

2023 Major Management Challenges for the Board



Office of Inspector General

Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau




Office of Inspector General

Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

MEMORANDUM

DATE: May 31, 2023

TO: Board of Governors

FROM: Mark Bialek 
Inspector General

SUBJECT: *2023 Major Management Challenges for the Board*

We are providing you with the major management challenges facing the Board of Governors of the Federal Reserve System in 2023. These challenges represent what we believe to be the areas that, if not addressed, are most likely to hamper the Board’s accomplishment of its strategic objectives.

We identified the Board’s major management challenges by assessing key themes from our discussions with management and our knowledge of the agency’s programs and operations. We reordered the management challenges as part of our 2023 update and identified a new challenge facing the agency related to financial sector innovations. We have also updated our previously identified challenges. The Board’s major management challenges, in order of significance, are as follows:

- Strengthening Organizational Governance and Enterprise Risk Management
- Managing Hybrid Work and Workforce Planning, Updating the Human Capital System, and Advancing Diversity Initiatives
- Remaining Adaptable While Supervising Financial Institutions
- Enhancing Oversight of Cybersecurity at Supervised Financial Institutions and Service Providers
- Ensuring an Effective Information Security Program
- Evolving With Financial Sector Innovations
- Monitoring COVID-19 Pandemic Emergency Lending Facilities and Underlying Loan Portfolios
- Ensuring That Physical Infrastructure Effectively Meets Mission Needs

We routinely monitor the Board’s efforts to address the management challenges we identify. Our monitoring work includes following up on open recommendations and conducting related audit and evaluation work. For information on our ongoing and planned audit and evaluation work, please see our [Work Plan](#).

We appreciate the cooperation that we received from the Board during our update to the management challenges. If you would like to discuss any of the challenges, please feel free to contact me.

cc: Patrick J. McClanahan
Ricardo A. Aguilera
Eric Belsky
Matthew J. Eichner
Michael S. Gibson
Andreas Lehnert
Ann E. Misback
Kofi Spong
Trevor Reeve
Michelle A. Smith
Stacey Tevlin
Mark E. Van Der Weide
Winona H. Varnon
Beth Anne Wilson



Contents

Strengthening Organizational Governance and Enterprise Risk Management	5
Managing Hybrid Work and Workforce Planning, Updating the Human Capital System, and Advancing Diversity Initiatives	6
Remaining Adaptable While Supervising Financial Institutions	7
Enhancing Oversight of Cybersecurity at Supervised Financial Institutions and Service Providers	8
Ensuring an Effective Information Security Program	9
Evolving With Financial Sector Innovations	10
Monitoring COVID-19 Pandemic Emergency Lending Facilities and Underlying Loan Portfolios	11
Ensuring That Physical Infrastructure Effectively Meets Mission Needs	12
Abbreviations	13



Strengthening Organizational Governance and Enterprise Risk Management

An effective governance system provides leadership, direction, and accountability in fulfilling an organization's mission; helps to ensure appropriate stewardship of public resources; and establishes clear lines of responsibility for results. Effective enterprise risk management (ERM) can provide an enterprisewide view of organizational risks that informs decisionmaking and resource prioritization. Together, effective governance and risk management can enhance the Board of Governors of the Federal Reserve System's ability to achieve its goals and objectives.

The Board has complex governance structures for guiding the operations of the Federal Reserve System, which include oversight of the Federal Reserve Banks as well as activities and operations within the Board. These governance structures have been established over time; however, challenges exist in determining the appropriate balance between centralizing or decentralizing certain functions and responsibilities. For example, at the System level, efforts to modernize the information technology (IT) environment can pose governance challenges because the Board often has requirements driven by executive orders and Office of Management and Budget criteria that may not be applicable to the Reserve Banks. While some efforts to improve governance structures in these scenarios regularly occur, such as tailoring oversight groups or leadership, the speed of IT modernization often magnifies these challenges. In another example, the Board is taking steps to adopt a more centralized approach to overseeing personal investment and trading activities for Federal Open Market Committee officials and System employees, such as implementing rules to govern these activities. Continued efforts to strengthen governance can help further mitigate the risk of potential conflicts of interest.

Because of its decentralized structure, the Board has a consensus-driven culture that makes it difficult to establish an enterprisewide approach for managing risks and administering certain business functions. Nonetheless, the Board has initiated several efforts that will centralize certain functions to strengthen governance, including workforce planning; managing IT investments to address challenges that arise from the decentralization of the Board's IT services; and deploying a shared cloud-based system that will replace the Board's core human resources, finance, and procurement systems. The Board has also developed an early-stage framework to support the implementation and maturation of its ERM program and has made progress in working with Board divisions to define and manage risk appetites and tolerance levels.

Although the Board has made some progress toward enhancing its organizational governance and establishing an ERM program, the agency should continue to focus on governance challenges at both the System and Board levels. The Board may have to address cultural challenges when introducing new governance structures, as these efforts require considerable coordination and effective change management. In circumstances where enhanced governance results in revised business processes, the Board will need to ensure that effective controls are in place and are actively monitored.



Managing Hybrid Work and Workforce Planning, Updating the Human Capital System, and Advancing Diversity Initiatives

An agency's efforts to manage its human capital program can directly affect its ability to effectively execute its mission and maintain a qualified, diverse, and agile workforce with the necessary technical, managerial, and leadership skills. To maintain such a workforce, the Board should continue focusing on managing hybrid work and workforce planning initiatives, updating the human capital system, and advancing diversity initiatives.

The Board has transitioned to a hybrid work environment following its full-time remote work posture during the COVID-19 pandemic. As the Board continues to provide assistance to divisions implementing workforce planning initiatives, it must also ensure that it maximizes the benefits of a hybrid work environment that supports employees' work-life balance and health and safety objectives while also meeting the agency's business needs and return-to-office goals. The Board will also need to ensure that it develops and implements additional long-term workforce strategies—such as succession planning—for acquiring, developing, and retaining staff, especially in a highly competitive hiring environment for specialized skills.

The Board has continued to make progress in replacing its human capital management system with modern, cloud-based technology; this modernization has taken on increased importance in a continually evolving workforce environment and reflects a need to ensure the integrity of existing data while properly protecting new data. The successful transition of human capital records and processes to the new cloud-based system is time and resource intensive; however, timely implementation of these modernized systems will help foster more efficient administration of workforce services and workforce collaboration.

The Board will need to continue to be strategic in how it addresses changes to its workplace environment while simultaneously advancing on its diversity initiatives, including increasing diversity in mission-essential job families and in senior management. The importance of the Board's workforce is highlighted in both its *Strategic Plan 2020–23* and its *Diversity, Equity, and Inclusion Strategic Plan 2022–25*. These strategic plans can support the Board's efforts to foster a culture that encourages collaboration, flexibility, transparency, and fairness. The Board can further support division and Systemwide diversity initiatives by coordinating such efforts effectively and by providing timely and instructive advisory services.



Remaining Adaptable While Supervising Financial Institutions

Promoting the safety and soundness of individual financial institutions and financial stability more broadly is a core mission of the Board. As part of executing this mission, supervisors must anticipate the risks associated with changing economic conditions and adapt their supervisory approach accordingly. In addition to anticipating emerging risks, supervisors must assess an institution's effectiveness in managing risks given current and future business conditions. The Board should also assess the effectiveness of its supervisory tools and approaches in light of developments in the banking sector, such as the failure of Silicon Valley Bank. In addition, the Board should ensure that the System's examination workforce is sufficiently trained to address changing conditions by reinforcing existing, or creating new, supervisory rules and guidance.

A key component of effective supervision is coordinating and collaborating with other state and federal regulators. As a result, the Board will need to maintain strong cooperative relationships with other agencies to coordinate supervisory activities; leverage the work of other supervisors, as appropriate; and collaborate, as necessary, on any updates to banking regulation and policy. Continued efforts to coordinate with other state and federal supervisory agencies are crucial to the Board's effective execution of its supervisory responsibilities because this coordination can reduce the potential for duplicative efforts or gaps in supervisory coverage and help monitor, identify, and respond to emerging risks.



Enhancing Oversight of Cybersecurity at Supervised Financial Institutions and Service Providers

Cyberthreats to financial institutions supervised by the Board continue to increase in both number and sophistication. For example, cybersecurity threats and attacks have increased since the onset of the COVID-19 pandemic, and geopolitical events have also led to the potential for increased cyberattacks. Additionally, supervised financial institutions of all sizes increasingly partner with financial technology companies to offer new products and services to customers and rely on third-party service providers to support their operational and technological infrastructures, further increasing the risk of cyberattacks. Cyberattacks can create substantial operational risk, disrupt critical services, and ultimately affect financial stability. As a result, cybersecurity remains an area of significant focus for supervised financial institutions and federal financial regulators. Accordingly, financial institutions and regulators must work to protect vital networks and data from cyberthreats and prepare to respond to cyberattacks.

The Board continues to refine its approach to cybersecurity supervision. As part of that refinement effort, the Board should continue to ensure that its supervisory approaches for financial institutions and service providers evolve with changing cybersecurity risks. In November 2021, federal banking regulators approved a rule requiring banking organizations to notify their primary federal regulator of significant computer security incidents that may affect the U.S. banking system. Accordingly, the Board will need to ensure it has effective and efficient approaches to assess the threat an incident poses and ensure banking organizations or any service providers involved take appropriate action to minimize any disruption to the organizations' or providers' operations or to the U.S. banking system.



Ensuring an Effective Information Security Program

Information security continues to be a key risk area for federal government agencies, including the Board, as evidenced by cyberattacks that have targeted software supply chains, key federal systems, and critical infrastructure. While the Board continues to maintain an effective information security program and is taking multiple steps to strengthen and mature its program, the agency faces challenges in three key areas: (1) full implementation of a zero trust architecture (ZTA),¹ (2) optimal integration of ERM and cybersecurity risk management, and (3) enhanced IT supply chain risk management practices.

The Board has incorporated specific ZTA concepts into its information security program and has developed a strategy to enable the organization to fully transition to a ZTA by fiscal year 2024, in accordance with federal requirements. However, the Board will face complex short- and long-term challenges in successfully implementing its ZTA. These challenges are compounded by the decentralized nature of some IT services, which results in an incomplete view of the risks affecting the Board's security posture. Successful implementation of a ZTA will require close partnerships and coordination between Board business lines and divisions and the overall System. In addition, governance structures and reporting relationships between various disciplines will need to be refined. Specifically, the Board has developed a new IT governance structure that includes new committees and reporting relationships to modernize its approach to IT management. The Board will need to develop and formalize charters for these new committees and successfully navigate the resulting cultural changes to ensure successful implementation. Furthermore, as the Board's ERM program matures, the agency will need to ensure alignment between IT governance and risk management processes.

Finally, the Board will need to ensure that it has effective IT supply chain risk management processes in place, as the agency relies on a variety of third-party-operated and third-party-maintained systems and prioritizes the use of cloud computing-based systems to meet its mission. Specifically, the Board will need to strengthen processes to ensure that it has effective insight into and knowledge of the cybersecurity environment of third-party and cloud computing providers. While the Board has updated its policies, procedures, and processes to account for several new IT supply chain risk management requirements, it is still working on implementation and will need to ensure that the agency and its vendors consistently follow secure software development standards. Effective IT supply chain risk management will require close coordination and integration across Board divisions and disciplines, such as procurement, ERM, and data management.

¹ A ZTA is a set of system design principles and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. A key principle of a ZTA is the assumption that traditional network perimeters have been compromised and federal agencies must build the appropriate security protection.



Evolving With Financial Sector Innovations

In recent years, the financial sector has experienced the emergence of innovations such as private-sector real-time payment systems, crypto assets, and financial technology. Financial innovation supported by new technologies can spur competition, create products that better meet customer needs, and extend the reach of financial services and products to those typically underserved. Congress, the media, and industry have expressed interest in the Board’s initial response to these innovations. While these innovations provide benefits, they also raise potential policy, operational, and supervisory risks that the Board must consider.

In 2023, the Board anticipates launching the System’s new real-time settlement system—FedNow. The Board believes that FedNow will create new opportunities for financial institutions of all sizes to provide safe and efficient payment services to communities across the United States. In addition, the Board is also researching the potential benefits and risks of a central bank digital currency (CBDC). A CBDC could provide households and businesses with a convenient, safe, and liquid electronic form of central bank money and expand consumer access to the financial system. However, a CBDC also raises a variety of policy questions, including how it might affect financial-sector market structure, the cost and availability of credit, the safety and stability of the financial system, and the efficacy of monetary policy.

The Board has also begun to adapt its supervisory approach in response to financial innovations including the rise of crypto assets. While the emerging crypto-asset sector presents opportunities—such as the potential for faster and cheaper payment and transaction settlement—it also includes potential risks—such as fraud, theft, manipulation, and exposure to money laundering activities—for banking organizations, their customers, and the overall financial system. Finally, the Board has responded to the increased interest in master accounts and related services from banking institutions with nontraditional charters or pursuing nontraditional business models. Notably, the Board implemented a framework that would ensure that requests from nontraditional financial entities for master accounts are evaluated consistently and transparently.



Monitoring COVID-19 Pandemic Emergency Lending Facilities and Underlying Loan Portfolios

The COVID-19 pandemic resulted in disruptions to financial markets and affected many credit channels relied on by households, businesses, and state and local governments. Under the authority of section 13(3) of the Federal Reserve Act, the Board authorized 13 emergency lending facilities to ensure the flow of credit to various parts of the economy. In addition, the U.S. Department of the Treasury made equity investments in certain lending facilities established by the Board as authorized by the Coronavirus Aid, Relief, and Economic Security Act.

On July 30, 2021, the last of the 13 lending facilities stopped purchasing assets or extending credit. Five facilities have since closed. The eight facilities still managing and processing loan repayments are the five Main Street Lending Program (MSLP) facilities, the Paycheck Protection Program Liquidity Facility (PPPLF), the Term Asset-Backed Securities Loan Facility, and the Municipal Liquidity Facility.² Of the lending facilities that continue to manage their loan portfolios, the MSLP and the PPPLF have experienced loan losses or fraud.

Although the first principal payments on MSLP loans are not due until July 2023, the MSLP has experienced loan losses of approximately \$136 million and has \$10.3 billion in outstanding loans as of April 30, 2023. It is the only lending facility to experience such losses. In addition, instances of borrowers improperly obtaining Paycheck Protection Program (PPP) loans—which have been pledged to the PPPLF as collateral— and MSLP loans have been detected. There was also an instance of a fraudulent lender making PPP loans and pledging them as collateral to the PPPLF.

In these instances of loan losses and fraud, the System is protected, as Treasury has contributed capital that would absorb losses to the MSLP and the U.S. Small Business Administration has provided explicit guarantees for the PPP loans. Although the Board does not expect the System to experience losses from the lending facilities, the System will need to continue monitoring these portfolios given the potential for complex loan workout situations to address loan defaults.

² The MSLP operated through five lending facilities: the Main Street New Loan Facility, the Main Street Priority Loan Facility, the Main Street Expanded Loan Facility, the Nonprofit Organization New Loan Facility, and the Nonprofit Organization Expanded Loan Facility.



Ensuring That Physical Infrastructure Effectively Meets Mission Needs

The Board is committed to ensuring that it has the physical infrastructure it needs to execute its mission in a cost-effective and safe manner. Over the past decade, the Board has supplemented its owned space with leased space to accommodate overall staff growth and to house staff displaced by renovation projects. However, the Board's goal is to renovate all Board-owned buildings and create a campus for all employees that will allow for improved collaboration and communication while reducing operating costs.

These renovation projects are multiyear efforts that involve significant resources. The first building renovation was completed in 2022 at an estimated cost of \$471.5 million. Two additional building renovations are scheduled for completion in 2027 at an estimated cost of \$1.6 billion, and a fourth building renovation has not substantially begun. These projects present significant risks and challenges because of their size, complexity, and interdependencies as well as risks associated with contractor oversight, cost management, and disruptions to employees. Moreover, the Board faced limited workforce availability, supply chain delays, and price increases due to the COVID-19 pandemic. Finally, the Board will be challenged with space planning during and after the renovations, particularly in light of the uncertainty regarding space needs and utilization associated with the Board's transition to a hybrid work schedule.

In response to the challenges associated with these infrastructure projects, the Board hired additional managers and staff to monitor project schedules and milestones, oversee contractors, and provide technical support. In addition, as employees continue to telework, the Board is collecting data on the number and frequency of staff coming into the office to help determine space needs and utilization.



Abbreviations

CBDC	central bank digital currency
ERM	enterprise risk management
IT	information technology
MSLP	Main Street Lending Program
PPP	Paycheck Protection Program
PPPLF	Paycheck Protection Program Liquidity Facility
ZTA	zero trust architecture

Report Contributors

Terese Blanchard, OIG Manager, Financial Management and Internal Controls
Josh Dieckert, OIG Manager, Information Technology Audits
Bettye Latimer, OIG Manager, Financial Management and Internal Controls
Christopher Lyons, OIG Manager, Management and Operations
Megan Taylor, OIG Manager, Financial Management and Internal Controls
Paul Vaclavik, OIG Manager, Information Technology Audits
Michael Zeitler, OIG Manager, Supervision and Regulation
Andrew Gibson III, Senior OIG Manager for Management and Operations
Jackie Ogle, Senior OIG Manager for Financial Management and Internal Controls
Timothy Rogers, Senior OIG Manager for Operations, Planning, and Policy
Laura Shakarji, Senior OIG Manager for Supervision and Regulation
Khalid Hasan, Assistant Inspector General for Information Technology
Cynthia Gray, Deputy Associate Inspector General for Audits and Evaluations
Michael VanHuysen, Associate Inspector General for Audits and Evaluations

Contact Information

General

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

Phone: 202-973-5000

Fax: 202-973-5044

Media and Congressional

OIG.Media@frb.gov



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 Center I-2322
Washington, DC 20551

Phone: 800-827-3340

Fax: 202-973-5044