ access. Specifically, the review and recertification was reviewed using manually maintained listings and was not performed using a system-generated listing from LBFMS.
- Appropriately design its control to maintain a complete and accurate system-generated list of production LBFMS application and DB changes that can be traced to approved change request documents for the production environment.
- Document controls to monitor the LBFMS’ interface job processes with other systems.

**Causes:**

These deficiencies are a result of insufficient entity level controls as follows:

- Green Book Principle 5 requires that “Management should evaluate performance and hold individuals accountable for their internal control responsibilities.”
- Green Book Principle 7 requires that “Management should identify, analyze, and respond to risks related to achieving the defined objectives.”
- Green Book Principle 13 requires that “Management should use quality information to achieve the entity’s objectives.”
- Green Book Principle 16 requires that “Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.”

**Effects:**

The deficiencies in the controls over the monitoring of service organizations limit the assurance on the design and operating effectiveness of the access, change management, configuration management, separation of duties, batch/interface processing, and privileged user access controls the Library is relying on for LBFMS, which increases the risk that the Library may not be aware of existing or potential weaknesses that could adversely affect the integrity of LBFMS financial and system data.

In addition, granting excessive privileges to developers and not utilizing a system-generated listing of users during periodic reviews of access exposes the Library’s financial data to increased risk of inadvertent or deliberate disclosure, modification, or destruction of financial data.

Similarly, relying on a ticketing system for control procedures and not a system-generated list of changes increases the risk that unauthorized changes may be implemented into the production application without being detected by management. The Library was unable to provide a reconciliation demonstrating all implemented LBFMS application and DB changes were tested and approved.

Also, the lack of adequately documented controls increases the risk that controls are performed incorrectly or inconsistently, increasing the risk that failed interface job processes are undetected by the Library. The lack of consistent interface job process monitoring and reconciliation of failed interface execution may lead to incomplete, inaccurate, or invalid financial data.
Recommendations:

We provided Library management with a separate letter that includes specific information about the control deficiencies, our understanding of the specific causes of the control deficiencies, and our recommendations.
MEMORANDUM

DATE November 9, 2022
TO Kimberly Byrd, Inspector General
FROM Carla Hayden, Librarian of Congress

The Library of Congress (Library) has reviewed the draft Independent Auditor’s Report from KPMG, which includes the auditor’s opinion on the Library’s financial statements, report on internal controls over financial reporting, and report on compliance with laws and regulations. We are pleased the Library received an unmodified, clean, audit opinion, finding the financial statements were fairly presented, and with no instance of noncompliance with laws and regulations.

The Library acknowledges the importance of a strong internal control environment. We have already begun to address the significant deficiencies identified in the report and, in fact, have completed nine of the ten corrective actions to date. In response to the material weakness, the Library revised its disclosures of invested funds held outside Treasury in the FY21 financial statements pursuant to the auditor’s recommendations and the Library will continue its analysis of generally accepted accounting principles to validate and document controlling standards as guidance for future Library financial reporting. We are also proud of the hard work the Library’s Financial Services Directorate (FSD) has undertaken over the last year to close the four financial recommendations from fiscal year 2020. The FSD’s efforts in resolving past material weaknesses show the Library’s commitment to and continual improvement of its financial management responsibilities.

We have provided corrective action plans in response to the individual audit recommendations and appreciate your support as we undertaken resolution.

cc: Mary Klutts, Chief Financial Officer
<table>
<thead>
<tr>
<th>Report Number</th>
<th>Prior Report or New</th>
<th>Finding</th>
<th>Recommendation</th>
<th>Responsible Office</th>
<th>Action Plan</th>
<th>Target Date</th>
<th>POA&amp;M Number</th>
<th>POA&amp;M Open/ Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFR 2021-FRP-001</td>
<td>new</td>
<td>Controls Not Designed to Identify Disclosures for Investments</td>
<td>1. Perform an annual review to identify all financial reporting requirements related to disclosures and design and implement internal controls to document the review.</td>
<td>FSD</td>
<td>The Library (FSD) has begun to perform quarterly reviews of FASAB accompanied by the USSGL as a guidance to document the review. In addition to documenting quarterly reviews, annually, we will perform a review of the A-136, GAO greenbook and prepare the FAM 2010. With these processes in place, we have designated a senior operating accountant in the financial reports division to oversee the reviews as well as initiate reviewing any other guidance deemed applicable to maintain compliance with GAAP. The senior operating accountant will maintain a checklist that will identify what was reviewed and all financial reporting requirements related to disclosures and what was done to resolve the issue(s).</td>
<td>1/31/2023</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFR 2021-FRP-001</td>
<td>new</td>
<td>Controls Not Designed to Identify Disclosures for Investments</td>
<td>2. Develop and document appropriate procedures for and train applicable FSD accounting staff on the review of draft financial statements to validate that all required financial statement disclosures have been included in compliance with GAAP.</td>
<td>FSD</td>
<td>The Library (FSD) has designated a senior operating accountant in the financial reports division to review all necessary documentation needed to maintain compliance with GAAP. This senior operating accountant will oversee the FSD accountants work performed for LOC as well as the cross service agencies to make sure that the investment note and other notes disclosures have been validated and are accurate based on the review of guidance as applicable to LOC. The senior operating accountant will maintain a checklist that will show all entailed in the review.</td>
<td>1/31/2023</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Independent Auditor’s Report on Internal Control over Financial Reporting - Significant Deficiency

- Deficiencies in Library of Congress’ Monitoring of Service Organization Reports
- Privileged User Recertification
- Deficiencies in Maintaining a Complete and Accurate System-Generated Listing of Legislative Branch Financial Management System’s (LBFMS) Application and Database Configuration Changes
- Deficiencies in Segregation of Duties Between LBFMS Application Change Developers and Deployers
- Lack of Documentation Over LBFMS Interface Monitoring Requirements
- Deficiencies in Scoping of LBFMS SOC 1 Report

<table>
<thead>
<tr>
<th>NFR 2021-IT-001</th>
<th>Deficiencies in Library of Congress’ Monitoring of Service Organization Reports</th>
<th>1. Create and/or update existing policies and/or procedures for performing risk assessments over the evaluation of SOC 1 reports whenever changes occur to LBFMS and/or its control environment at the A1 service organization.</th>
<th>OCIO &amp; FSD</th>
<th>The Library (FSD) has ensured that the SOC 1 reports cover all changes related to LBFMS and/or its control environment.</th>
<th>Closed 06-10-2022</th>
<th>POA&amp;M-936844</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFR 2021-IT-001</td>
<td>Deficiencies in Library of Congress’ Monitoring of Service Organization Reports</td>
<td>2. Require the LBFMS service organization to update the SOC 1 report to cover: a. Current logical access, change management, and separations of duties controls for the production OS and DB; and b. Any major changes and upgrades affecting the control environment, when applicable.</td>
<td>OCIO &amp; FSD</td>
<td>The Library (CGI via FSD) retained Schneider Downs (SD) to perform the SSAE-18 SOC 1 Type II Audit to include the requirements outlined in the NFR.</td>
<td>Closed 06-10-2022</td>
<td>POA&amp;M-936844</td>
<td>Closed</td>
</tr>
<tr>
<td>NFR 2021-IT-002</td>
<td>Privileged User Recertification</td>
<td>Update LBFMS-specific policies and procedures to require CGI to provide a system-generated listing of privileged users during the performance of management’s periodic review and recertification of application, DB, and OS access.</td>
<td>OCIO &amp; FSD</td>
<td>The Library (FSD) updated the SOW requiring CGI to provide a system generated list of users as part of the quarterly privileged access reviews, and a memo stating CGI’s certification of their review. CGI is providing these artifacts to the Information System Business Owner (ISBO) and Information System Security Officer (ISSO) for review and will continue to do so on a quarterly basis.</td>
<td>Closed 05-23-2022</td>
<td>POA&amp;M-936845</td>
<td>Closed</td>
</tr>
</tbody>
</table>
Deficiencies in Maintaining a Complete and Accurate System-Generated Listing of LBFMS Application and Database Configuration Changes

1. Establish a process or mechanism to monitor changes implemented to the production LBFMS application to prevent and detect changes not tracked in Jira. This process should allow for the generation of a system report of all changes made to the LBFMS application.

OCIO & FSD

This deficiency will be remediated with the implementation of Momentum 8.x, which is scheduled for Q2 FY2024. The Library (FSD) is working with CGI to schedule a full demo of Momentum 8.x automated change management feature. The automated process available in Momentum 8.x will provide auditing of code deployment, allowing for tracking of each line of code to approved changes to the Momentum application. This project is estimated to cost $2.6 million and the task order award for this effort is planned for February 2023. Afterwards the project is estimated to take up to fifteen (15) months with the expected Go-Live in May 2024. The Authorizing Official signed a Risk Acceptance for this on 8/22/2022 to allow time for procurement and installation. FSD understands and accepts that this will remain a finding in the upcoming FY2022 and FY2023 Financial Statement audits.

May 2022:
Per FSD, the target Go-Live for Momentum 8.x release will be April-May, 2024.

2. Periodically reconcile the system-generated listing of changes with the ticketing system to ensure unauthorized changes are not implemented to the production application without management’s awareness.

OCIO & FSD

The ISSO is scheduling monthly reconciliation of system-generated listing of changes with the ticketing system between the OCIO and FSD. Confirmation of this review will be logged in the LBFMS Momentum Production Database Change Review Book on a monthly basis.

Closed 09-23-2022

POA&M-936839

Closed
| NFR 2021-IT-004 | Deficiencies in Segregation of Duties Between LBFMS Application Change Developers and Deployers | 1. Require CGI to either implement a systemic access control that will restrict developers from deploying changes to production or implement a review of changes implemented to the production environment to verify that developers have not implemented their own changes to the production environment and include those controls in the SOC 1 assessment. | OCIO & FSD | The Library (CGI via FSD) implemented a process to ensure developers do not have access to deploy change to the LBFMS production environment. | Closed 05-23-2022 | POA&M-936845 | Closed |
| NFR 2021-IT-004 | Deficiencies in Segregation of Duties Between LBFMS Application Change Developers and Deployers | 2. Monitor and evaluate CGI over its application change management and access controls to ensure that segregation of duties principles are being enforced. | OCIO & FSD | The Library implemented a process to include review of developers’ access in the production environment as part of the quarterly segregation of duties and least privilege review. | Closed 05-23-2022 | POA&M-936845 | Closed |
| NFR 2021-IT-005 | Lack of Documentation Over LBFMS Interface Monitoring Requirements | Develop and communicate formal policies and procedures over the process for monitoring the completeness and accuracy of LBFMS’ financial interface job processes, specifically with WebTA and EmpowHR. | OCIO & FSD | The Library (FSD) documented controls to monitor the successful completion of LBFMS’ interface job processes in the Momentum Interface Jobs Review SOP. During this FY2021 audit, FSD informed KPMG that they only monitor job processing failures for the WebTA interface as Momentum only receives files generated from WebTA automation. Additionally, FSD does not monitor EmpowHR and should not have been noted in the NFR. | Closed 05-17-2022 | POA&M-936851 | Closed |
| NFR 2021-IT-006 | Deficiencies in Scoping of LBFMS SOC 1 Report | 1. Catalogue all controls performed by CGI Federal and direct CGI Federal to have the service auditor test the controls deemed financially relevant | OCIO & FSD | The Library (FSD) has ensured that the SOC 1 reports cover all changes related to LBFMS and/or its control environment. | Closed 06-10-2022 | POA&M-936844 | Closed |
| NFR 2021-IT-006 | Deficiencies in Scoping of LBFMS SOC 1 Report | 2. Require CGI to update its future single-user LBFMS SOC 1 reports to cover all financially relevant controls performed on behalf of LOC, including application configuration management, batch/interface processing, and application privileged user access controls. | OCIO &FSD | The Library (CGI via FSD) retained Schneider Downs (SD) to perform the SSAE-18 SOC 1 Type II Audit to include the requirements outlined in the NFR. | Closed 06-10-2022 | POA&M-936844 | Closed |