April 30, 2025

Board of Governors of the Federal Reserve System

2025–2026 Major Management Challenges for the Board

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

Contents

Introduction

The major management challenges facing the Board of Governors of the Federal Reserve System in 2025 and 2026 represent what we believe to be the areas that, if not addressed, are most likely to hamper the Board's ability to accomplish 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. This year, we have identified new management challenges related to leveraging artificial intelligence and modernizing information technology systems. The Board's major management challenges, in order of significance, are as follows:

- Strengthening Organizational Governance and Enterprise Risk Management
- Managing Workforce Planning and Updating the Human Capital System
- Enhancing Cybersecurity Oversight at Supervised Financial Institutions and Service Providers
- Remaining Adaptable While Supervising Financial Institutions
- Ensuring That Physical Infrastructure Effectively Meets Mission Needs
- Modernizing Information Technology Systems, Services, and Operating Models
- Ensuring an Effective Information Security Program
- Evolving With Financial Sector Innovations
- Leveraging Artificial Intelligence to Enhance Mission Delivery
- Wind-Down of COVID-19 Pandemic Emergency Lending Facilities and Their Underlying Loan Portfolios

We monitor the Board's efforts to address its management challenges. 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*.

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) provides an enterprise view of organizational risks that informs decisionmaking and resource prioritization. The Board should ensure that it has effective governance and risk management processes. Together, effective governance and risk management can enhance the Board'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 the activities and operations of the Board. These governance structures have been established over time; however, the Board is challenged to determine the appropriate level of centralization for certain functions and responsibilities. The System is centralizing certain functions across the Reserve Banks, which can create efficiencies but can also create challenges in Reserve Bank oversight. For example, the Board has been evolving the way it oversees Reserve Banks from an individualized approach toward a Systemwide approach.

In addition, the System's efforts to modernize its information technology (IT) environment can pose governance challenges. Specifically, the Board must ensure that federal goals and requirements to strengthen cybersecurity and IT governance practices are being met for System modernization efforts that affect Board data and delegated functions. While the Board tries to adapt to these scenarios, such as by 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 the personal investment and trading activities of Federal Open Market Committee officials and System employees. Continued efforts to strengthen governance in this area can help mitigate the risk of conflicts of interest.

Because of its decentralized structure, the Board has a consensus-driven culture that makes it difficult to establish an enterprise approach for managing risks and administering certain business functions. Nonetheless, the Board has begun to strengthen governance by centralizing certain functions, 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, once fully implemented, 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 is 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, because these efforts require considerable coordination and effective change

management. For circumstances in which enhanced governance results in revised business processes, the Board should ensure that effective controls are in place and actively monitored.

Managing Workforce Planning and Updating the Human Capital System

An agency's response to changes in its human capital environment can directly affect its ability to effectively execute its mission and maintain a qualified and agile workforce with the necessary technical, managerial, and leadership skills. Maintaining such a workforce may be affected by recent workforce directives, including a hiring freeze for executive branch employees. Considering the evolving federal workforce environment, the Board should consider whether to adapt its approach to workforce planning. The Board should also continue focusing on enhancing and maintaining its new human capital system.

The Board continues to help divisions implement workforce planning initiatives. Specifically, the Board standardized certain job families to ensure consistent roles and responsibilities across divisions; however, achieving division agreement on the standardization was a challenge. Because divisions tend to view job families as distinct based on division-specific roles and responsibilities rather than as having commonalities, they did not initially embrace standardization. The Board should identify which strategies were effective in promoting standardization during recent workforce planning initiatives and apply those when standardizing the remaining job families.

Thirty percent of current Board officers will be eligible for retirement by the end of 2029, which may result in gaps in leadership and institutional knowledge. In 2020, the Board's human capital section implemented succession planning, and the section continues to work with divisions on their succession planning needs and to promote such planning through educational outreach. Additionally, the Board estimates that succession planning tools will be implemented in 2027 as part of future releases of the Board's human capital management system. These tools will increase transparency in job opportunities across divisions. The Board should continue developing and implementing long-term workforce strategies—such as succession planning—for acquiring, developing, and retaining staff, especially in a highly competitive hiring environment for specialized skills. For example, as noted in both the IT modernization and artificial intelligence (AI) challenges, specialized expertise is needed and poses a human capital challenge for the agency as it competes with the private sector for resources. The human capital section continues to work with relevant IT and AI stakeholders to address these challenges.

The Board has continued to make timely progress in replacing its human capital management system with modern, cloud-based technology. Modernizing this system provides an opportunity to standardize and streamline core business processes so that the Board can effectively execute its mission. In addition, the new system will improve the data the Board collects, which will better inform the Board's financial decisionmaking as a whole. The Board has successfully transitioned its talent and performance modules to the new cloud-based system but will continue using a separate system for recruiting because the vendor for the recruiting system cannot meet certain Board implementation requirements. The need to use two different human capital systems because of integration challenges may lead to additional resource requirements and inefficiencies. Although the Board dedicated short-term resources to implement and manage the human capital system, it should dedicate permanent resources to maintain the system and prevent inefficient and duplicative processes.

Enhancing Cybersecurity Oversight at Supervised Financial Institutions and Service Providers

Cyber threats to Board-supervised financial institutions and their service providers continue to increase in both number and sophistication. Cyberattacks can create substantial operational risk, disrupt critical services, result in the loss of valuable and sensitive data, and ultimately affect financial stability. The Board continues to refine its approach to cybersecurity supervision and, as part of that effort, should continue to ensure that its supervisory approaches for financial institutions and service providers evolve with changing cybersecurity risks.

Supervised financial institutions face a variety of threats, such as ransomware, phishing, and spoofing attacks, which can affect their operations and services. 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 their exposure to cyberattacks. Moreover, because many financial institutions outsource their IT operations to a few large service providers, an attack on one provider could have widespread effects.

Under a rule issued by federal banking regulators, banking organizations must notify their primary federal regulator of significant computer security incidents that may affect the U.S. banking system. Accordingly, the Board should ensure that it has effective and efficient approaches to assess the threat an incident poses and ensure that banking organizations and service providers take appropriate action to minimize any disruption to the organizations' or providers' operations or to the U.S. banking system. Further, under its authority in the Bank Service Company Act, the Board, jointly with the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency, examines certain services performed by service providers that pose a significant risk to client financial institutions and the financial sector. The Board should ensure that it works effectively with its partner federal financial regulators to determine whether service providers have effective IT security programs and protect their networks and their clients' customer data against cyberattacks.

Remaining Adaptable While Supervising Financial Institutions

A core mission of the Board is supervising financial institutions to promote their safety and soundness and financial stability. To execute this mission, supervisors must identify evolving risks associated with changing economic conditions and adapt their supervisory approaches accordingly. The Board should continue evaluating the effectiveness of its supervisory guidance, tools, and approaches based on insights from the banking stress of 2023 as well as emerging developments and risks in the banking sector. The Board should also ensure that the System's examination workforce continues to hone its technical expertise and is adequately trained to address changing conditions and developments.

In recent years, financial institutions supervised by the Board have been increasingly exploring or pursuing new activities and technologies. Supervisors will need to assess whether firms engaging in these activities are sufficiently mitigating the associated risks and take appropriate supervisory action as needed. For example, some banking organizations are considering or engaging in crypto-related activities and technology-driven partnerships with nonbanks. To enhance its oversight of these activities, the Board established the Novel Activities Supervision Program. This program partners with existing supervisory teams to examine novel activities conducted by supervised banking organizations. The Board should ensure that these novel activities program resources are seamlessly integrated into existing examination programs when appropriate. In addition to the activities the Novel Activities Supervision Program oversees, the Board should ensure that supervised institutions assess and mitigate the risks posed by increasing adoption of AI technologies.

Further, a key component of effective supervision is coordinating and collaborating with other state and federal regulators. Accordingly, the Board should continue 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. Coordinating with other state and federal supervisory agencies is crucial to the effective execution of the Board's supervisory responsibilities because such coordination reduces the potential for duplicative efforts or gaps in supervisory coverage and strengthens the Board's ability to monitor, identify, and respond to emerging risks.

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. Current and planned renovation 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. In addition, the Board must address space design, space needs, and space utilization during and after the renovations.

Over the past decade, the Board has supplemented its owned space with leased space to accommodate overall staff growth and to accommodate staff displaced by renovation projects. The Board's goal is appropriate stewardship of its owned buildings either through renovation or annual maintenance. The Board also seeks to create a campus for all employees that will allow for improved collaboration and communication and plans to retain some leased space. These renovation projects are multiyear efforts that involve significant resources. The first building renovation was completed in 2022 and cost approximately $472 million. As of February 2025, two additional building renovations are scheduled for completion in 2027 at an estimated total cost of $2.4 billion, a $0.5 billion increase from the projected cost 2 years ago. The Board will pursue a 15-year rehabilitation plan for the fourth location.

In response to its physical infrastructure challenges, the Board is assessing its use of space and evaluating its real estate portfolio to determine its long-term position on real estate holdings.

Modernizing Information Technology Systems, Services, and Operating Models

IT plays a critical role in the Board's ability to accomplish its mission. To better ensure that IT investments support mission needs, the Board has developed a technology strategy to modernize its IT operating model and systems and to accelerate the pace of technology transformation. Further, the Board has taken steps to strengthen and centralize its approach to IT governance and services delivery. IT modernization and transformation will be key to ensuring that the Board's evolving business needs are met, particularly in the areas of forecasting, modeling, and data analytics.

In support of its IT modernization efforts, the Board has developed a significant, multiyear investment plan to reduce existing and emerging operating risks. The Board and the System are also undertaking a significant initiative to migrate IT systems and workflows to the cloud. Taken together, these initiatives represent billions of dollars of potential investment. To ensure that it achieves an effective return on investment, the Board should mitigate several risks, including those related to IT governance and financial management, human capital, change management, and information security. The Board should also mitigate the risk posed by interdivisional initiatives that have multiyear implementation schedules. Historically, those types of projects have frequently exceeded the expected budget and duration.

The Board has accumulated significant technical debt because it has not invested strategically in IT modernization.[1] The significant investment needed to effectively modernize the Board's IT systems, infrastructure, and operating models will require the agency to take an ERM approach to prioritizing budget growth areas. Further, the agency should continue to refine its IT governance approach to support enterprise IT investment, portfolio, and project management. In addition, the Board should ensure that investments in its IT workforce cultivate the knowledge, skills, and abilities to effectively manage and maintain new technologies and operating models.

Change management also represents a significant risk to the Board as it modernizes its IT. Specifically, business process reengineering, which includes inventorying current processes and determining where they need to be reengineered and enhanced, will be key to the Board successfully modernizing its IT and maximizing its return on investment. In addition, effective cybersecurity processes, including supply chain risk management, will be critical to ensuring that the Board and its systems, data, and personnel are protected.

[1] *Technical debt* is the cost of future rework when short-term fixes are prioritized over long-term decisions.

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. Cybersecurity risks to the Board are increasing and can come from a variety of sources, including nation-state actors and trusted insiders. The Board faces risks in modernizing its information security program and organizational cybersecurity culture to adapt to technological changes; the Board plans to modernize its legacy IT infrastructure that supports forecasting and modeling and is managing the increased migration of IT systems and workflows to the cloud.

The Board's agencywide information security program is managed by the Division of Information Technology and is led by the agency's chief information officer. Most of the agency's cybersecurity spending, however, is done by divisions other than the Division of Information Technology, and the Board invests less in cybersecurity as a percentage of its overall IT budget than many of its peer regulators. This presents challenges in maintaining enterprise cybersecurity situational awareness and implementing modernization efforts such as zero-trust architecture; secure identity, credentials, and access management; and integration of security into the software development life cycle. Further, the Board should modernize its security assessment and authorization and information security continuous monitoring processes to adapt to agile development methods, increased use of emerging technologies, and increased adoption of cloud services.

As the Board continues to adopt cloud-based solutions and looks to significantly invest in modernizing its legacy IT environment and infrastructure, effective supply chain risk management will be increasingly important. Elements of supply chain risk management include determining the organization's supply chain risk appetite and tolerance, developing a supply chain risk management strategy, and determining an overall governance structure. The Board will also need to develop a strategic approach and investment plan to address legacy cybersecurity weaknesses, such as its insider threat program, while modernizing cybersecurity capabilities.

Evolving With Financial Sector Innovations

Financial innovation supported by emerging technologies, such as real-time payment systems, distributed ledger technologies, and digital assets, can improve the timeliness of services, increase accessibility, and create efficiencies. The System has made progress in evolving with some financial sector innovations; however, it should further pursue modernization efforts and develop the proper risk mitigants to maintain the integrity and trust of services.

In July 2023, the System launched its new real-time settlement system, FedNow. As of January 2025, over 1,000 of the 9,000 U.S. banks and credit unions were participating. Since the launch, the System has focused on maturing FedNow by increasing participation and developing fraud prevention and detection tools, which will strengthen trust in the system. With the increased demand for instant payments, the System is exploring the business case and associated risks for interlinking cross-border payment systems, which would allow for faster, more accessible payments internationally. The Board implemented a framework that would allow for consistent and transparent evaluations of nontraditional institutions' access to its master accounts and payment systems and began publishing a database of requested or existing access. With these changes, the System is also managing ongoing litigation concerning decisions related to master account access.

Although the System has evolved with the launch of FedNow and updated the framework for master account access, other key areas are still being explored. During the 2023 banking crisis, some banks faced challenges accessing the discount window—which provides quick liquidity support to banks—because of preparedness issues for pledging collateral for use at the discount window. Challenges related to promoting use of the discount window also involve modernizing access to the discount window and destigmatizing a bank's use of the window. When new technologies are introduced into financial ecosystems, the Board should consider whether existing services are evolving with these technologies and can be used as intended. The Board has researched AI and machine learning, as well as stablecoins and tokenized assets, to better understand the implications of these private-sector developments on the financial and payments system. It has also researched the use of a central bank digital currency and concluded that it would only proceed with a central bank digital currency pursuant to an authorizing statute becoming law.

Leveraging Artificial Intelligence to Enhance Mission Delivery

AI is an "engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy."[2] AI presents significant opportunities for the Board to enhance mission delivery. AI, and particularly generative AI, which can create new content, is rapidly advancing, has become widely available, and has the potential to transform the way in which Board employees conduct their work. Effectively leveraging AI to improve operations and mission delivery will require the Board to manage risks through robust governance and risk management practices.

The Board has taken steps to develop governance and risk management practices for evaluating and adopting AI. For example, the agency has designated an acting chief artificial intelligence officer to advance the agency's AI objectives, coordinate use of AI across the agency, and mature the agency's AI program. As part of its governance structure, the agency has also established a program team and a working group that consist of members from across the agency and developed a policy to guide the evaluation and use of AI technologies. Further, the Board has initiated strategic investments and has made progress in launching a generative AI governance pilot program to evaluate the benefits, drawbacks, and guardrails related to staff using generative AI in their day-to-day tasks. However, the Board has not formalized an overall plan to strategically invest in AI technologies, infrastructure, and talent acquisition and development. Further, the majority of the Board's AI activities to date have been concentrated in the areas of research and testing and involve publicly available data. Robust governance and risk management practices will be needed to operationalize AI use cases to enhance mission delivery.

The Board has made progress in testing and deploying AI tools and platforms with supporting security and validation processes across the agency. As AI technologies mature and adoption increases in the public and private sectors, the Board should also continue taking steps to manage risk related to acquiring and developing secure enterprise AI tools and platforms, including establishing appropriate processes for model validation, code review, and security assessments. Maturing these processes will help the Board achieve and maintain market competitiveness and recruit and retain talent to support the Board's AI efforts.

In addition, while the Board has taken several steps to strengthen its data management program, continuing to mature data governance and related processes that promote data quality and integrity will support the Board's ability to effectively harness the power of AI. Such efforts should include ensuring that the agency's data inventory for both structured and unstructured data sets is comprehensive and includes the descriptive and technical metadata to allow the efficient and effective use of data in AI models. Finally, the Board should continue to refine its approach to governing AI within its existing security, architecture, and review processes, including determining whether and how those processes should be adjusted to address the unique opportunities and risks presented by AI.

[2] National Institute of Standards and Technology, *The Language of Trustworthy AI: An In-Depth Glossary of Terms*.

Wind-Down of COVID-19 Pandemic Emergency Lending Facilities and Their 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. When winding down the facilities, the System should be prepared to proactively address additional instances of loss and fraud.

On July 30, 2021, the last of the 13 lending facilities stopped purchasing assets and extending credit, and 7 facilities have since closed. The 6 facilities still managing and processing repayments are the 5 Main Street Lending Program (MSLP) facilities, with $2.9 billion outstanding as of February 28, 2025, and the Paycheck Protection Program Liquidity Facility (PPPLF), with $1.9 billion outstanding as of February 28, 2025.[3] The System is winding down these facilities, with the majority of loans maturing by 2026.

As of February 28, 2025, the MSLP had realized approximately $2 billion in interest, fees, and other revenue after accounting for its $1.36 billion in losses, and the PPPLF had realized $467 million in interest, fees, and other revenue with de minimis losses. Even if the size of these losses increases and exceeds the facility-generated interest, fees, or other revenue, the System has further protections against loss: Treasury has contributed capital that would absorb MSLP losses, and the U.S. Small Business Administration has provided a conditional guarantee for the Paycheck Protection Program loans. Regardless of the System's protections, facility losses could affect U.S. taxpayers and should be minimized to the extent possible.

[3] 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.

Abbreviations

AI	artificial intelligence
ERM	enterprise risk management
IT	information technology
MSLP	Main Street Lending Program
PPPLF	Paycheck Protection Program Liquidity Facility

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