Board of Governors of the Federal Reserve System

The Board's Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced

OIG

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Executive Summary, 2021-IT-B-011, September 15, 2021

The Board's Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced

Findings

Overall, we found that the Board of Governors of the Federal Reserve System continues to take steps to develop and implement an enterprise risk management (ERM) program. Specifically, the Board is performing several foundational ERM activities within the Office of the Chief Operating Officer (OCOO) with the goal of establishing core ERM capabilities before agencywide rollout. For instance, the agency's ERM team is collaborating with each of the divisions operating under the OCOO to perform risk assessments, identify the risk universe, and develop a risk profile. Further, the agency has established an interim risk committee to serve as a temporary forum for enterprise risk discussions.

We identified opportunities to enhance the agency's planning, governance, and implementation of its ERM program and processes. With respect to planning, the Board could benefit from an assessment of the risk management practices and risk culture currently in place across the agency. Further, the establishment of an effective governance structure should help ensure that risk management roles and responsibilities are carried out effectively. Lastly, an early-stage ERM framework would assist in obtaining the executive-level support and division-level buy-in needed to effectively implement ERM agencywide.

Our report also includes two matters for management's consideration: one regarding the definition of requirements for a Boardwide governance, risk, and compliance tool and one regarding the use of a federal best practice, where appropriate, to strengthen the agency's ERM program.

Recommendations

This report includes three recommendations and two matters for management's consideration related to the foundational aspects of the Board's ERM program. In its response to our draft report, the Board concurs with our recommendations and outlines actions that have been or will be taken to address them. We will follow up to ensure that the recommendations are fully addressed.

Purpose

Our evaluation objective was to assess the effectiveness of the Board's ongoing efforts to plan, develop, and integrate ERM processes across the agency. Specifically, this evaluation focused on (1) the establishment of supporting ERM governance and operational structures and (2) steps taken to cultivate a risk culture that aligns the risk management program with the Board's mission, vision, strategy, and values.

Background

As the central bank of the United States, the mission of the Board is to foster the stability, integrity, and efficiency of the nation's monetary, financial, and payment systems. To carry out its mission effectively, the Board must implement processes to identify, assess, respond, and report on internal and external risks. To better manage the full spectrum of internal and external risks, federal agencies, including the Board, are increasingly implementing ERM. ERM refers to an agencywide approach to addressing the full spectrum of an organization's significant risks by considering them as an interrelated portfolio rather than within silos.

Recommendations, 2021-IT-B-011, September 15, 2021

The Board's Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced

Finding 1: A Comprehensive Assessment of Division-Level Risk Management Practices and Culture Could Facilitate Successful Adoption and Implementation of ERM

Number	Recommendation	Responsible office
1	Work with Board divisions to conduct an assessment of the current risk management practices and risk culture across the agency and use the results to inform the direction of the Board's ERM program.	Office of the Chief Operating Officer

Finding 2: Establishment of an Optimal Governance Structure and Reporting Relationships Could Facilitate Boardwide Adoption of ERM

Number	Recommendation	Responsible office
2	Work with the administrative governor, as appropriate, to determine an optimal governance structure and associated reporting relationships for the agency's ERM program and update the *Delegations of Administrative Authority* accordingly.	Office of the Chief Operating Officer

Finding 3: An Early-Stage Framework Could Help Communicate the Vision for an ERM Program

Number	Recommendation	Responsible office
3	Develop and use an early-stage ERM framework to inform broader adoption of ERM across the Board.	Office of the Chief Operating Officer

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

MEMORANDUM

DATE: September 15, 2021

TO: Patrick J. McClanahan
Chief Operating Officer
Board of Governors of the Federal Reserve System

FROM: Peter Sheridan *Peter Sheridan*
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2021-IT-B-011: *The Board's Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced*

We have completed our report on the subject evaluation. We conducted this evaluation to assess the effectiveness of the Board of Governors of the Federal Reserve System's ongoing efforts to plan, develop, and integrate enterprise risk management (ERM) processes across the agency. Specifically, this evaluation focused on (1) the establishment of supporting ERM governance and operational structures and (2) steps taken to cultivate a risk culture that aligns the risk management program with the Board's mission, vision, strategy, and values. We will use the results of this evaluation to help meet our responsibilities under the Federal Information Security Modernization Act of 2014, which requires each agency inspector general to perform an annual independent evaluation of the information security program and practices of their respective agency.

Our report contains recommendations related to the foundational aspects of the Board's ERM program. We provided you with a draft of our report for review and comment. In your response, you concur with our recommendations and outline actions that have been or will be taken to address them. We have included your response as appendix C to our report.

We appreciate the cooperation that we received from Board and Federal Reserve System personnel during our review. Please contact me if you would like to discuss this report or any related issues.

cc: Sharon Mowry
Ricardo A. Aguilera
Cheryl Patterson
Raymond Romero
Charles Young
Nicole Bynum
Winona H. Varnon

Andrew Leonard
Matthew J. Eichner
Lawrence Mize
Jeffrey Marcus

Contents

Introduction

Objective

Our evaluation objective was to assess the effectiveness of the Board of Governors of the Federal Reserve System's ongoing efforts to plan, develop, and integrate enterprise risk management (ERM) processes, including the establishment of supporting governance structures, across the agency in accordance with best practices and guidelines. To meet our objective, we reviewed the progress the Board has made to implement an ERM program. Our scope and methodology are detailed in appendix A.

Background

As the central bank of the United States, the mission of the Federal Reserve System is to foster the stability, integrity, and efficiency of the nation's monetary, financial, and payment systems. As the governing body of the System, the Board conducts the nation's monetary policy, promotes the stability of the financial system, and promotes the safety and soundness of individual financial institutions. To carry out its mission effectively, the Board, similar to other federal agencies, must implement processes to identify, assess, respond, and report on internal and external risks.

Risk is commonly defined as the effect of uncertainty on an organization's objectives and is measured as a function of the likelihood of an event occurring and its impact. *Risk management* refers to a series of coordinated activities to direct and control challenges or threats to achieving an organization's goals and objectives. To better manage the full spectrum of an organization's internal and external risks, federal agencies, including the Board, are increasingly implementing ERM.[1] *ERM* refers to an agencywide approach to addressing the full spectrum of an organization's significant risks by considering them as an interrelated portfolio rather than within silos. An effective ERM program provides several benefits, including

- improved decisionmaking through a structured understanding of opportunities and threats

- a culture of better understanding, disclosure, and remediation of agency risks

- more effective prioritization and allocation of resources

Several frameworks and resources exist for organizations seeking to establish a comprehensive and effective ERM program. One such framework is the Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM Integrated Framework, which is being used by both the Board and the System. Figure 1 depicts the five interrelated components of the COSO ERM Framework: *governance and culture*; *strategy and objective setting*; *performance*; *review and revision*; and *information, communication, and reporting*.[2]

---

[1] Office of Management and Budget, Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2016.

[2] The COSO ERM Framework was updated in 2017 to address the evolution of ERM and the need for organizations to improve their approaches to managing risk to meet the demands of an evolving business environment.

Figure 1. COSO ERM Integrated Framework

Source: COSO *Enterprise Risk Management—Integrating with Strategy and Performance*.

ERM at the Board

Initiated by the chief operating officer (COO) in 2016, the Board continues to take steps across each of the COSO ERM Framework components to establish an ERM program. Figure 2 provides an overview of the key activities the Board has undertaken since 2017 to mature its ERM program. Notably, in January 2017, the Board hired a senior adviser to provide strategic direction for, and oversight of, the design and implementation of the agency's ERM program. At that time, the Board's *Delegations of Administrative Authority*, which establishes which Board employees are authorized to carry out the agency's internal administrative functions, gave each division director the responsibility and authority for formulating, approving, and implementing policies, such as risk management, in their respective divisions. However, in October 2018, these delegations were updated to provide authority over specific policy areas to select division directors while delegating primary responsibility and authority for the implementation of policy areas to the Office of the Chief Operating Officer (OCOO).[3]

As part of the OCOO's efforts to begin an early-stage implementation of ERM, the Senior Officer Committee (SOC) was designated as the agency's interim risk committee in November 2018. The SOC, which is composed of a deputy director or officer from each of the Board's divisions, has served as a temporary forum for enterprise risk discussions since 2018 and has promoted coordination and alignment of the Board's various risk management efforts.

---

[3] The Board's *Delegations of Administrative Authority* was most recently updated in January 2021; however, this update did not change the COO's responsibility or authority for the implementation of policy areas, such as risk management.

Figure 2. Key Steps Taken by the Board to Mature Its ERM Program


Source: OIG analysis.

Additionally in 2018, the COO initiated an approach to pilot ERM within one of the divisions in the OCOO. This effort included the development of a division-level risk profile, which is used to identify significant risks and options to address them.[4] In 2020, the COO established a formal ERM team, which consists of three team members, to expand the ERM proof of concept, beginning with the remaining two OCOO divisions. Board officials informed us in June 2021 that risk profiles for all divisions under the OCOO are in progress. ERM team officials informed us that they plan to expand this effort to include critical business processes across all Board divisions, with the eventual goal of developing an organizationwide risk profile.

As shown in figure 3, the COO is directly responsible for three divisions and reports to the Board of Governors, as do the directors of the remaining Board divisions. As such, successful implementation of ERM at the Board will require the COO to obtain buy-in and create partnerships with divisions that do not report to him. We have previously made a recommendation that remains open for the COO to ensure that an optimal ERM governance structure and strategy are implemented at the Board.[5] Board officials informed us that given the Board's organizational structure, they hope to use the ERM pilot approach within the OCOO to refine ERM processes, communicate program components, and obtain division- and executive-level support to further the rollout of the program.

---

[4] As noted in Office of Management and Budget Circular A-123, a key purpose of a risk profile is to provide a comprehensive analysis of the risks an agency faces in achieving its strategic objectives and arising from its activities and operations. The risk profile assists in facilitating a determination around the aggregate level and types of risk the agency and its management are willing to assume.

[5] Office of Inspector General, *2017 Audit of the Board's Information Security Program*, OIG Report 2017-IT-B-018, October 31, 2017.

Figure 3. The Board's Organizational Structure
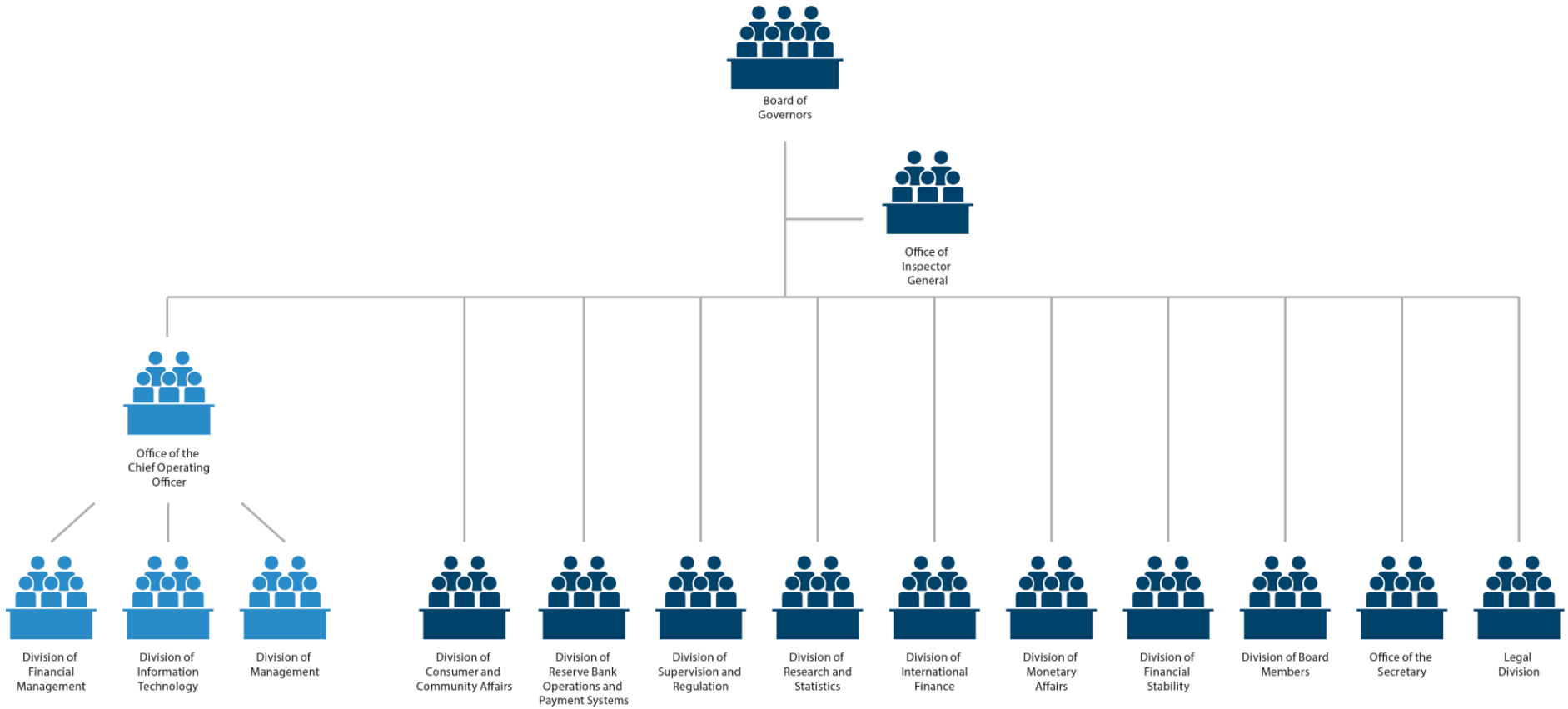
Source: OIG representation.

Summary of Findings

As we noted above, the Board has taken several steps to implement an ERM program that is modeled after the COSO ERM Framework. However, the agency's program is still in the early stages of implementation and efforts to date have largely been focused on operational risk within the divisions operating under the OCOO. Given the early state of the Board's implementation, we analyzed the agency's progress in establishing an ERM program against the Gartner® *ERM Foundations—Implementation Guidance to Build an ERM Program* report.[6] This document provides best practices for organizations to consider in the early stages of establishing an ERM program. Some of these include those modeled after the COSO ERM Framework.

Specifically, this guidance provides practices, approaches, and tools to support four key early-stage ERM priorities: engaging stakeholders, establishing ERM governance, accelerating ERM leader effectiveness, and executing the ERM life cycle (figure 4).

Across these four priorities, Gartner has identified key actions, or milestones, that are critical to establishing effective ERM programs. These actions range in scope from developing an initial risk framework to identifying the best way to perform an initial risk assessment and are designed to help organizations overcome challenges and avoid pitfalls when creating and maturing an ERM program.

Figure 4. Key Early-Stage ERM Priorities

Source: Gartner, *ERM Foundations*, Enterprise Risk Management Research Team, refreshed September 21, 2020, published October 11, 2013.

We identified opportunities within each of the four early-stage ERM priority areas to enhance the Board's ERM program. Specifically, with respect to engaging stakeholders, we found that the Board has not performed a complete assessment of the risk management practices and culture currently in place throughout each of the agency's divisions. Concerning establishing ERM governance, we noted that the Board has not yet established an effective governance structure for its ERM program. Regarding accelerating ERM leader effectiveness, we found that the Board has not formally developed an early-stage ERM framework. Lastly, with respect to executing the ERM life cycle, we noted that the Board has not yet defined its requirements for a governance, risk, and compliance (GRC) tool to support the organization's ERM program.

---

[6] Gartner, *ERM Foundations*, Enterprise Risk Management Research Team, refreshed September 21, 2020, published October 11, 2013. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the United States and internationally and is used herein with permission. All rights reserved.

Finding 1: A Comprehensive Assessment of Division-Level Risk Management Practices and Culture Could Facilitate Successful Adoption and Implementation of ERM

We found that the Board has not performed a complete assessment of the risk management practices and culture across the agency. Performing such an assessment as a means to engage stakeholders and understand risk management processes and culture across the organization is one of the best practices outlined by Gartner. Agency officials involved in the Board's ERM effort informed us that a complete assessment of risk management practices has not yet been performed for all Board divisions because of a strategic decision to first pilot ERM concepts within the OCOO. These officials also informed us that they plan to complete such an assessment as they continue to engage with divisions across the Board. We believe that an understanding of the current risk management practices and culture within each of the agency's divisions can help identify lessons learned and practices that can be leveraged to successfully implement ERM Boardwide.

Division-Level Risk Management Practices

We found that the Board has not completed an assessment of the risk management practices and culture across the agency. As part of its current strategy, the Board is focusing on piloting ERM concepts and processes within the divisions that compose the OCOO and then using this information to obtain executive-level buy-in and inform broader adoption. Specifically, the agency's ERM team, which consists of three individuals within the OCOO, is piloting ERM concepts and practices within the divisions that are under the COO's purview. This includes gathering baseline information about risk management practices, methodologies, authorities, and escalation procedures, as well as the development of risk profiles. The agency's ERM team informed us that risk management maturity and practices vary across Board divisions. The team also informed us that they plan to perform a broader assessment of risk management practices across Board divisions once they complete the ERM pilot and obtain executive-level approval of their planned approach.

As highlighted above in figure 4, the Gartner *ERM Foundations* report notes that one of the key priorities in establishing a strong foundation for an ERM program is the engagement of stakeholders. Specifically, the guidance notes that the engagement of functional leaders who direct risk and control processes throughout the organization will help with the integration of ERM across the agency. One of the actions recommended to support this priority is to analyze how the organization currently performs risk management activities by taking stock of each division's current risk processes.

As noted earlier, the Board is composed of various divisions (for example, the Division of Supervision and Regulation, the Division of Research and Statistics, and the Division of Reserve Bank Operations and Payments Systems) that support the mission of the agency. We recognize that some divisions, such as the research divisions, have policy-driven risks that differ from those of the Federal Reserve Banks and the

Board's operational divisions. However, we believe that an understanding of current risk processes across these divisions can help the ERM team expand the program beyond the operational divisions under the OCOO. Further, we believe that this information can help the ERM team adapt its approach to risk assessments and inform the types of support it can provide throughout the agency.

Division-Level Risk Culture

As the Board's ERM team gains a better understanding of risk management practices across the agency, we believe that the team can also gather valuable information on the risk culture that exists within each division.[7] The Gartner implementation guidance notes that as part of the process to build buy-in from [division-line] management, it is important for an ERM team to not only communicate the program's value but to also understand the risk culture already in place within the agency's business units.

To better understand the implementation of ERM at the Board, we conducted a survey of SOC members (appendix B). Based on this survey, we found that answers varied by agency division in response to questions regarding risk culture. Specifically, with regard to risk culture, our survey asked if SOC members agreed with the following three statements:

1. The agency maintains an appropriate balance between taking and managing risks (question 9 in appendix B).

2. There is a culture of risk awareness, transparency, and openness, which encourages employees to identify, discuss, report, and escalate potential risks (question 10 in appendix B).

3. The agency actively seeks to embed risk management as a component in all critical decisions throughout the agency (question 11 in appendix B).

Our survey results found that indicators regarding the agency's risk culture averaged 3.18 out of 5.00 (figure 5). These results on risk culture are similar to those of surveys conducted by the Association for Federal Enterprise Risk Management (AFERM), a professional organization dedicated to the advancement of federal ERM that has collaborated with Guidehouse to survey federal government leaders and staff for their insights into the current state of ERM in their organizations.[8] The 2020 AFERM survey results found that culture is one of the key barriers facing organizations attempting to establish and maintain formal ERM programs. While we found that the Board's results on risk culture were higher, on average, than the AFERM survey results (figure 5), we believe that an assessment of risk culture throughout the Board divisions will help identify ways that these risk culture indicators can be improved.

---

[7] According to the Institute of Risk Management, *risk culture* refers to the values, beliefs, knowledge, attitudes, and understanding about risk shared by a group of people with a common purpose. See Institute of Risk Management, *Risk Culture— Under the Microscope: Guidance for Boards*, 2012, p. 7, https://www.theirm.org/media/8447/risk_culture_a5_web15_oct_2012-executive-summary.pdf.

[8] In the most recent survey conducted by AFERM and Guidehouse in 2020, responses were received from a total of 37 department-level federal organizations, including all 15 cabinet agencies. See Guidehouse, Federal Enterprise Risk Management 2020 Survey Results, https://guidehouse.com/insights/advanced-solutions/2020/aferm-survey-results-2020.

Figure 5. ERM Survey Culture Indicators

	The agency maintains an appropriate balance between taking and managing risks.	There is a culture of risk awareness, transparency, and openness, which encourages employees to identify, discuss, report, and escalate potential risks.	The agency actively seeks to embed risk management as a component in all critical decisions throughout the agency.
5 - Strongly agree			
4 - Agree	Board: 3.05	Board: 3.19	Board: 3.29
3 - Neither agree nor disagree	2.76 / 2.70	3.28 / 3.23	3.05
2 - Disagree	2.37 / 2.47	2.93 / 2.96	2.63 / 2.88 / 2.93
1 - Strongly disagree			
	2017 2018 2019 2020	2017 2018 2019 2020	2017 2018 2019 2020

Source: OIG analysis of 2020 OIG survey results and AFERM survey results from 2017–2020.

We recognize the value provided by the Board's current approach to ERM, which is to use lessons learned within the COO divisions to inform broader agency adoption. We believe that an understanding of the current risk management practices and culture in place within each of the Board's divisions could identify additional lessons learned and best practices that can be leveraged as the agency continues to mature its ERM program. In addition, such an understanding could facilitate continued engagement with, and buy-in from, division leadership as well as provide insight into the risk culture across the Board.

Recommendation

We recommend that the COO

1. Work with Board divisions to conduct an assessment of the current risk management practices and risk culture across the agency and use the results to inform the direction of the Board's ERM program.

Management Response

The Board's COO concurs with our recommendation and notes that the agency's ERM team has been learning about and assessing the risk management practices of the divisions under the COO's purview as they implement the program. Further, the COO noted that administering a survey assessment across the agency would help inform the program's direction by garnering more information on risk management

understanding, current practices, and readiness for ERM. The ERM team has already begun drafting a survey and discussing the optimal audience for it.

OIG Comment

We believe that the actions described by the COO are responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed.

Finding 2: Establishment of an Optimal Governance Structure and Reporting Relationships Could Facilitate Boardwide Adoption of ERM

We found that the Board has not yet established an effective ERM governance structure and associated reporting relationships for its ERM program, which are foundational priorities identified in the Gartner *ERM Foundations* report. Further, we also found that responsibility for ERM has not been clearly defined in the agency's *Delegations of Administrative Authority*. Agency officials involved in the Board's ERM effort informed us that they decided to leverage the SOC as the agency's interim risk committee because they did not want to create a new governance structure until the ERM program was more mature. In addition, these officials noted that given the current organizational structure at the Board, there is no one position within the agency to serve as a chief risk officer (CRO) or an equivalent function. We believe that the Board's ERM implementation would benefit from a determination of the optimal governance structure and reporting relationship for the program in order to ensure that all necessary risk management roles and responsibilities are carried out effectively.

ERM Governance and Reporting Relationships at the Board

We found that the Board has not yet established an effective governance structure or determined the optimal reporting relationships for its ERM program. Specifically, we found that while the SOC was designated as the agency's interim risk committee in 2018, it is not performing all the roles and functions recommended of a risk committee. Further, we also found that responsibility for ERM has not been clearly defined in the agency's *Delegations of Administrative Authority*. We have previously reported on the challenges in implementing enterprisewide initiatives, such as ERM, given the Board's decentralized governance structure.[9] For example, while the COO has authority to create binding policies for all divisions, he does not always have mechanisms to ensure that those divisions comply with such policies. In addition, the COO does not have a line of sight into the nonadministrative divisions and therefore may not know the extent to which these divisions are complying with policies.

The Board has established committees designed to facilitate information sharing and coordination across the agency—most notably, the Executive Committee (EC) and the SOC. The EC is composed of the Board's division directors and is chaired by the COO. The EC's purpose is to advise the governors and the chair. As noted earlier, the SOC is composed of a deputy director or officer appointed by each of the Board's division directors; the SOC serves as an advisory committee, providing recommendations on internal administrative issues and functioning as a forum for risk discussions, for the EC. While the SOC has been

---

[9] Office of Inspector General, *The Board's Organizational Governance System Can Be Strengthened*, OIG Report 2017-FMIC-B-020, December 11, 2017.

discussing the status of the Board's ERM program, as required by the group's charter, it has not provided guidance on the organization's risk governance structure and framework, its risk appetite statement, or the effectiveness of its risk monitoring. These recommended practices are defined in the Chief Financial Officer Council's *Playbook: Enterprise Risk Management for the U.S. Federal Government*.[10]

We also benchmarked the EC and SOC charters with those serving equivalent functions within the System—the Risk Management Committee (RMC) and the Subcommittee on Operational Risk Management (SORM), respectively.[11] As a result of this benchmarking effort, we noted that the Board's risk committee charters were missing several key components (table 1). In addition, we found that the Board's risk committees performed self-assessments less often and met less frequently than the System's risk committees.

Table 1. Benchmarking of the Alignment of Board and System Risk Committees

Charter element	Definition	Board committees		System committees	
		EC	SOC	RMC	SORM
Purpose	The purpose as a risk committee is defined.	○	○	●	●
Authority	The committee has the authority to make and enforce risk management decisions.	○	○	●	●
Composition	The committee is composed of senior leaders in all division/offices.	●	●	●	●
Responsibilities	Specific key risk management responsibilities and activities are defined.	○	○	●	●

Source: OIG analysis of Board and System committee charters and best practices.
Note: ● aligns, ○ does not align.

---

[10] Chief Financial Officers Council, *Playbook: Enterprise Risk Management for the U.S. Federal Government*, July 29, 2016, https://www.cfo.gov/wp-content/uploads/2016/07/FINAL-ERM-Playbook.pdf.

[11] Our reference to the System is intended as a benchmark for operational risk management.

Our survey results also highlight the importance of establishing an effective governance structure and reporting relationships for ERM. For example, our survey found the following:

- Over half of SOC members disagreed that the organizational structure at the Board is such that there are clear lines of responsibility and authority for risk management (question 5 in appendix B).

- Almost half of all SOC members disagreed that the role of the SOC in ERM is clear (question 6 in appendix B). The only members that agreed with this statement are those directly involved in the Board's ongoing ERM implementation.

- No one from the SOC disagreed with the idea that the agency's ERM program would benefit from an executive-level position, such as a CRO, responsible for the success of the program (question 14 in appendix B).

- The Board's organizational structure was listed as one of the top three challenges associated with implementation of the Board's ERM program (question 19 in appendix B).

The Gartner *ERM Foundations* report notes the importance of establishing ERM governance and, more specifically, a risk committee as a platform for risk owners to meet and discuss risk-related issues. The guidance also highlights the responsibilities assigned to an agency's risk committee, such as coordinating decisionmaking, prioritizing risk conversations for senior leadership, aligning risk responses to overall organization strategies and objectives, reviewing the suitability of risk management processes and risk responses, and monitoring the performance of ERM programs. Gartner also notes that an ERM program's reporting structure can affect its influence and role within an organization.

In December 2020, the Board's ERM team performed a benchmarking exercise on the presence and reporting structure of a CRO position within federal agency ERM programs, focusing primarily on other financial regulators. From this exercise, the ERM team found that CRO is the most common title held by leaders of federal ERM programs at financial regulators. This result aligns with those from the 2020 AFERM survey, which found that federal ERM programs are most commonly led by a CRO (figure 6). The same governance model is leveraged by several of the Reserve Banks as well as the central bank of Canada, with a CRO serving as the executive owner of the ERM program. The reporting model selected can help inform who within the organization is charged with key ERM roles and responsibilities, such as program oversight, establishing an ERM framework, risk monitoring and reporting, and continuous improvement and advancement of the program.

Figure 6. Leaders of Federal ERM Programs
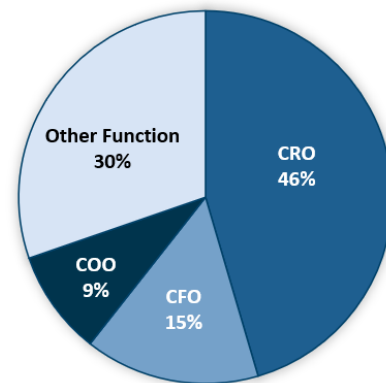
Source: 2020 AFERM federal ERM survey results.

Agency officials noted that given the current organizational structure at the Board, there is no one position within the agency to serve as a CRO or an equivalent function. Further, they noted that the SOC was not intended to perform all the activities of a traditional risk committee. Specifically, the ERM team noted that as the Board's ERM program matures, a separate, more formal risk committee will be established. We believe that the Board's early-stage ERM implementation would benefit from a

determination of the optimal governance structure and reporting relationships for the program in order to ensure that current and future risk management roles and responsibilities are carried out effectively.

Recommendation

We recommend that the COO

> 2. Work with the administrative governor, as appropriate, to determine an optimal governance structure and associated reporting relationships for the agency's ERM program and update the *Delegations of Administrative Authority* accordingly.

Management Response

The Board's COO concurs with our recommendation and notes that as the ERM program matures, the governance structure around it will need to evolve. The COO notes that a new governance body is needed at this point in the ERM implementation and believes that a small risk steering committee would be best to oversee continued implementation, advise the ERM team on program design and methodology, and assist with ERM implementation in the other divisions. As the ERM program matures across the agency, the ERM team will evaluate whether the risk steering committee continues to be the optimal structure or whether a different structure would be more appropriate at that time. The reporting relationships and any updates to the *Delegations of Administrative Authority* will be discussed and assessed with the administrative governor, considering the structure of the Board and its limitations on authorities over divisions.

OIG Comment

We believe that the actions described by the COO are responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed.

Finding 3: An Early-Stage Framework Could Help Communicate the Vision for an ERM Program

While the Board's ERM team has an overall vision for the future state of the agency's ERM program, we found that the team has not formally developed an early-stage framework to inform rollout of the program Boardwide. Once an ERM governance structure and associated reporting relationships have been established, Gartner recommends the use of an early-stage framework to implement and mature an organization's ERM program. Board officials on the ERM team informed us that they are focusing early efforts on divisions operating under the COO before developing a framework that would apply across the agency. However, we believe that the development of an early-stage framework will provide the Board with several benefits, including the executive-level support and division-level buy-in needed to effectively implement ERM agencywide.

Development of an Early-Stage ERM Framework

We found that the Board has not formally developed an early-stage ERM framework to support the agency's implementation of ERM. As highlighted in figure 4, the Gartner *ERM Foundations* report notes that one of the key priorities in establishing a strong foundation for an ERM program is accelerating ERM leader effectiveness to ensure that specific responsibilities are defined and any skill gaps are addressed. As part of accelerating ERM leader effectiveness, Gartner recommends the use of an early-stage ERM framework to strengthen governance and reporting relationships. Specifically, Gartner recommends that the early-stage framework include

- an affirmation of support for ERM by the agency's senior leaders

- a risk management process outline, including guidelines for managing risk assessments, monitoring, and review

- communication guidelines on the frequency and manner of reporting to internal and external stakeholders

- elements of accountability, detailing the responsibilities and any potential performance evaluation criteria for those with ERM-related functions (for example, the risk committee, the head of ERM, risk owners, etc.)

Officials on the Board's ERM team informed us that while they have not formally documented an early-stage ERM framework, the team does have a vision for the future state of ERM at the Board. For example, the team has developed milestones for completing risk profiles across all Board divisions. As part of this effort, the team plans to focus on risk profiles for critical business processes across Board divisions. The ERM team also noted that without formal organizationwide authority for ERM, they have decided to focus their efforts on the divisions operating under the COO before developing a framework that would apply Boardwide. We believe that the development of an early-stage ERM framework will help provide the ERM team with the senior-level support it needs to effectively implement its vision for the program.

We also believe that this framework, taken together with the agencywide risk management assessment and governance determinations we recommended earlier, can provide the Board with additional benefits, including

- a strategic vision to assist with the broader rollout of the ERM program

- identification of goals and objectives for the ERM program

- increased stakeholder engagement

Recommendation

We recommend that the COO

3. Develop and use an early-stage ERM framework to inform broader adoption of ERM across the Board.

Management Response

The Board's COO concurs with our recommendation and notes that the ERM team has incorporated many aspects of the Gartner recommendations for an early-stage framework as part of its ERM program design and implementation efforts. The COO notes that formalizing this information would be beneficial to the continued implementation of the ERM program, and the ERM team has already begun drafting a formal document to be used as a framework now, which will be updated, as appropriate, as the program matures.

OIG Comment

We believe that the actions described by the COO are responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed.

Matters for Management Consideration

We identified two matters for management consideration: one related to ensuring that requirements for a GRC tool to support the execution of the ERM life cycle are defined and one related to determining whether to voluntarily adopt components of Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, as part of the agency's implementation of ERM. While we are not making formal recommendations in these areas, we will continue to monitor the Board's progress in maturing its ERM program.

Defining Requirements for a GRC Tool

While we understand that the Board's ERM program is in the early stages of implementation, we noted that the Board has not fully defined requirements for a GRC tool to support the execution of the ERM life cycle. The Board's ERM team has tested the GRC tool supporting the agency's internal control activities and participated in several vendor demonstrations of alternate tools. ERM team officials notified us that, at this early stage of implementation, they are primarily using Microsoft Excel to support the ERM program and intend to continue that approach until the needs of the program and its stakeholders are sufficiently defined. These officials also noted that once these needs are defined, they intend to select a GRC tool that will support the broader rollout of the agency's ERM program.

As highlighted in figure 4, the Gartner *ERM Foundations* report notes that executing the ERM life cycle is one of the four key priorities in the early stages of an ERM program. The early-stage ERM life cycle includes activities such as identifying the risk universe, selecting a risk assessment methodology, supporting risk mitigation, tracking risk events as they occur, and preparing for ERM reporting. Specifically, Gartner notes that risk tracking can be facilitated by a GRC tool to catalog and record risk events. The Gartner *GRC Success Stories: Making the Most of an Imperfect Solution* report also recommends getting input, support, and consensus upfront from all relevant stakeholders within the organization to ensure that the GRC tool selected will meet the needs of all involved in the ERM process.[12]

The federal ERM survey published by AFERM in 2020 shows similar trends with respect to the implementation of a GRC tool across the government. Specifically, the 2020 AFERM survey results show that 96 percent of federal agencies do not utilize GRC tools for their ERM programs. The survey also shows that the most common technology enablers used by federal ERM programs were Microsoft Excel and SharePoint. Our survey results show that there is broad support for the use of a common GRC tool across the Board. Specifically, the results highlight that the majority of SOC members agree that the Board's ERM program would benefit from the use of standard tools, technologies, and processes for risk management (question 16 in appendix B). We believe that partnering with Board stakeholders to define all necessary requirements for a GRC tool during early-stage implementation of the ERM program will help facilitate the successful implementation of a long-term solution for the Board. We understand that effective implementation of an agencywide GRC tool will rely on further maturity of the Board's ERM

---

[12] Gartner, *GRC Success Stories: Making the Most of an Imperfect Solution*, Enterprise Risk Management Research Team, refreshed May 5, 2020, published November 13, 2018.

program and related processes. As the agency's ERM program matures, we suggest that management work with Board divisions to define the requirements for and select a GRC tool that meets stakeholders' needs. While we are not making a formal recommendation, we will continue to monitor the agency's progress in this area.

Formally Leveraging OMB Circular A-123 in the Board's ERM Program

We also identified a matter for management's consideration regarding the use of OMB Circular A-123 with respect to the Board's ERM program. Congress passed the Federal Managers' Financial Integrity Act of 1982 (FMFIA) to enhance the management of federal government operations through improved internal control. In accordance with FMFIA, OMB issued implementation guidance in an update to OMB Circular A-123, then titled *Management's Responsibility for Internal Control*.

The Board is not required to comply with FMFIA because it is a financially related statute that is made inapplicable to the Board by section 10 of the Federal Reserve Act.[13] However, while the Board has voluntarily decided to comply with FMFIA, the agency made a formal determination in 2006 that OMB Circular A-123 does not apply. Since this determination, OMB Circular A-123 was updated in July 2016 to require executive agencies to implement an ERM capability that is coordinated with the strategic planning and review processes of the agency. The circular notes that nonexecutive agencies, such as the Board, are also encouraged to adopt it. Another independent government agency, the Federal Deposit Insurance Corporation, has stated that it seeks to comply with the spirit of OMB Circular A-123 with respect to its ERM program.[14] However, we found that the Board has not determined whether components of the revised OMB Circular A-123 would be beneficial to voluntarily adopt as part of its implementation of ERM.

The Board's ERM team informed us that they have incorporated several components of OMB Circular A-123 into their ERM approach. However, these officials noted that they are hesitant to leverage the circular as a mandate for ERM because they do not want the program to become a compliance-focused activity. We believe that a decision to formally leverage ERM-related elements of OMB Circular A-123 could help ensure a more effective implementation of key ERM program components. While we are not making a formal recommendation, we will continue to monitor the agency's progress in maturing its ERM program.

---

[13] Section 10 of the Federal Reserve Act empowers the Board to "determine and prescribe the manner in which its obligations shall be incurred and its disbursements and expenses allowed and paid." 12 U.S.C. § 244.

[14] Office of Inspector General, Federal Deposit Insurance Corporation, *The FDIC's Implementation of Enterprise Risk Management*, July 2020.

Additional Takeaways From the OIG's ERM Survey

As noted earlier, we conducted a survey of SOC members or their delegated representatives regarding the current and future states of the agency's ERM program (appendix B). The earlier sections of our report reference our ERM survey results as they relate to risk culture, governance, and the use of standard tools and technologies. Our survey also includes additional takeaways that we believe management should consider as it matures the Board's ERM program. These takeaways are as follows:

- The majority of respondents disagreed that risk information is effectively communicated across the Board (question 7).

- The majority of respondents disagreed or strongly disagreed that the Board prioritizes and manages risk across the organizational structure via an interrelated risk portfolio (question 8).

- The majority of respondents agreed or strongly agreed that the scope of the Board's ERM program should include all the Board's divisions and functions (question 12).

- Almost half of respondents agreed or strongly agreed that it is important to have a defined enterprisewide risk appetite linked to the achievement of the Board's strategic objectives (question 13). [15]

- Respondents disagreed on whether the future state of ERM governance at the Board should include an executive-level position responsible for the success of the program, an enterprise risk committee, or both (questions 14 and 15).

- Almost half of respondents agreed that the Board's ERM program would benefit from the inclusion of ERM-related objectives into the performance management frameworks for Board executives and their divisions/sections (question 17).

- Respondents identified that the top three benefits of an ERM program at the Board are prioritizing and mitigating enterprise risks, supporting a risk-aware culture, and reducing organizational silos and improving information sharing (question 18).

- Respondents identified that the top three challenges to implementing an ERM program at the Board are cultural resistance to change, bridging silos across the organization, and the current organizational structure (question 19).

---

[15] *Risk appetite* is defined as the amount and type of risk that an organization is willing to accept in the pursuit of its mission, vision, business objectives, and overall strategic goals.

Appendix A: Scope and Methodology

Our evaluation objective was to assess the effectiveness of the Board's ongoing efforts to plan, develop, and integrate ERM processes across the agency. Our scope included the steps taken by the Board (1) to establish supporting ERM governance and operational structures and (2) to cultivate a risk culture that aligns the risk management program with the agency's mission, vision, strategy, and values.

To accomplish our objective, we

- reviewed applicable laws, regulations, and best practices, including OMB Circular A-123, the 2017 COSO ERM Framework, federal ERM survey results published by AFERM, and ERM-related best practices published by Gartner

- reviewed publicly available ERM-related resources published by other central banks, including the Bank of Canada and the Bank of England

- interviewed Board and System officials with ERM-related roles

- examined the Board's ERM-related documentation, including committee charters, meeting minutes, organizational charts, and risk profiles

- performed a benchmarking exercise focused on ERM governance and risk culture throughout the System

- conducted a survey of SOC members, or their delegated representatives, regarding the current and future states of the agency's ERM program (appendix B)

Our review focused on the Board's progress in developing the foundations of an ERM program. As noted in our report, the Board's efforts to implement ERM have largely been focused on operational risk considerations within the divisions operating under the OCOO. While this is our first formal evaluation of the Board's ERM program, we plan to perform additional evaluation work in this area as the Board continues to mature its ERM capabilities and expand its program beyond the divisions operating under the OCOO.

We performed our fieldwork from March 2020 to May 2021. We performed our evaluation in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

Appendix B: OIG ERM Survey Results

To better understand the current and future states of the agency's ERM program, we conducted a survey of Board SOC members or their delegates.[16] We developed our survey questions based on a review of templates available on the Gartner *Risk Exchange: ERM Surveys and Interview Guide Library* as well as the annual AFERM federal ERM survey questions and results.[17] The figures below detail the results of our ERM survey.

Current State of ERM at the Board

Question 1: With which of the Board's recent ERM efforts are you familiar and/or involved? Select all that apply.


---
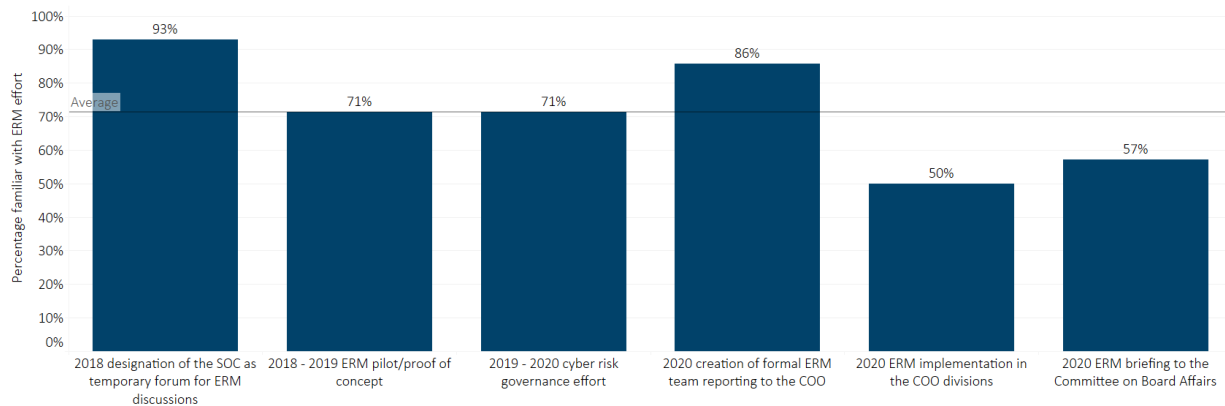
[16] We conducted this survey regarding the current and future states of the Board's ERM program during August–September 2020. Responses were received from all 15 of the Board's divisions. However, officials from 1 division informed us that their responses to survey questions regarding the current state of ERM were based on the Board's cyber risk governance program and not ERM as a whole. Therefore, the responses from this division were excluded except for questions regarding the future state of the agency's ERM program (questions 12–17).

[17] Gartner, *Risk Exchange: ERM Surveys and Interview Guide Library*, Enterprise Risk Management Research Team, refreshed August 6, 2021, published April 18, 2020.

Question 2: Which types of risk does the Board focus its resources on the most? Select all that apply.
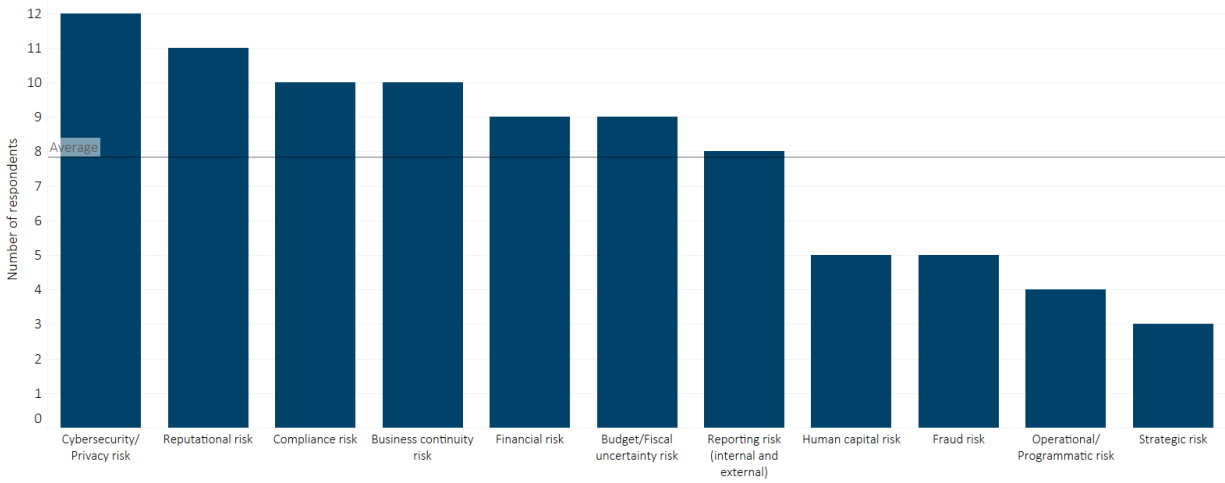
Question 3: Which types of risk pose the greatest threat to the Board's mission and strategic objectives? Select all that apply.
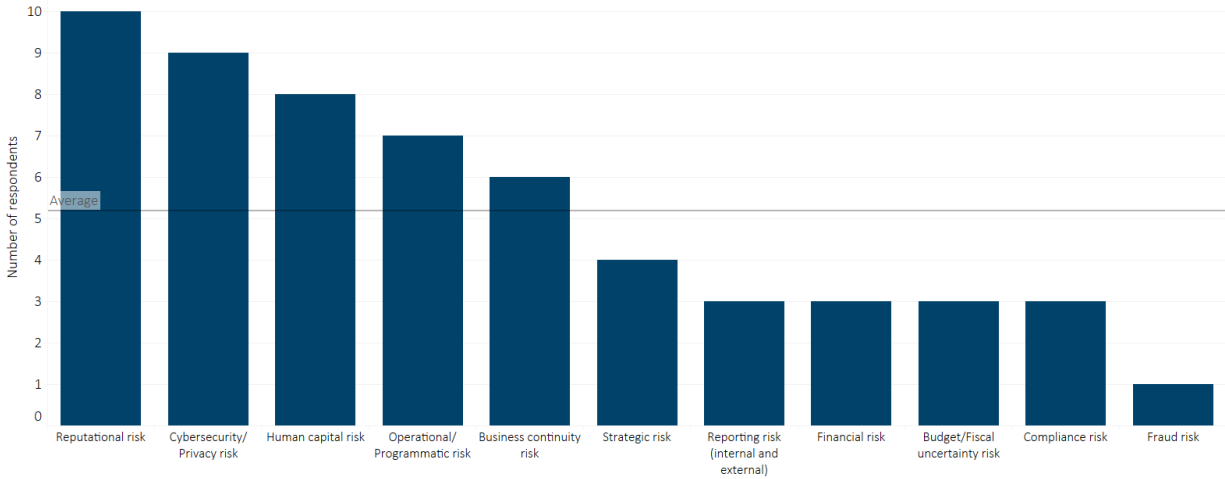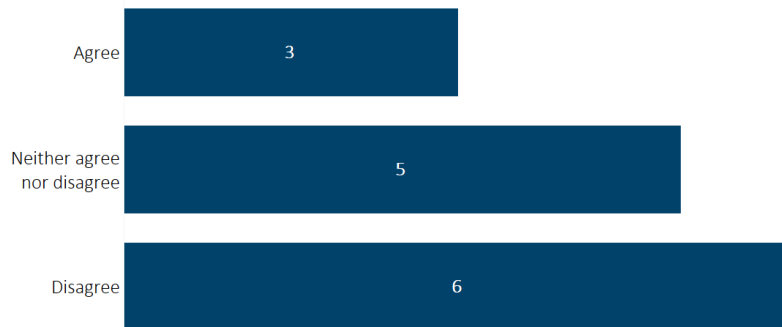
Question 4: Do you agree with the following statement? "The resources (people, processes, and technology) dedicated by the Board to ERM are appropriate."

| Response	Count
Agree	7
Neither agree nor disagree	3
Disagree	4
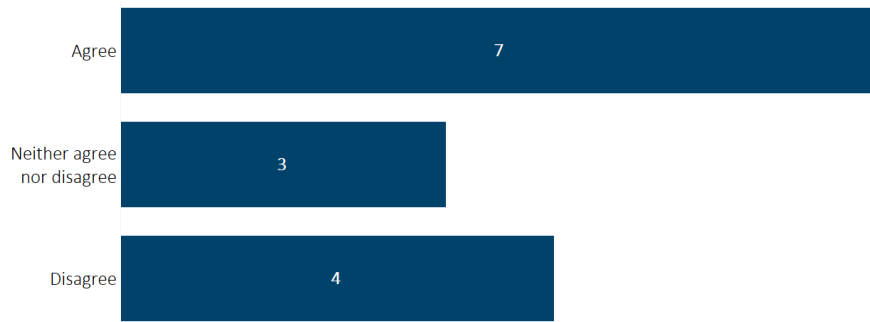
Question 5: Do you agree with the following statement? "The organizational structure at the Board is such that there are clear lines of responsibility and authority for risk management."

Response	Count
Agree	4
Neither agree nor disagree	1
Disagree	7
Strongly disagree	2

Question 6: Do you agree with the following statement? "The role of the Senior Officer Committee in ERM is clear."

Response	Count
Agree	3
Neither agree nor disagree	5
Disagree	6

Question 7: Do you agree with the following statement? "Risk information is effectively communicated across the Board."

| Response	Count
Neither agree nor disagree	4
Disagree	10
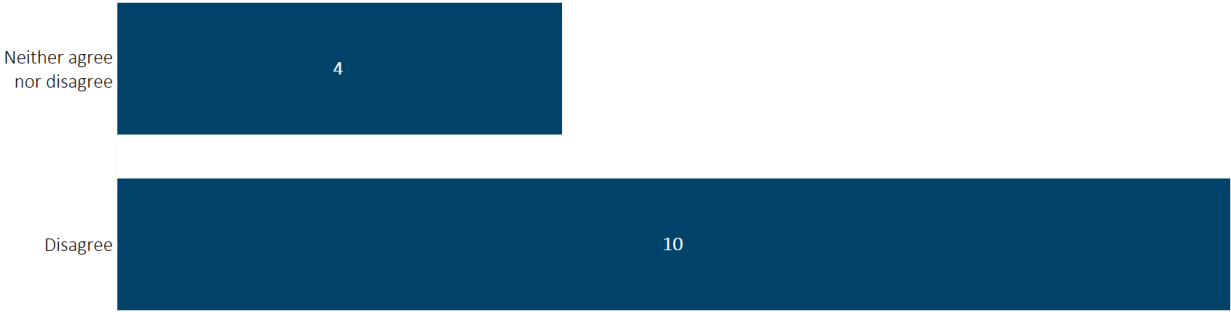
Question 8: Do you agree with the following statement? "The Board prioritizes and manages risk across the organizational structure via an interrelated risk portfolio rather than within individual silos."

Response	Count
Neither agree nor disagree	3
Disagree	9
Strongly disagree	2

Question 9: Do you agree with the following statement? "The Board maintains an appropriate balance between taking and managing risks."

Response	Count
Agree	5
Neither agree nor disagree	4
Disagree	3
Strongly disagree	2

Question 10: Do you agree with the following statement? "At the Board, there is a culture of risk awareness, transparency, and openness, which encourages employees to identify, discuss, report, and escalate potential risks."

| Response	Count
Agree	4
Neither agree nor disagree	6
Disagree	4
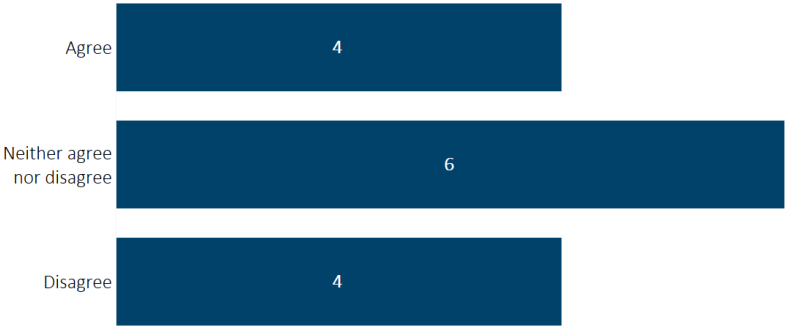
Question 11: Do you agree with the following statement? "The Board actively seeks to embed risk management as a component in all critical decisions throughout the organization."

Response	Count
Agree	6
Neither agree nor disagree	4
Disagree	4
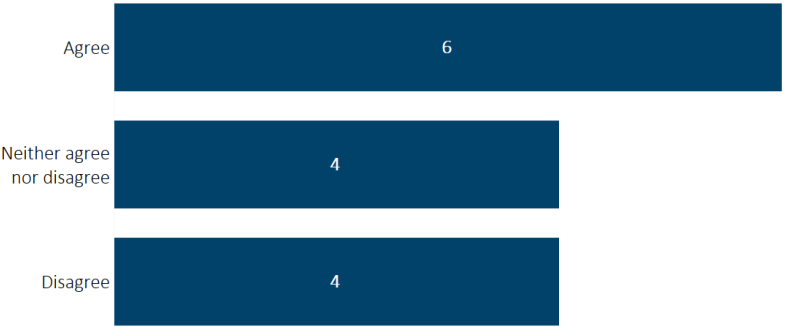
Future State of ERM at the Board

Question 12: Do you agree with the following statement? "The scope of the Board's ERM program should include all of the Board's divisions and functions."

| Response	Count
Strongly agree	9
Agree	4
Neither agree nor disagree	2
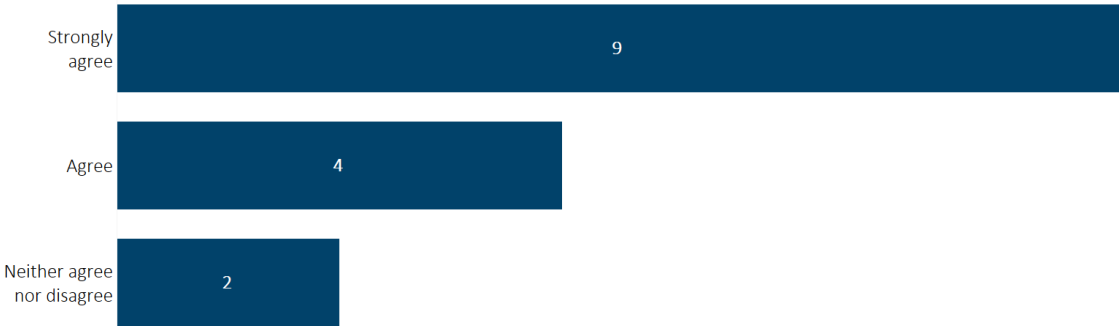
Question 13: Do you agree with the following statement? "It is important to have a defined enterprisewide risk appetite linked to the achievement of the Board's strategic objectives."

| Response	Count
Strongly agree	1
Agree	6
Neither agree nor disagree	4
Disagree	4
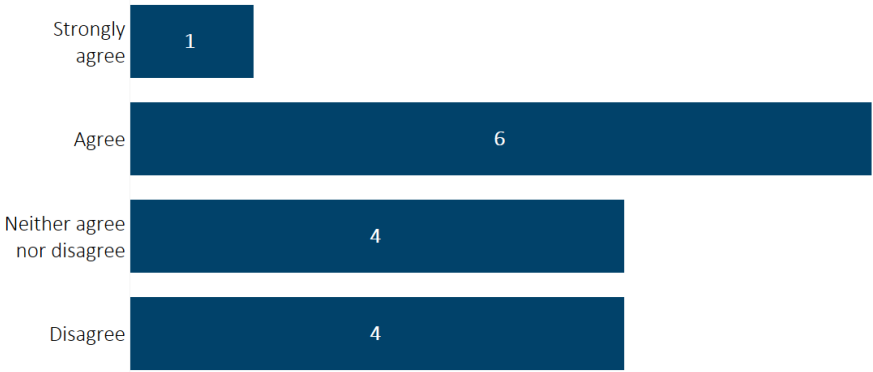
Question 14: Do you agree with the following statement? "The Board's ERM program would benefit from establishing an executive-level position (e.g., a chief risk officer) responsible for the success of the program."

Response	Count
Strongly agree	1
Agree	5
Neither agree nor disagree	9

Question 15: Do you agree with the following statement? "The Board's ERM program would benefit from establishing an executive-level forum (e.g., an Enterprise Risk Committee) to make ERM-specific discussions and decisions."

Response	Count
Strongly agree	1
Agree	5
Neither agree nor disagree	7
Disagree	2
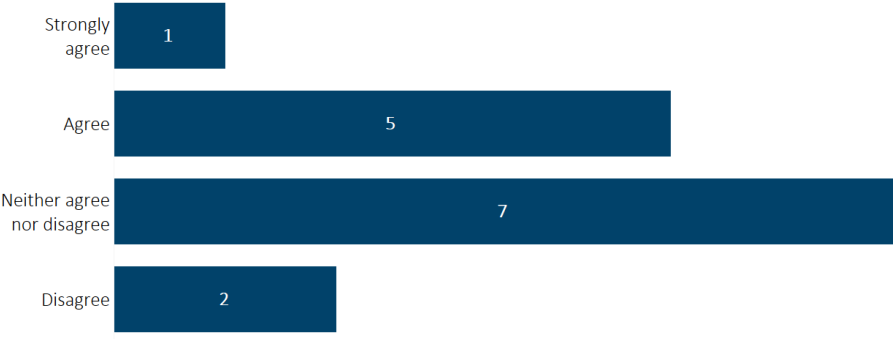
Question 16: Do you agree with the following statement? "The Board's ERM program would benefit from the use of standard tools/technologies and processes for risk management."

| Response	Count
Strongly agree	1
Agree	10
Neither agree nor disagree	2
Disagree	2
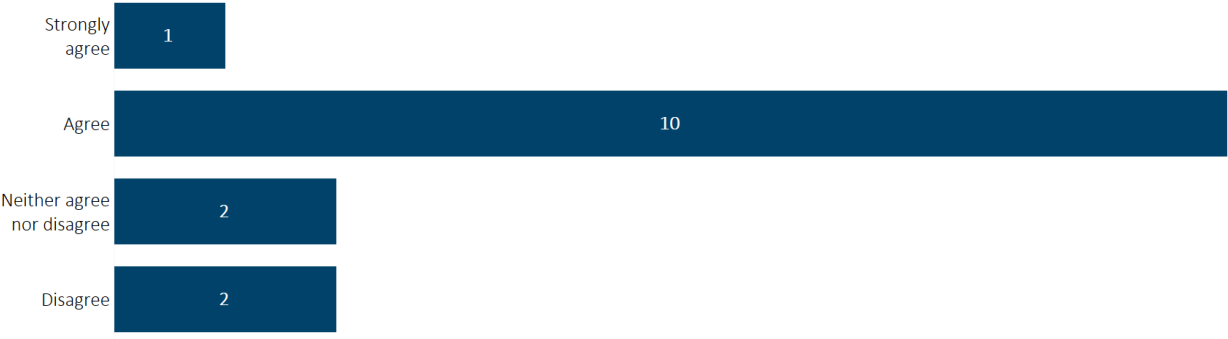
Question 17: Do you agree with the following statement? "The Board's ERM program would benefit from the inclusion of ERM-related objectives into the performance management frameworks for Board executives and their divisions/sections."

Response	Count
Agree	7
Neither agree nor disagree	4
Disagree	4

Benefits and Challenges to ERM at the Board

Question 18: What benefits do you believe will be realized from the implementation of the Board's ERM program? Please rank your top 5 answers.
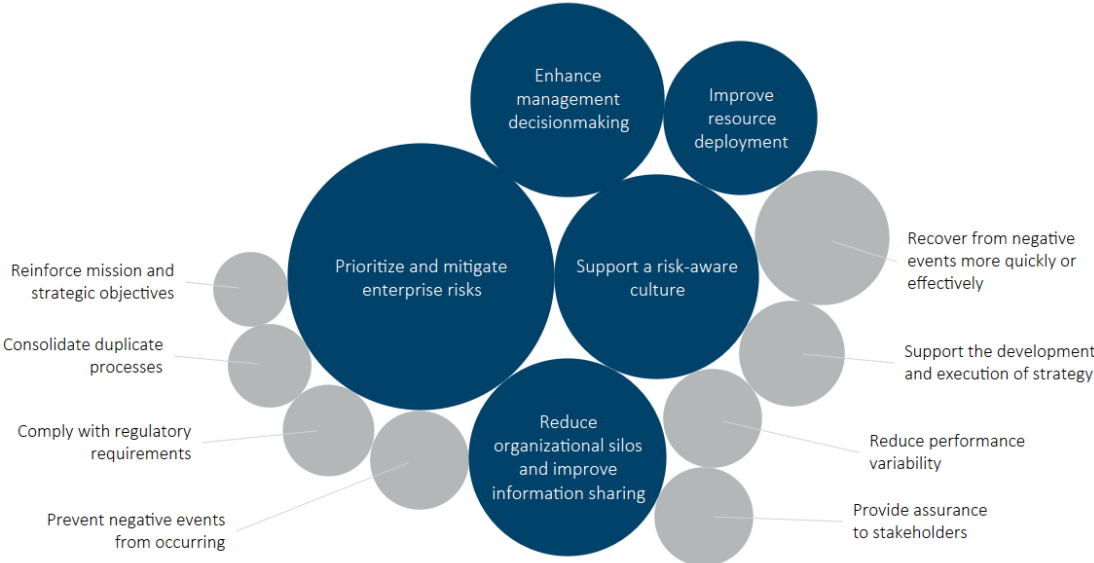
Question 19: What challenges do you believe will be associated with implementation of the Board's ERM program? Please rank your top 3 answers.
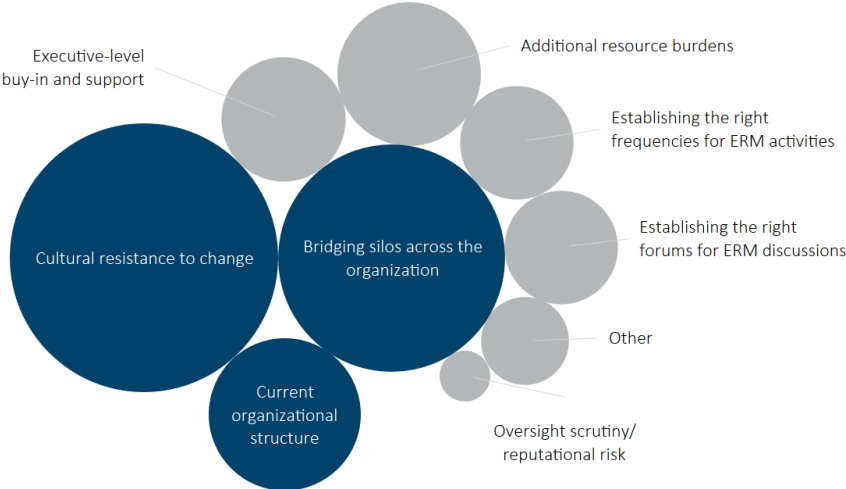
Appendix C: Management Response

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, DC 20551

OFFICE OF THE
CHIEF OPERATING OFFICER

September 8, 2021

Peter Sheridan
Associate Inspector General for Information Technology
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Peter,

Thank you for the opportunity to comment on the report, *The Board's Implementation of Enterprise Risk Management Continues to Evolve and Can be Enhanced*. We appreciate the Office of the Inspector General's (OIG) effort in developing this report and the recommendations for continuing the evolution of Enterprise Risk Management at the Board.

There were three findings noted in the report with recommendations listed under each finding. We generally agree with the recommendations offered in the report and provide our response for each recommendation to the OIG.

We value your objective, independent viewpoints and appreciate the professionalism demonstrated by all OIG personnel throughout this audit. We look forward to working with your office in the future.

Regards,

PATRICK
MCCLANAHAN
Digitally signed by PATRICK
MCCLANAHAN
Date: 2021.09.09 11:14:23
-04'00'

Patrick McClanahan
Chief Operating Officer
Federal Reserve Board

Cc: Sharon Mowry
     Ricardo A. Aguilera
     Raymond Romero
     Charles Young
     Nicole Bynum
     Winona H. Varnon
     Andrew Leonard

www.federalreserve.gov

2

Response to Recommendations Presented in the IG Report, "*The Board's Implementation of Enterprise Risk Management Continues to Evolve and Can be Enhanced*"

Recommendation 1: Work with Board divisions to conduct an assessment of the current risk management practices and risk culture across the agency and use the results to inform the direction of the Board's ERM program.

Management Response: The ERM team has been learning about and assessing the risk management practices of the divisions under the COO's purview as they implemented the program. We agree that administering a survey assessment across the agency would garner more information on risk management understanding, current practices, and readiness for ERM to help inform the program's direction. To that end, the ERM team has already begun drafting a survey and discussing the optimal audience for it.

Recommendation 2: Work with the administrative governor, as appropriate, to determine an optimal governance structure and associated reporting relationships for the agency's ERM program and update the *Delegations of Administrative Authority* accordingly.

Management Response: As the ERM program matures, the governance structure around it will need to evolve. We agree that a new governance body is needed at this point in the ERM implementation. We believe a small Risk Steering Committee would be best to oversee the continued implementation, advise the team on program design and methodology, and assist with ERM implementation in the other divisions. As the ERM program matures across the agency, we should evaluate whether the Risk Steering Committee continues to be the optimal structure or if a different structure would be more appropriate at that time. The reporting relationships and any updates of the *Delegations of Administrative Authority* will be discussed and assessed with the administrative governor considering the structure of the Board and its limitations on authorities over divisions.

Recommendation 3: Develop and use an early-stage ERM framework to inform broader adoption of ERM across the Board.

Management Response: The ERM team has incorporated many aspects of the Gartner recommendations for an early-stage framework as part of its ERM program design and implementation efforts. We agree that formalizing this information would be beneficial to the continued implementation of the ERM program. The ERM team has already begun drafting a formal document to be used as a framework now and to be updated as appropriate as the program matures.

Abbreviations

AFERM	Association for Federal Enterprise Risk Management
COO	chief operating officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRO	chief risk officer
EC	Executive Committee
ERM	enterprise risk management
FMFIA	Federal Managers' Financial Integrity Act of 1982
GRC	governance, risk, and compliance
OCOO	Office of the Chief Operating Officer
OMB	Office of Management and Budget
RMC	Risk Management Committee
SOC	Senior Officer Committee
SORM	Subcommittee on Operational Risk Management

Report Contributors

Khalid Hasan, Senior OIG Manager for Information Technology
Paul Vaclavik, OIG Manager, Information Technology Audits
Joshua Dieckert, Senior IT Auditor
Chelsea Nguyen, Senior IT Auditor
Peter Sheridan, Associate Inspector General for Information Technology

Contact Information

General

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551

Phone: 202-973-5000
Fax: 202-973-5044

Media and Congressional

OIG.Media@frb.gov

![OIG logo]

Hotline

Report fraud, waste, and abuse.

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, web form, phone, or fax.

OIG Hotline
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551

Phone: 800-827-3340
Fax: 202-973-5044