This is the accessible text file for Library of Congress Office of the Inspector General's Final Audit Report Enterprise Risk Management Audit, Report No. 2020-PA-104 on June 8, 2021.

Office of the Inspector General
Library of Congress
Memo

Date June 8, 2021
To Dr. Carla Hayden
Librarian of Congress
From Kurt W. Hyde
Inspector General
Subject Final Audit Report Enterprise Risk Management Audit, Report No. 2020-PA-104

The attached final report presents the results of Cotton & Company s (Cotton) audit. The objective was to determine the adequacy of the Library s Enterprise Risk Management (ERM) policies and procedures including compliance with those procedures. ERM is a future state for the Library so Cotton evaluated what the Library is doing to build towards an ERM program. Cotton found that the Library and the Strategic Planning and Performance Management Office (SPPM) have made strides in building a program that focuses on the integration of risk management and internal control activities. However, the Library must address several challenges before it can mature to ERM and made 12 recommendations to assist the Library with reaching its ERM goals.
Based on management s written response to the draft report, we consider all of the recommendations resolved. Your responses provided an action plan for the implementation of each recommendation, in accordance with LCR 9-160, Rights and Responsibilities of Employees to the Inspector General, 6.A. This report will be made publicly available.
We appreciate the cooperation and courtesies extended by the SPPM.
cc Principal Deputy Librarian
Director, SPPM
General Counsel

Appendix A: Cotton & Company s audit report

ENTERPRISE RISK MANAGEMENT PERFORMANCE AUDIT LIBRARY OF CONGRESS
OFFICE OF THE INSPECTOR GENERAL
May 26, 2021

Cotton & Company LLP 333 John Carlyle Street Suite 500
Alexandria, Virginia 22314
703.836.6701 [voice]
703.836.0941 [fax]
www.cottoncpa.com

Michael W. Gillespie, CPA, CFE, Partner mikeg@cottoncpa.com

ENTERPRISE RISK MANAGEMENT PERFORMANCE AUDIT LIBRARY OF CONGRESS OFFICE OF THE INSPECTOR GENERAL

1. EXECUTIVE SUMMARY

Enterprise Risk Management (ERM) considers an agency-wide portfolio view of challenges to provide improved insight into how to prioritize and manage risks more effectively for mission delivery. Effective ERM facilitates improved decision-making through a structured understanding of opportunities and threats and to implement strategies to ensure effective use of resources, enable an optimized approach to the identification and remediation of compliance issues, and promote reliable reporting and monitoring across business units.
According to the January 2020 Council of Inspectors General on Integrity and Efficiency s (CIGIE s) Inspectors General Guide to Assessing Enterprise Risk Management, federal agency management is responsible for implementing practices that effectively identify, assess, respond to, and report on risks. Agencies must incorporate risk awareness into their cultures and ways of doing business.

The Library of Congress (Library) is not subject to Office of Management and Budget (OMB) Circular A-123, Management s Responsibility for Internal Control. However, the Circular does present to agencies a valuable foundation for ERM efforts. The Circular indicates that agencies need to establish and foster an open, transparent culture that encourages people to communicate information about potential risks and other concerns with their superiors without fear of retaliation or blame. In implementing an ERM program, it is management s responsibility to: determine the comprehensiveness and granularity of the risk profile and risk inventory; determine which risks should be captured in the risk inventory and summarized in the risk profile; prioritize risks based on the likelihood and impact of risks occurring; and decide the appropriate risk responses. The CIGIE guide indicates, Although this guide provides the OIG community with a baseline framework for assessing ERM programs, there is no one-size-fits-all approach toward ERM. Therefore, U.S. federal government agencies can decide their individual approaches to ERM.

In fiscal year (FY) 2018, the Library implemented its Integrated Risk Management and Internal Controls (iRIC) program. The Library s Strategic Planning and Performance Management (SPPM) office opted to view enterprise-level as a future state in its ERM maturity process, rather than beginning with an enterprise-level approach towards risk management. Therefore, we evaluated what the Library is doing to build towards an enterprise-level risk management program.

The purpose of this performance audit report is to provide the results of our analysis of the Library s ERM program. Our testing found that, although the Library has a plan to reach the enterprise-wide level by FY 2021, the Library must address several challenges before it is able to reach an ERM maturity status. Our testing indicated that, while we believe the Library s stated timeframes are ambitious, there are actions the Library could take to more timely implement its ERM goals.

We communicated the results of our audit and the related findings and recommendations to SPPM and the Office of Inspector General (OIG). We have included management s responses to our findings in Appendix C.

2. OBJECTIVES, SCOPE, AND METHODOLOGY

The OIG engaged Cotton & Company to conduct a performance audit of the Library s ERM program.

We performed an end-to-end and holistic evaluation of the Library s program. This included:

- Reviewing key documentation that the Library produced to support its approach to integrated risk and controls management.
- Performing interviews and walkthroughs with key risk management personnel, including two service unit heads.
- Determining the extent to which the Library s program aligns with its strategic initiatives and overall governance efforts.
- Mapping the risk identification process, including coordination with the Library s service units to ensure proper identification of risks, and the maturity of its existing program.
- Performing an external benchmarking analysis; please see Appendix B: Benchmarking Analysis.

Further, we took into consideration the recommendations of various ERM-related directives and guidance for effective ERM in federal agencies, such as:

- OMB Circular A-123
- Committee of Sponsoring Organizations of the Treadway Commission s (COSO s) Enterprise Risk Management Integrated Framework
- Government Accountability Office s (GAO s) Standards for Internal Control in the Federal Government (Green Book)
- GAO s A Framework for Managing Fraud Risks in Federal Programs
- ERM Playbook 2
- International Organization for Standardization s (ISO) 31000:2018 Risk management Guidelines

Additionally, the recently released CIGIE ERM assessment lists 30 potential activities for OIG evaluations of ERM. Our testing incorporated these 30 activities, scaled accordingly due to the size of the Library as a federal agency and the anticipated nature of its ERM program.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), 2018 Revision, as issued by the Comptroller General of

the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

3. BACKGROUND

The Library is the world s largest and most comprehensive library, maintaining a collection of more than 170 million items many of them unique and irreplaceable in more than
470 languages. The Library s mission is to support the U.S. Congress in fulfilling its constitutional duties and to further the progress of knowledge and creativity for the benefit of the American people.

The Library s OIG was established in 1988 as a non-statutory office deriving its authority from the Librarian of Congress. The OIG became statutory with the passage of the Library of Congress Inspector General Act of 2005 (2 U.S.C. section 185), which mandated the Library OIG must:

- Independently conduct and supervise audits and investigations of fraud, waste, and abuse relating to the Library;
- Lead, coordinate, and recommend policies to promote economy, efficiency, and effectiveness; and
- Keep the Librarian of Congress and the U.S. Congress fully and currently informed about problems and deficiencies relating to the administration and operations of the Library.

The Inspector General is a member of CIGIE, a unified council of all federal statutory Inspectors General. The Audits Division conducts in-depth reviews that address the efficiency, effectiveness, and economy of the Library s programs, activities, and functions; provides information to responsible parties to improve public accountability; facilitates oversight and decision-making; and initiates corrective action as needed.

We designed this performance audit to meet the objectives identified in the Objectives, Scope, and Methodology section of this report. We conducted the audit in accordance with GAGAS. Cotton & Company performed the work from June 26, 2020, through May 3, 2021. We communicated the results of our audit and the related findings and recommendations to both SPPM and the OIG.

4. AUDIT RESULTS

We found that, since 2018, the Library and SPPM made strides in building a program that focuses on the integration of risk management and internal control activities, as noted below.

SPPM aligned its risk management efforts with the Library s strategic initiatives. The Library- wide strategic plan (currently FYs 2019 2023) serves as a baseline for measuring performance. Each service unit must create its own directional plan that communicates the service unit s plan for implementing the Library s strategic plan.

The directional plans have granular detail and specific initiatives to execute. They identify agency-level initiatives and measures for which agency-level performance goals and targets, as well as reference risks and controls, are set for annual reporting. SPPM s Directional Plan Extension Guidance states that the unit s Directional Plan is the core element of the Planning, Performance, and Risk Management lifecycle. With the Strategic Plan as its foundation, Directional Plans establish the five-year path for each service unit and center, and is the basis for determining unit performance goals, targets, and strategic and operational risks. - The directional plans are internal management documents, although the Copyright Office does have one version created for external stakeholders. In this process, planning is performed first, then the strategic Agency Performance Goals (APGs) are submitted to the Principal Deputy Librarian for review. The Principal Deputy Librarian then meets with the service unit heads to discuss their strategies and any necessary adjustments.
After making these adjustments, the service units proceed with their individual risk management efforts. Each service unit plans; sets goals and targets; and identifies, assesses, and determines management plans for risks associated with the work.

SPPM also established a framework that provides an approach for the Library and its service units to establish individual service unit goals and objectives, determine the work needed to achieve them, monitor performance, and modify strategies based on performance and changes in the external environment and the Library. A written guide to the risk management component of the framework titled the SPPM Planning, Performance and Risk Management Framework - Integrated Risk Management and Internal Controls Guidance (iRIC Guide) states that risk management is both a required activity (i.e., monitoring and reporting on internal controls) and a management best practice (i.e., integrating risk management into planning and performance activities).

The iRIC framework focuses the Library s attention on risks associated with priority work, as indicated by agency-level performance goals (APGs) and Key Service Unit Business Processes (KBPs). A Library-wide risk register, which the service units update quarterly, document and monitor these risks considered to be Library level. The most recent iRIC Guide (dated March 2020) provides guidance to service units in the creation of their directional plans, annual performance planning, and performance and risk reporting through an integrated risk management process. The iRIC section of the guide details risk management process and includes risk identification, risk assessment scoring (risk impact and probability), internal controls identification to manage risks, documenting risks in a risk register, and monitoring and reporting.

The status of risks are updated quarterly, and risk language is used in directional plans and regular Executive Committee (EC) spotlights. It is implemented into annual reporting, and it impacts the annual Statement of Assurance process, in which letters of assurance are received by SPPM from each service unit.

As part of the Library s risk program, SPPM guides the service units through the OMB Circular A-123 Annual Statement of Assurance Process, as well as collects and compiles letters of assurance annually to send to the Deputy Principle Librarian for signature and approval. The service units are responsible for crafting the letters

of assurance.

In August 2020, SPPM provided a draft plan titled Integrated Risk Management and Internal Controls Plan for Continuous Improvement. The purpose of the plan is to set the path toward maturity of the Library s iRIC to a mature ERM. The plan included a list of FYs 2019 2020 accomplishments and noted progress through the first maturity phase during FYs 2018 and 2019, as well as key activities expected to continue maturation through Integrated, Proactive, and Full Maturity. SPPM presented the maturity model below.

iRIC Maturity Model Table (Library of Congress SPPM pre-decisional draft)

iRIC Maturity Progress Indicators

Implementation (Initial Progress - stages in parenthesis reflect iRIC Maturity Mapping to OMB/GAO. See Appendix A.) (activity complete)
iRIC Maturity Progress Indicators
SU Risk Registers updated quarterly. (activity complete)
Governance structure is approved/established. (activity complete)
Performance and Risk Work Group (PRG) convened. (activity complete)
LCR published. (activity complete)
Internal control guidance updated/disseminated and implemented. (activity complete)
Assurance Letter process defined and executed. (activity complete)
Ongoing communication and training plan developed and executed. (activity complete)

Milestone Activity
Implement iRIC Framework (activity complete)

Integrated (Moderate Progress) FY 2020 through FY 2021
iRIC Maturity Progress Indicators
Library-wide risks are prioritized and risk profile is developed.
Library-wide risks are discussed and incorporated into decision making and budget considerations.
Requirements identified for enabling automated (post-Compass) system. (activity complete)
LCD published.
Deepened understanding and skills for risk owners.
Continuous improvement plan developed/approved. (The purpose of this deck).

Milestone Activity
Enterprise-approach to Risk Management.

Proactive (Significant Progress) FY 2022 through FY2023
iRIC Maturity Progress Indicators
Risks are managed as a portfolio, i.e., across organizational silos, inter-relationships between risks and risk responses.
New risk culture supports effective identification and management of risks, i.e.,

leadership is engaged and managers and staff actively participate.
LCR and directives are updated to reflect Lessons Learned in iRIC approach.
Risk information more visibly informs budget formulation.

Milestone Activity
Agency-wide Risk Appetite established.

Full Maturity (Fully Aligned with OMB/GAO) FY 2024 (stages in parenthesis reflect iRIC Maturity Mapping to OMB/GAO. See Appendix A.)
iRIC Maturity Progress Indicators
LOC is recognized for implementation of fully mature Risk Management Process
iRIC fully meets the ERM criteria for and effective risk management process.
Risks are managed proactively with well-developed response plans.
Continuous improvement processes continues.

Milestone Activity
SU-leve Risk Appetite and Tolerance statements established.

As a result of the testing that we performed in several areas, we determined that the Library s program operates at the service unit level, with each of the Library s eight service units identifying risks to their strategic goals and key business processes. These risks are captured in COMPASS (an internally created automated tool), which contains the content of the Library s risk register. Service units are responsible for inputting and managing risks in the risk register. SPPM manages the overall risk register and the COMPASS system for agency-level reporting.

Although Library leadership reviews the quarterly risk registers across the board, risks are not identified and managed at a Library-wide level. Additionally, while individuals at the service unit level have insight into risks in their own operations, the service units are limited in managing Library-wide processes because of the silo-based risk identification approach at the Library. The Office of the Chief Information Officer (OCIO) and the Office of the Chief Operations (OCOO) are accountable for overseeing risk management and internal controls associated with centrally coordinated business processes throughout the Library. According to the iRIC Guide:

OCOO and OCIO should collaborate with service units in identifying and assessing risks, monitoring and reporting on risk and risk response status, and designing and communicating corrective actions when necessary. However, OCOO and OCIO will be responsible for declaring and monitoring any operational risks associated with these centrally coordinated business processes in their risk register.

We determined that service units do and should identify risks at the service unit level. However, an enterprise-wide risk management approach would provide a better approach to identifying risks that present the greatest threat across the entire agency.

The Library must address several challenges before it can mature to ERM. We have

identified five areas below that need improvement and provided associated recommendations.

Finding #1: As the Library implements a more mature ERM, it should form a governing body to ensure proper oversight and tone at the top.

Condition
The Library would benefit from a governance structure and dedicated risk management governance committee to meet its enterprise-wide goals. Specifically, we believe the Library should employ an improved tone at the top to move the Library from its current iRIC approach to a future state centered on ERM in the timeline provided in the SPPM improvement plan.

ERM governance sets the agency s tone that reinforces the importance of having a robust ERM function in place. A dedicated risk management board s role may include, but is not limited to: reviewing, challenging, and concurring with management on proposed strategy and risk appetite. It also includes determining whether strategy and objectives within the stated mission, vision, and core values are being compromised by external and/or internal risk impacts throughout the entire agency not just at the service unit level, as is the case at the Library. It further allows for alignment of significant business decisions, including responding to significant fluctuations in agency performance and identifying, approving, and enhancing the portfolio view of risk. Over the longer term, ERM can also enhance enterprise resilience: the ability to anticipate and respond to change. According to COSO: [Footnote 1]

[I]t helps organizations identify factors that represent not just risk, but change, and how that change could impact performance and necessitate a shift in strategy. By seeing change more clearly, an organization can fashion its own plan. Enterprise risk management provides the right framework for boards to assess risk and embrace a mindset of resilience.

The Library has an Executive Committee (EC) and the Planning, Performance, and Risk Working Group (PRG), which consider risk management as a part of their overall responsibilities.
However, these bodies are not considered appropriate governing bodies for an ERM when established at the Library.

The EC a working group of the Library s top executives meets regularly and considers top risks as a part of its meetings, yet the EC s focus is not solely on risk management and it does not make risk management decisions. SPPM facilitates ad hoc meetings with working groups and monthly spotlight meetings for the EC, which include risk status for priority work. SPPM owns and manages the iRIC process that relies on the individual service units for risk identification, and each service unit maintains both its own risk register (through the COMPASS system) and risk responses. The SPPM director holds monthly meetings with the Librarian and Principal Deputy Librarian, as well as provides updates to the EC as needed.

The PRG serves as a liaison between SPPM and the service units. The group members are representatives from the service units. They attend meetings with SPPM, then

disseminate information to the risk owners in their individual service units. The PRG is not a governing body, as it does not focus exclusively on risk management, and the risks they identify are at the service unit level, not cross-cutting or at the enterprise level for the Library.

In their current roles, the EC and PRG do not provide the type of governance oversight and tone at the top to best assist the Library to meet its enterprise-level goals. A governance body dedicated to risk management has its own charter specifically focused on risk management, as well as the authority to emphasize agency-wide attention to risk identification and drive risk management throughout the entire agency from both a top-down and bottom-up perspective.

SPPM management has already found gaps within the existing structure and process to address if it is to be successful in establishing an ERM program. In August 2020, SPPM compared its existing risk management program to the GAO Green Book and ERM Playbook components.
This revealed several issues related to the lack of a governing body dedicated to risk management, as is required for an ERM. We evaluated the SPPM analysis; please see Appendix A: GAO Green Book and ERM Playbook Extracts and Analysis.

According to SPPM s Obstacles to Reaching Next Level of Maturity within the August 2020 iRIC Improvement Plan, the Library lacks the data and language to identify and communicate risk at the enterprise level. We also found that the Library does not have a designated Chief Risk Officer (CRO) to oversee/lead ERM efforts and work closely with an ERM governance body to further the movement toward enterprise-level maturity at the Library.

Cause
The Library embedded risk management into current committees that neither set a tone for agency-wide risk management nor serve as governing bodies totally dedicated to driving an enterprise-level view of risk management.

Effect
The tone at the top drives the success or failure of achieving an ERM program. Lack of an ERM- dedicated governing body with its own separate charter has a cascading effect throughout an agency and does not allow for bottom-up buy-in and cultural acceptance of an ERM program.

Criteria
Playbook: Enterprise Risk Management for the U.S. Federal Government (2016) [Footnote 2] - V. Risk Governance states:

Strong leadership at the top of the organization, including active participation in oversight, is extremely important for achieving success in an ERM program. ERM also requires active involvement and commitment from leaders in each business and program area (i.e., across silos) to develop and maintain a risk aware culture.

GAO Standards for Internal Control in the Federal Government (Green Book), Principle 2- Exercise Oversight Responsibility 2.01

The oversight body should oversee the entity s internal control system.

OMB Circular A-123, Management s Responsibility for Internal Control

To provide governance for the risk management function, agencies may use a Risk Management Council (RMC) to oversee the establishment of the Agency s risk profile, regular assessment of risk, and development of appropriate risk response.

COSO Enterprise Risk Management Integrated Framework (2017)

Every board has an oversight role, helping to support the creation of value in an entity and prevent its decline. Traditionally, enterprise risk management has played a strong supporting role at the board level. Now, boards are increasingly expected to provide oversight of enterprise risk management.

Recommendations
We recommend that:
1. SPPM add the establishment of an ERM governing body to its iRIC Improvement Plan
and maturity model.

2. The Library establish the ERM governing body during the integrated stage of maturity and prior to reaching enterprise-level of maturity.

3. The Library designate a Chief Risk Officer (CRO) to lead ERM efforts and to work closely with an ERM governing body to further the movement towards enterprise-level of maturity.

Finding #2: The Library would benefit from a more integrated budget and resource allocation process.

Condition
The Library needs an integrated budget and resource allocation process in order to meet its enterprise-wide goals. We determined that within the SPPM, Planning, Performance, and Risk Management Integrated Risk Management and Internal Controls Guidance indicates that through the development of Directional Plans and the surfacing and monitoring of both strategic and operational risks the integration of risk management activities into planning and performance activities begins to inform budget formulation, execution, and operations. Stated within this guide, there is specific guidance to the service units regarding budgetary consideration related to scoring risks. The guidance raises the following question that service units should consider related to risk scoring: will the risk influence current or future budget deliberations? The guidance also raises the following questions that service units should consider related to developing a risk response plan and mitigation through a budget plan: will the solution require additional or new funding? Will we need to request a general provision in the next budget request?

We reviewed the consolidated risk register as of FY 2020 Quarter (Q) 2, which revealed only two references to budget decisions within risk statements, four

references to budget decisions within risk plans, and one reference to budget decisions in the risk review statement. The consolidated risk register and the SPPM guidance do not specifically mention resource allocation decisions and how service units, EC, or PRG determine, discuss, or consider these decisions.

In August 2020, SPPM compared its existing risk management program to the GAO Green Book and ERM Playbook components. This revealed several issues needing resolution for the future- state ERM related to the lack of effective integration between budgeting, resource allocation, and risk management. We evaluated the SPPM analysis; please see Appendix A: GAO Green Book and ERM Playbook Extracts and Analysis.

In August 2020, SPPM also prepared an iRIC Improvement Plan indicating that the emphasis on budget and risk management integration will not occur until the FYs 2022 2023 timeframe. This period will include the ERM Proactive maturity stage, when the Library will ensure that risk information more visibly informs budget formulation. We noted no reference in the iRIC Improvement Plan to the critical path for addressing the tie between resource allocation decisions and risk considerations for an enterprise risk level of maturity. However, the Director of SPPM stated that, even though the Plan . . . did not specifically mention budget, it is well understood that the EPM project is necessary to enable resource allocation decisions based on desired impact, anticipated risk, and budget.

Cause
The Library has delayed its implementation of tying budget decisions to risk impact. Specifically, the Director of SPPM stated that

Our ability to effectively integrate risk with budget and other Library processes is dependent upon the progress of COO s Financial Services Directorate s critical Enterprise Planning Management (EPM) system, which includes a new integrated software solution to replace Compass in ~FY23-24 and integrate budgeting into the planning/performance management/risk management & IC frameworks.

Effect
The lack of integration between the budgetary process and risk management can hamper the ability of the Library to reach its future state as a mature ERM program.

Criteria
Playbook: Enterprise Risk Management for the U.S. Federal Government (2016)

2.D. Principle 6: The risk management process should be integrated within organizational processes such as strategic planning, budgeting, and performance management. Agencies should consider risks from across the agency and use them as important inputs to these processes (page 14). ERM should operate with the purpose of: Supporting budget decisions and performance management (page 9).

Recommendations
We recommend that:
4. The Library incorporates risk considerations into its budgetingand resourcing approach.

Finding #3: To ensure successful implementation of ERM, SPPM should establish a risk appetite statement and/or risk tolerance for the Library and service unit levels.

Condition
The Library does not have a defined risk appetite or risk tolerance statement as part of its iRIC program. Since the service units are responsible for risk identification, we evaluated SPPM s existing Guide to Integrated Risk Management and Internal Controls for any guidance to the service units pertaining to either risk appetite or risk tolerance. There is no guidance to the service units on how to develop risk appetite or risk tolerance at the service unit level, per our review of the SPPM s Guide to Integrated Risk Management and Internal Controls. We also evaluated the Consolidated Risk Register as of FY 2020 Q2 to determine whether the service units made reference to either risk appetite or risk tolerance. There were no references to either in the consolidated risk register.

We reviewed the SPPM timeline for defining a risk appetite or risk tolerance statement and although on the radar screen since at least FY 2018 activity to develop the risk appetite statement was not planned until FY 2021. SPPM s current target date to establish agency-wide risk appetite is FY 2022, and service unit risk appetite and tolerance statements by FY 2024.

The Library OIG March 2018 Semi-Annual Report to Congress listed top management challenges. The OIG specifically referenced risk tolerance in this report and listed as a risk: The documentation and assessment of the impact of identified risks should include consideration of the Library s tolerance for risk.

In August 2020, SPPM compared its existing risk management program to the GAO Green Book and ERM Playbook components and revealed several issues related to the lack of defined risk appetite and risk tolerance. We evaluated the SPPM analysis; please see Appendix A: GAO Green Book and ERM Playbook Extracts and Analysis.

Although the current iRIC process calls for service units to identify and assess risks, as well as develop the appropriate risk responses, it is unclear how the Library s service units may develop an appropriate risk response without first defining risk appetite or tolerance statements within the individual service units.

Cause
SPPM deferred creating a risk appetite or risk tolerance statements due to staffing turnover, a desire to focus on developing stronger risk management skills within the service units, and the potential difficulties in defining risk tolerances in different areas.

Effect
The lack of any guidance in this area within the current program does not allow service units to determine acceptable thresholds within their own service units or to make consistent decisions about potential consequences to their own operations or other parts of the Library.

Criteria
Playbook: Enterprise Risk Management for the U.S. Federal Government (2016)

2.D.7. Establishing Risk Appetite is Key: Risk is unavoidable and sometimes inherent, as is the case with a credit program, in carrying out an organization s objectives. Agencies should evaluate, prioritize, and manage risks to an acceptable level. Clearly expressed and well communicated risk appetite statements establishing thresholds for acceptable risk in the pursuit of objectives are important. These statements help agencies make decisions about potential consequences or impacts to other parts of the organization, limiting unexpected losses.

The most senior members of an organization should define overall acceptable levels in conjunction with goals and objectives, and within the context of established laws, regulations, standards, and rules. Risk appetite helps to align risks with rewards when making decisions. Agencies can accept greater risks in some areas than in others. Each program establishes risk appetite levels that, when consolidated, are within the risk appetite boundaries established for the entire organization. Risk appetite can be implicitly established and communicated when setting strategic or operational goals and objectives. These levels may be expressed qualitatively or as quantitative metrics. They can also be explicitly set and communicated through targets associated with performance measures and indicators.

GAO Standards for Internal Control in the Federal Government (Green Book)

Principle 6 Management should define objectives clearly to enable the identification of risks and define risk tolerances.

Recommendations
We recommend that:
5. SPPM provide guidance to the service units on risk appetite and risk tolerance, as well as update the SPPM iRIC Guidance accordingly, even while SPPM s future-state efforts regarding risk appetite and risk tolerance are developing.

Finding #4: The Library would benefit from having a portfolio view of risks as part of its overall risk identification process.

Condition
As the Library matures its ERM program, its service units should report all risks within a common system, which would allow a portfolio view of risks within the agency. SPPM relies on Library service units to perform risk identification activities. SPPM s current target date to manage risks as a portfolio is FY 2022 2023, according to the iRIC Improvement Plan. Although there is interaction between the service units and SPPM as it pertains to the existing risk management process, we found the following issues in the risk identification process.

Within the iRIC process, service units identify risks under the auspices of APGs and KBPs. Service units must also work closely with partner units and leadership to ensure that risks associated with cross-cutting and centrally coordinated business processes are shared and effectively monitored. The SPPM Guide to Integrated Risk Management and Internal Controls provides the foundation for the risk identification

process that service units are to follow. The service units work closely with SPPM; yet, ultimately, it is up to the service units to identify and report on risks. When each service unit identifies risks, they determine whether the risk is significant enough to be included in the agency-level service unit risk registers reported in COMPASS, the Library s current common system in which APG and KBP-related risks are reported. Subsequently, SPPM combines these risk registers into consolidated risk registers on a quarterly basis.

Service units have the option to manage these risks through the COMPASS system or by other methods. Only APG and KBP-related risks reported in the COMPASS system are visible to all staff. We interviewed representatives of two service units during the audit: OCOO and OCIO. We found that these service units also maintain risk registers at the service unit level, which include risks that only the service unit has visibility into and are not reported into the agency- level COMPASS system. Having some risks that are designated for service unit-level tracking and not agency-level tracking does not facilitate an integrated view of the Library s risks.

The service units are ultimately responsible for scoring risks and determining what risks will be included in the agency-level risk register, and so reported to Library leadership on a quarterly basis. Because agency-level designation in iRIC is tied to the need for executive oversight, risks may shift into or out of the agency-level risk register over time, given leadership, agency, and unit priorities. Other factors have affected the content of the current agency-level risk register. The FY 2020 Mid-Year iRIC report stated that 75 percent of the 52 APG-related risks identified in the FY 2020 Q2 Risk Register are either new or substantially altered from the previous year.
SPPM believes this is due to the significant change in how the Library perceived and established APGs between FY 19 and FY20, changing from developing Annual (1-year) Performance Goals with risks expected to be resolved in a short timeframe to the more standard, multi-year Agency Performance Goal (APG) construct. This had the impact of also changing the articulation of risks related to the goals.
Additionally, the Director of SPPM stated that another factor for this condition was a need to build awareness and understanding of risk concepts and how best to apply them to the service units work.

As an example of the high turnover of risks from the agency-level register, the FY 2019 EOY report showed seven Annual Performance Goal related risks related to the Office of Preservation. However, the consolidated risk register as of FY 2020 Q2 just 6 months later did not have Agency-level Performance Goals tied to preservation, and so did not include APG- related preservation risks. As of FY 2020 Q2, one KBP-related risk under the name of asset protection was reported on the agency-level risk register. This substantial reduction in the number of preservation risks reported at the agency level in the span of only a 6-month period would require a review of the service-unit level risk register to determine the proper reporting of all risks.

In its August 2020 iRIC Improvement Plan, SPPM also identified flaws in the use of COMPASS and the risk identification process among Library employees. The plan indicates a:

[L]ack of service unit staff attention and urgency to provide quality risk registry updates: Although service units are meeting the data call deadlines, updates are generally limited to the risk response updates. Staff rarely revise other risk elements, such as the risk score or response type. Updates are further hampered by staff s infrequent use of COMPASS. Even veteran users often forget how to use COMPASS between quarterly updates.

We learned that the available SPPM training is not mandatory, further contributing to the lack of risk identification awareness and proper reporting. The plan indicates that:

[S]taff understanding of risk management concepts remains inconsistent across the Library: Although SPPM made progress through its diagnostic sessions, additional training is needed to improve service unit risk understanding. Unless staff improve in their application of iRIC concepts, it will be difficult for Library management to use service unit-generated risk data to make informed, impactful decisions about their programs and operations.

The Library SPPM Guide to Integrated Risk Management and Internal Controls specifically calls out certain risks (e.g., external and political risks) as Out of Scope risks for the established iRIC program. The guide defines Out of Scope risks as follows:

Given the limited time and resources that service units face, it is important to be clear about the scope under consideration, and whether some potential risks fall out of the scope of the risk register.

It further states:

The iRIC framework focuses on areas of priority work that impact agency performance and operations, as designated by service units as APGs or KBPs. Therefore, the iRIC may not be [sic] the appropriate process for responding to the events described below, for which the Library may already have response plans in place.

The guide further indicates that characteristics of Out of Scope risks include:

[B]ig risks that are well beyond the capabilities of any individual service unit and require a collaborative effort across the Library as well as risks that are too small, or too rare to be included within the scope of a risk management effort; external risks that lie well beyond the service unit s ability to realistically change or influence, and will not respond

to an service unit-managed response plan; and risks that are already owned by other parties.

The examples of Out of Scope risks within the SPPM guide include the following in the extract below:

External (non-Federal) Risks
- weather-related disasters/shutdown

- major economic crisis
- war
- terrorism
- biohazardous event
- international political disruptions
- cultural preferences and trends

Political Risks
- sequestration or budget shutdown
- unanticipated decrease in appropriations
- changes in legislation an/or regulations
- unexpected loss of Library leadership
- Political scandals

Minor Risks
- Minute disruptions to staff attendance (traffic, sick days, etc.)
- Brief IT outages or slowdowns
- Minor delays in shipping/receiving non-critical collections items
- Marginal losses (lost, theft, damages) to common collection items (i.e., replaceable).

We performed a benchmarking study as part of this performance audit and raised the concept with the four similar agencies. Although we understand the Library s iRIC is more limited than an ERM, none of these agencies use this concept, whether the agency is at an integrated risk management or enterprise risk management level of maturity. Using an Out of Scope risks concept also does not present the opportunity for a portfolio view of risks even at the current maturity level of initial integrated within the Library. The August 2020 SPPM improvement plan indicates that library-wide risks are prioritized and library-wide risks are discussed and incorporated into decision making and budget considerations, yet does not specify how to accomplish this. Further, with the silo approach to risk management currently in place, the individual service units are limited in their insight into and ability to identify Library-wide risks.

A sample of two recent information technology (IT) audit reports [Footnote 3] identified 13 findings or areas of concern. The FY 2020 Consolidated Risk Register only recorded three of those findings and partially addressed one, leaving nine findings recognized during an audit, but not recognized as a risk in the consolidated risk register.

Cause
The silo nature of service units risk identification and reporting results in risk decisions and reporting risks deemed to be significant only at the individual service unit level. This results in risks reported at the unit level not being visible for agency-level reporting within the COMPASS system and a lack of a portfolio view of risks.

Effect
The lack of a portfolio view of risks limits the Library from reaching its future

state as a mature ERM program and does not allow for proper cross-cutting risk identification throughout the Library.

Criteria
Playbook: Enterprise Risk Management for the U.S. Federal Government (2016)

3. ERM Model - Tips for Documenting Risks

Develop meaningful risk categories: When defining or categorizing risks, agencies should consider categorization in ways that are most helpful and relevant to agency mission. Agencies should be cautious to not limit categories only within silos or to neglect categorizing sources of risks not typically associated with a particular silo, while recognizing any single risk may be associated with more than one category.

Use common language: Risks should be described using a common language that resonates within the agency regardless of program office or individual expertise. Removing jargon whenever possible improves communication.

Document risks regardless of control: Agencies should consider the risks that are both within and outside of an agency s direct control, including third parties, vendors, or contractors, but present a genuine risk to an agency s mission. For major risks outside of the agency s direct control, often the only response may be to prepare contingency plans.

Document action plans and outcomes: It is important for agencies to document what was done to respond to possible risks and use these as lessons learned that can be leveraged for future strategic planning and response plans for new risks that may arise.

Recommendations
We recommend that:
6. SPPM work with the service units to gain a further understanding of risks not being reported into COMPASS, in order to achieve a broader application of a portfolio view of internal and external risks.

7. SPPM revisit LCRs or LCDs to ensure any adjustments made to risk identification in the system be captured.

8. SPPM revisit the concept of Out of Scope risks in the context of the draft maturity model as of August 2020, which indicates an enterprise-level approach towards risk management as a key milestone between FYs 2020 and 2021.

9. SPPM define a path in its iRIC Improvement Plan regarding how to identify Library-wide risks in the context of the draft maturity model as of August 2020, which indicates an enterprise-level approach towards risk management as a key milestone between FYs 2020 and 2021.

Finding #5: The Library would benefit from implementing a fraud risk framework that aligns with its overall risk management efforts.

Condition
The Library does not have a formal fraud risk framework built into its iRIC program. Centrally coordinated business process areas (e.g., OCOO, OCIO) address fraud risks in their respective efforts risk registers as needed.

Since the service units are responsible for risk identification, we evaluated SPPM s existing Guide to Integrated Risk Management and Internal Controls for any guidance for the service units as it pertains to fraud risk. There are two brief definitions of fraud risk within the guidance and two mentions of insufficient controls that can result in fraud, misuse, or delinquencies. The guide does not include direction to the service units that aligns with the GAO Green Book components of a Fraud Risk Management Framework. We also evaluated the Consolidated Risk Register as of FY 2020 Q2 and identified a few discrete references to fraud in risk statements or risk responses, or when fraud was selected as a risk type for External Financial Reporting, Accounting Operations, Financial Systems, Contracts, and Registration Ingestion.

On August 27, 2020, SPPM provided the following response when we inquired about a copy of the existing Fraud Risk Framework: There is not a separate risk framework for fraud. Rather, fraud is identified as a risk type in the Risk Register, so that applicable risk information can be easily sorted and reviewed .

Cause
SPPM has relied on the service units to embed identification of fraud risks into their integrated risk reporting process. Therefore, there has not been emphasis on developing a formal, agency- wide fraud risk management program.

Effect
The lack of a formal fraud risk management framework that drives fraud risk identification including monitoring along with ongoing fraud risk assessments can hamper the Library s ability to reach a mature ERM program. With the service units responsibilities for fraud risk identification, lack of internal fraud risk guidance also leads to inconsistent approaches and risk responses in treating risk-related issues by the service units.

Criteria
GAO Fraud Risk Framework (2015)

In its Fraud Risk Framework guidance issued in 2015, GAO indicates that fraud poses a significant risk to the integrity of federal programs and erodes public trust in government. Managers of federal programs maintain the primary responsibility for enhancing program integrity. Legislation, guidance by the Office of Management and Budget (OMB), and new internal control standards have increasingly focused on the need for program managers to take a strategic approach to managing improper payments and risks, including fraud. Moreover, GAO s prior reviews highlight opportunities for federal managers to take a more strategic, risk-based approach to managing fraud risks and developing effective antifraud controls. Proactive fraud risk management is meant to facilitate a program s mission and strategic goals by ensuring that taxpayer dollars and government services serve their intended purposes. GAO

recommends the following four key components of a Fraud Risk Framework:

Commit Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.

Assess Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.

Design and Implement Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.

Evaluate and Adapt Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.

OMB Circular A-123, Appendix A

OMB Circular A-123, Appendix A, supports the formation of a Fraud Risk Framework and indicates within its guidance that the intention of the Fraud Risk Framework is to help managers to combat fraud and preserve integrity in government agencies and programs.

GAO Standards for Internal Control in the Federal Government (Green Book)

The GAO Green Book references fraud risk management, stating:

Management analyzes and responds to identified fraud risks so that they are effectively mitigated. Fraud risks are analyzed through the same risk analysis process performed for all identified risks. Management analyzes the identified fraud risks by estimating their significance, both individually and in the aggregate, to assess their effect on achieving the defined objectives. As part of analyzing fraud risk, management also assesses the risk of management override of controls. Management responds to fraud risks through the same risk response process performed for all analyzed risks.

Recommendations
We recommend that:
10. SPPM use the GAO Fraud Risk Framework components as a guide for creating an internal fraud risk framework.

11. SPPM incorporate a fraud risk framework into their existing iRIC program.

12. SPPM revisit the future-state dashboard and determine how to incorporate the dashboard.

COTTON & COMPANY LLP
Michael W. Gillespie, CPA, CFE Partner

APPENDIX A: GAO GREEN BOOK AND ERM PLAYBOOK EXTRACTS AND ANALYSIS

In August 2020, SPPM prepared and delivered an internal analysis of its existing risk management program to the components of the GAO Green Book and/or the ERM Playbook. Since these were two directives evaluated during the ERM audit, we evaluated SPPM s analysis and call out in this appendix any relevant supporting evidence whereby SPPM self-identified weaknesses within its existing risk management program. Below, we cover the results of this analysis, organized by weakness.

A. Lack of ERM Governing Body:

SPPM compared its governance progress to Green Book Principle 2, which focuses on the control environment and the exercise of oversight responsibility, and performed its own self- evaluation and rating. The rating (on a scale of 1 to 5) slid backward as of August 2020, and it is rated as red, having reduced from a 3 Moderate Progress to a 2 Initial Progress.

SPPM s analysis stated, the EC is not systematically using risk register data to interrogate internal controls and discussions of risk during spotlight meetings rarely lead to specific actions. The next step within this analysis indicates: The establishment of an enterprise risk management (ERM) governance body, including a charter, should improve the Library s ability to systematically review and respond to risk and internal control deficiencies.

B. Lack of Alignment of Budget and Resource Allocation to Risk Management:

SPPM compared its budget and resource allocation progress to the ERM Playbook Principles 3 through 7. SPPM identified several issues related to lack of alignment of budget and resource allocation to risk management. This comparison shows budget and resource allocation efforts as future-state activities. We noted that, for the Playbook Step 7, SPPM scoring has moved from 2 Initial Progress to 3 Moderate Progress. However, this is shown as having a lack of integration of risk management into budget decision-making, and SPPM kept this at the Initial Progress level when compared to Playbook Steps 4 through 6.

ERM Playbook Reference followed by Progress Scoring Mapping as of August 2020 and then Evidence/Comments by SPPM

Playbook Step 3: Analyze and Evaluate Risks - Management prioritizes the resulting identified risk.

Moved from Not Started (1) to Initial Progress (2) Moderate, High, and Critical risks associated with amber/red Performance Targets are assessed by SPPM in the biannual risk report. The risk register is sorted by risk score and distributed with the report to Library leadership and the PRG. While these are meaningful outputs for the iRIC program, SPPM lacks data on outcomes. E.g., How is management using this data to prioritize and respond to risk? Is it influencing hiring, budget, or other planning decisions? These decisions may be happening organically, but not systematically.

Playbook Step 4: Develop Alternatives - Management evaluates the cost of addressing risks with risk exposure, determines the value of potential benefits and loses, and determines how to allocate resources accordingly.
Moved from Not Started (1) to Initial Progress (2)
Difficult to determine given that resource decisions (and the data related to those decisions) occurs at the service unit level. However, by their nature all response plans should involve a consideration or the cost vs. benefits of risk mitigation. While risk is a required consideration in NEPRs, that is a separate process not formally tied to the iRIC framework. For example, there is no way to track whether risk register data is resulting in any budget decisions or ending up in a NEPR unless explicitly declared in the risk review statement. Next Steps: Improve consistency and understanding through training and outreach. Future state activities include explicit linkage between declared risks and resource requests (budget, staff, etc.).

Playbook Step 5: Respond to Risks - Management decides how to allocate scarce resources (budget resources, analytical capabilities, and management attention to address them).

Stayed Steady at Initial Progress (2)
The senior leadership considers risks in the general subjective sense during resource planning discussions, including the Directional Planning process. These discussions do not consistently connect to the iRIC Framework. Currently, it is difficult to determine how resource decisions are made, given that this information (and the data related to those decisions) occurs at the service level. Risk consideration is part of the budget process, but risk register and response plans are not linked to budget process systematically.
Next Steps: Improve understanding of risk response concepts through training and outreach. Future state activities include explicit linkage between declared risks and resource requests (budget, staff, etc.).

Playbook Step 6: Monitor and Review Risk - Management incorporates results into organization s performance management, measurement, and internal/external reporting activities.

Stayed Steady at Initial Progress (2)
Service units are reporting on risks associated with Executive Committee reported performance goals at monthly spotlight meetings for Agency-level performance goals. Some service units also have quarterly performance meetings to include update on risks. Results are reported on in the biannual iRIC report. Additional service unit specific outcomes regarding risk management are not effectively tracked or known at this time.
Next Steps: Future state activities include a more explicit linkage between declared risks and resource requests (budget, staff, etc.); development of risk dashboards for service units; and possibly reporting our risk information in the Annual Financial Report.

C. Lack of Defined Risk Appetite and/or Risk Tolerance:

We determined that the ERM Playbook has 58 references to risk appetite and 25

references to risk tolerance. We reviewed the SPPM analysis, comparing its existing risk management program to the ERM Playbook. We have noted the following:
- Playbook Step 2 for management examination of risks indicates that risks are identified and scored individually but are not compared in terms of significance from an agency perspective. Individual service units may be leveraging risk scores or other risk data to identify significant risks, but we [SPPM] have no evidence that this is occurring in a systematic way and that the next steps are to improve enterprise perspective of risk through the development of a Risk Appetite and pilot risk scorecards.
The rate for this overall effort is a 2 Initial Progress. However, SPPM will not implement its Risk Appetite statement until FY 2022.
- Playbook Step 3 Analyze and Evaluate Risks: In this same document, we noted that, for management assessing the positive or negative development of risks, the SPPM comments that the development of Risk Appetite is intended to introduce risk as opportunity concept.
- Playbook Step 4 bears the same comments as mentioned in the above paragraph. The FY 2018 EOY Appendix E analysis rated this activity a 1 Not Started and the evidence comments as: the Library currently does not determine risk appetite. Determining risk appetite is a future state activity.
- Principle 6 of the Green Book focuses on Defining Objectives and Risk Tolerances and specifically indicates that management should define objectives clearly to enable the identification of risks and define risk tolerances. We noted there is no mapping of this Green Book Principle to the iRIC or to the OMB Playbook GAO Green Book. The only mention of Risk Appetite as it pertains to the Green Book is under risk monitoring and reporting, rated as a 2 Initial Progress. Next steps are shown as shift to enterprise perspective of risk [, which] will allow for more visible components of risk program, including Agency Risk Appetite.

D. Lack of Portfolio Risk Identification Process: N/A

We did not see this reflected in the comparison documentation provided by SPPM.

E. Lack of Fraud Risk Framework

In the SPPM self-assessment, we noted the following as it pertains to fraud risks:

- Assess Fraud Risks: Management considers the potential for fraud when identifying, analyzing, and responding to risks. This is rated at 2 Initial Progress. Evidence is shown as:

Fraud risks are an available risk type in the Risk Register. Additional steps will need to be taken to ensure fraud risks receive more visibility, should they emerge as a serious issue. Next Steps: The development of risk dashboards to improve our ability to highlight specific risk areas for leadership.

APPENDIX B: BENCHMARKING ANALYSIS

We conducted a benchmarking analysis from August 28 to September 17, 2020. We selected the benchmarked federal agencies based on a like agency criteria defined by the Library OIG in conjunction with discussions that had been conducted with SPPM

leadership. The Deputy Library OIG defined like agency criteria as follows:
- Include federal agencies with more than 3,000 full-time equivalents (FTEs), which are comparable in size to the Library.
- Determine whether the federal agency is within the legislative branch of the U.S. government.
- Identify agencies with comparable funding complexity as that of the Library.
- Determine whether the GAO agrees with or approves of the federal agency s ERM Program.

We were not able to find agencies that fit all of the above criteria. Therefore, we selected agencies that effect a mix of criteria in order to perform this benchmarking analysis. Further, we noted that there are only limited circumstances in which GAO identifies best practices for ERM programs. Generally, this is reserved for Chief Financial Officers (CFO) Act federal agencies.

The agencies selected for benchmarking are, in alphabetical order: Architect of the Capitol (AOC), National Archives and Records Administration (NARA), National Institute of Standards and Technology (NIST), and Securities and Exchange Commission (SEC). Please note that, although we selected a fifth agency, that agency s OIG office recommended that we delay pursuing the agency for the benchmarking study due to internal efforts underway to rework its existing risk management program.

To ensure the confidentiality of the agencies selected for the benchmarking, we have not identified them in the comparative analysis presented in the table below; instead, we listed the agencies in a random order and identified them by a number. We interviewed agency representatives to gain insights into their agencies respective ERM programs and to cover the areas shown in the table below. We indicated whether the practice does or does not exist within each agency. We did not audit each of the individual programs of the agencies selected for this benchmarking analysis. We then compared the agencies success in implementing these criteria to the Library s success.

ERM Program Evaluation
Criteria
Dedicated ERM governance committee exists: Agency 1 Yes Agency 2 No Agency 3 Yes Agency 4 Yes Library of Congress No
Alignment with agency strategic plan initiatives, goals, etc.: Agency 1 Yes Agency 2 Yes Agency 3 Yes Agency 4 Yes Library of Congress Yes
Adopted ERM during initial implementation of program: Agency 1 Yes Agency 2 Yes Agency 3 Yes Agency 4 Yes Library of Congress No
Identified ERM as an end state rather than adopting at the outset: Agency 1 No Agency 2 No Agency 3 No Agency 4 No Library of Congress Yes
Designation of a Chief Risk Officer: Agency 1 Yes Agency 2 Yes Agency 3 Yes Agency 4 Yes Library of Congress No
Agency-wide portfolio view of risks in risk identification process: Agency 1 Yes Agency 2 Yes Agency 3 Yes Agency 4 Yes Library of Congress No
ERM program considers all risks: Agency 1 Yes Agency 2 Yes Agency 3 Yes Agency 4 Yes Library of Congress No
Risk appetite and/or risk tolerance statements in place: Agency 1 Yes Agency 2 No Agency 3 Yes Agency 4 Yes Library of Congress No

Use of external tools to measure maturity of ERM program (i.e., RIMS, Gartner Model) in addition to internal measuring tool: Agency 1 Yes Agency 2 No Agency 3 Yes Agency 4 Yes Library of Congress No

The overall key takeaways that we identified from this benchmarking study are shown below. The Library should consider:
- Ensuring top leadership support, as it is critical for agency-wide buy-in for ERM.
- Standardizing the tone at the top, which is essential to the success of an ERM program.
- Having an ERM-dedicated council or committee to allow for a tie-in between risk management, governance, strategy, and overall decision-making.
- Taking a top-down approach.
- Tying risk management to agency strategy, as it is considered a best practice.
- Embedding risk management in leadership training.
- Simplifying the risk management program to ease adoption and understanding agency-wide.
- Ensuring the ERM program and its progression is transparent across the agency.
- Identifying a portfolio view of risks, which allows for easier determination of risks that cross-cut the entire agency.
- Using ERM to drive decision-making across the agency.

APPENDIX C: MANAGEMENT RESPONSE
Library
Library of Congress
Office of the Librarian
Memorandum

Date May 3, 2021
To Kurt Hyde, Inspector General
From J. Mark Sweeney, Principal Deputy Librarian of Congress
Subject Management Response to OIG report 2020-PA-104, Enterprise Risk Management

Thank you for providing the draft audit report on Library Enterprise Risk Management. The Strategic Planning and Perfom1ance Management Office (SPPM) has been steadily progressing towards the incorporation of risk analyses into major planning and strategic
decision-making processes with the end goal of achieving an enterprise-wide risk management program. Because of the library's unique position in the legislative branch and, thus, flexibility, by not being subject to the Office of Management and Budget requirements, the Library welcomes the opportunity to formulate its risk management
policies in a way that advances its particular, mission-critical activities. The best practices and comparative analyses from other agencies that the audit has provided will be useful as we continue along the traj ectory towards an enterprise risk management program.

One challenge the Library has encountered involves the education and engagement of management and staff on fundamental risk management concepts and realization of an enterprise-wide program. Although the Library's Executive Committee receives the semi-annual iRIC status report and, during its regular meetings, considers strategic

risks as aligned with priority initiatives, as you observe, work remains to fully integrate risk analyses into enterprise-level decision-making. Recognizing this gap, the Library's
iRIC Improvement Plan includes an executive-level oversight group, and a Chief Risk Officer to oversee the work of that group. In addition, SPPM is in the process of developing an enterprise risk appetite statement that, when completed, will serve to guide service units in applying the concepts of risk appetite and tolerance to their work.

We acknowledge the strategic planning and budget processes are linked, which is why the library is engaged in an enterprise planning and management (EPM) initiative that strives to better integrate resource and budget planning with performance and risk
management. SPPM's enterprise risk management requirements will be incorporated as the library develops an integrated master schedule for EPM. As the integrated master schedule develops and the library's risk management matures, the Library will refine and update its policies, procedures, and previously drafted model and planning documentation. Finally, we wish to clarify that risk registers are updated according to the applicable planning cycle and, therefore, note that they include risks arising from
fina1 audit recommendations. Accordingly, we object to language in this report suggesting draft audit findings related to Data Center Transformation and IT Modernization were missing from the Library's 2020 Consolidated Risk Register, and, instead, note that those audits were, and remain, in progress so the information you mention was unavailable at the time that the register was created.

The attached spreadsheet provides specific responses and target dates for addressing each of the recommendations. We appreciate your efforts and the opportunity to work together to improve the Library's risk management and internal control processes.
cc: Dianne Houghton, Director. SPPM
Elizabeth Pugh. General Counsel

Management Comments on Draft OIG Report No. 2020-PA-104
Enterprise Risk Management
Management Comments on draft OIG report 2020-PA-104, Enterprise Risk Management

Recommendation followed by Responsible Office followed by Comments and target Completion

1.
SPPM add the establishment of an ERM governing body to its iRIC Improvement Plan and maturity model.
SPPM.
The addition of an executive-level oversight group was included in the iRIC Improvement Plan, released in August 2020, as an improvement for FY22-24. We consider this closed.
Closed.
2.
The Library establish the ERM governing body during the integrated stage of maturity and prior to reaching enterprise-level of maturity.

SPPM.
The addition of an executive-level oversight group was included in the iRIC Improvement Plan, released in August 2020, as an improvement for FY22-24. SPPM expects to meet our timeline for establishing a governing body that aligns with ERM best practices in accordance with the "proactive stage" of the presented maturity model.
Q1 FY22.
3.
The Library designate a Chief Risk Officer (CRO) to lead ERM efforts and to work closely with an ERM governing body to further the movement towards enterprise-level of maturity.
PDL.
A Chief Risk Officer will be named ahead of establishment of the governing body.
Q4 FY21.
4.
The Library incorporates risk considerations into its budgeting and resource approach.
COO/FSD and SPPM.
Risk considerations will be incorporated into the current iRIC framework in FY22, and included in the forthcoming Enterprise Planning & Management system (EPM), which will integrate the Library's planning, performance management, and risk management and internal control workflows with its budgeting and resource allocation decisions.
Q4 FY22.
5.
SPPM provide guidance to the service units on risk appetite and risk tolerance, as well as update the SPPM iRIC Guidance accordingly, even while SPPM s future-state efforts regarding risk appetite and risk tolerance are developing.
SPPM.
In keeping with its improvement plan, SPPM has already undertaken development of the Library's enterprise Risk Appetite Statement, and is on track for planned completion, approval, and integration into iRIC guidance in FY22.
Guidance will be released during the FY22-23 risk refresh to help service units understand the concepts of risk appetite and tolerance, and how to apply the concepts to their work.
Q3 FY22.
6.
SPPM work with the service units to gain a further understanding of risks not being reported into COMPASS, in order to achieve a broader application of a portfolio view of internal and external risks.
SPPM.
As part of its plan to mature to a full ERM, iRIC will expand from the current set of APG and KBP-related risks to include risks currently addressed and reported through other structures into the central risk framework. This expansion will be enabled by the forthcoming EPM.
Q4 FY23.
7.
SPPM revisit LCRs or LCDs to ensure any adjustments made to risk identification in the system be captured.
SPPM.

SPPM will review appropriate LCRs and LCDs and other guidance and supports to ensure risk identification adjustments are captured.
Q1 FY24.
8.
SPPM revisit the concept of Out of Scope risks in the context of the draft maturity model as of August 2020, which indicates an enterprise-level approach towards risk SPPM.
SPPM has removed this concept from its guidance and training. We consider this accepted and closed.
Complete.
9.
SPPM define a path in its iRIC Improvement Plan regarding how to identify Library-wide risks in the context of the draft maturity model as of August 2020, which indicates an enterprise-level approach towards risk management as a key milestone
between FYs 2020 and 2021.
SPPM.
SPPM will define the path before the close of FY21.
Q4 FY21.
10.
SPPM use the GAO Fraud Risk Framework components as a guide for creating an internal fraud risk framework.
SPPM.
SPPM will use the GAO Fraud Risk Framework as a guide for further incorporating its fraud risk into its risk
management program.
Q3 FY22.
11.
SPPM incorporate a fraud risk framework into their existing iRIC program.
SPPM.
Elements of the GAO Fraud Risk Framework will be incorporated into the existing iRIC program. There are preexisting structures and processes within the Library that satisfy many elements of the GAO Fraud Risk
Framework. These will be formally detailed in iRIC guidance and support documents, and included as part of iRIC training.
Q4 FY22.
12.
SPPM revisit the future-state dashboard and determine how to incorporate the dashboard.
SPPM.
SPPM concurs with this recommendation with respect to the future state dashboard. The iRIC dashboard is currently under development.
Q1 FY22.

Footnotes:
1. COSO Enterprise Risk Management, Integrating with Strategy and Performance, Executive Summary, June 2017
2. The ERM Playbook titled Enterprise Risk Management for the U.S. Federal Government (the Playbook), dated July 2016 serves as a key foundational guidance for the Library iRIC. The Chief Financial Officers Council (CFOC) and the Performance

Improvement Council (PIC) released the ERM Playbook on July 29, 2016, to help government departments and agencies meet the requirements of the revised OMB Circular A-123 and provide high-level concepts for consideration when establishing a comprehensive and effective ERM program.
3. OIG s draft Data Center Transformation Executive Summary; 2. IT Modernization Evaluation Report dated August 14, 2020, Obsidian Draft Report