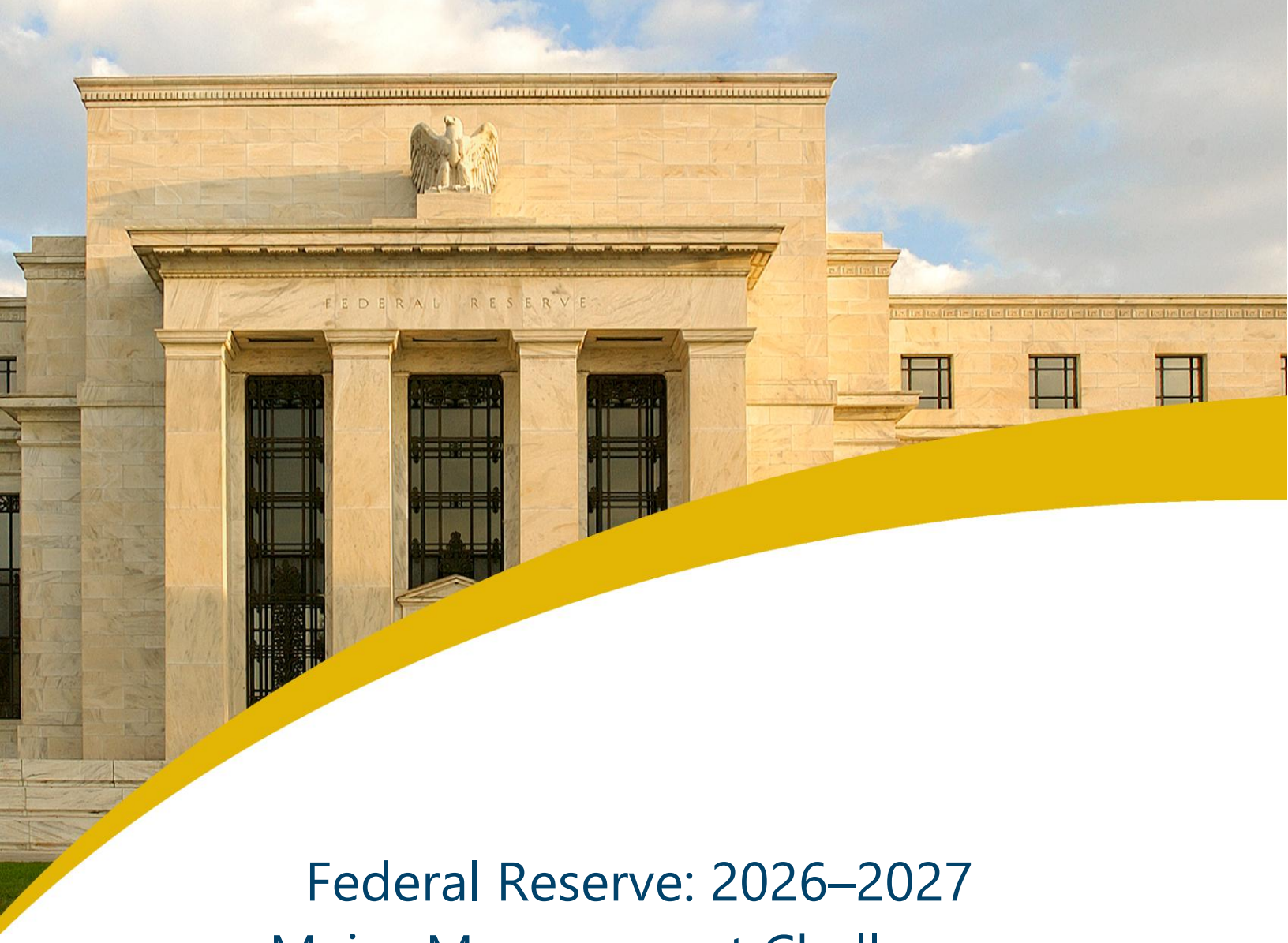


Federal Reserve: 2026–2027 Major Management Challenges

November 9, 2026
Special Report

Contents

Introduction 3

Strengthening Organizational Governance and Enterprise Risk Management 5

Ensuring an Effective Information Security Program 6

Enhancing Cybersecurity Oversight at Supervised Financial Institutions and Service Providers 7

Remaining Adaptable While Supervising Financial Institutions 8

Ensuring That Infrastructure Effectively Meets Mission Needs 9

Modernizing Information Technology Systems, Services, and Operating Models 10

Sustaining Mission-Critical Functions While Streamlining the Workforce 11

Evolving with Financial Sector Innovations 12

Using Artificial Intelligence to Enhance Mission Delivery 14

Abbreviations 16

Introduction

The mission of the Board of Governors of the Federal Reserve System is to foster the stability, integrity, and efficiency of our nation's monetary, financial, and payment systems to promote optimal macroeconomic performance. In carrying out this mission, the Board has significant influence and responsibility over the nearly $31 trillion U.S. economy.

To help ensure that the agency can succeed in this critical mission, we identify and monitor the major management challenges the Board faces. The following are the areas we believe that, if not addressed, are most likely to hamper the Board's ability to accomplish its strategic objectives in 2026–2027. We use these challenges as the basis for our planning activities and seek to conduct audit, evaluation, and inspection work connected to many of these topics during any work-planning cycle. We identified the Board's major management challenges by assessing key themes from our prior and ongoing audit, evaluation, and inspection work, our discussions with Board management, and our knowledge of the agency's programs and operations. While we typically issue these challenges every other year, we are updating them off cycle to share timely information with the new Board chairman. Our next management challenges update will be issued in 2028.

The Board's major management challenges are

- Strengthening Organizational Governance and Enterprise Risk Management
- Ensuring an Effective Information Security Program
- Enhancing Cybersecurity Oversight at Supervised Financial Institutions and Service Providers
- Remaining Adaptable While Supervising Financial Institutions
- Ensuring That Infrastructure Effectively Meets Mission Needs
- Modernizing Information Technology Systems, Services, and Operating Models
- Sustaining Mission-Critical Functions While Streamlining the Workforce
- Evolving with Financial Sector Innovations
- Using Artificial Intelligence to Enhance Mission Delivery

We monitor the Board's efforts to address these management challenges by conducting audits, evaluations, inspections, and other reviews and by issuing recommendations to improve performance in these areas.[1] As a result of our efforts to monitor open recommendations in these areas, we removed a top challenge, Wind-Down of COVID-19 Pandemic Emergency Lending Facilities and Their Underlying Loan Portfolios, from our previous list. Only one pandemic-era lending program remains in the repayment phase as of August 31, 2026, and the Board does not anticipate losses for the Federal Reserve System from the program. The

[1] Our website includes a list of our open recommendations and a list of ongoing work.

remaining challenges from our prior list continue themes, concerns, and risks we have previously identified.[2]

[2] Office of Inspector General, *2025–2026 Major Management Challenges for the Board*, April 30, 2025.

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 provides an enterprise view of organizational risks that informs decisionmaking and resource prioritization. Together, effective governance and enterprise risk management can enhance the Board's ability to achieve its goals and objectives.

The Board has complex governance structures for the operations of the System, which include oversight of the Federal Reserve Banks as well as the activities and operations of the Board. These governance structures have developed organically, and the Board faces challenges in managing a largely decentralized organization and in determining the appropriate level of centralization for certain functions and responsibilities. For example, the Board does not have a centralized program or enterprisewide policies and procedures for its insider risk management program. *Insider risk* refers to the likelihood and effect of incidents in which individuals with authorized access to an organization's critical assets use that access, either maliciously or unintentionally, in a way that negatively affects the organization. This omission limits the Board's ability to effectively and proactively identify and manage risks to its people, information, and assets.

The Board has begun to strengthen governance by centralizing certain functions and standardizing certain activities. For example, in response to our prior recommendations, 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. As part of this effort, the Board and the Reserve Banks are using a phased approach to implement by early 2027 a new system to monitor certain investment and trading activities. Continued efforts to strengthen governance in this area can help mitigate the risk of conflicts of interest.

Although the Board has made some progress toward enhancing its organizational governance, the agency should continue to focus on governance challenges at both the Board and System levels, including issues like insider risk management that may require System-level coordination. The Board may have to address cultural challenges when introducing new governance structures, because these efforts require considerable coordination and effective change management.

Ensuring an Effective Information Security Program

Information security continues to be a key risk area for federal agencies, including the Board, as shown 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 information technology (IT) infrastructure that supports economic 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 led by the agency's chief information officer. However, the Division of IT does not control all the agency's cybersecurity spending, as the Board's decentralized structure includes embedded IT units in other divisions. This structure presents challenges in maintaining enterprise cybersecurity situational awareness and implementing modernization efforts like zero-trust architecture; secure identity, credentials, and access management; and integration of security into the software development life cycle. In addition, while the Board has taken steps to update its policies on security assessment and authorization and information security continuous monitoring to incorporate ongoing authorizations, challenges remain in operationalizing those policy changes across the agency. Further, integrating cybersecurity into agile development methods and increased efforts to modernize the Board's IT environment by adopting cloud services present challenges to the Board's ability to maintain an effective information security program.

The Board is taking steps to centralize cybersecurity workforces and services, currently spread among divisions, in the Division of IT. At this stage, this initiative largely involves the transfer of IT personnel performing cybersecurity functions. Having a strategy for effective change management, training, and upskilling of transferred personnel will help ensure that the Board's cyber workforce has the knowledge, skills, and abilities that align with the agency's technology operating model.

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—such as defining a supply chain risk appetite and tolerance and developing a supply chain risk management strategy—will be increasingly important. The Board will also need to develop a strategic approach and investment plan to address legacy cybersecurity weaknesses, such as its insider threat program, data loss prevention capabilities, and cyber risk management processes, while modernizing cybersecurity capabilities.

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 ensure that its supervisory approaches for financial institutions and service providers evolve with changing cybersecurity risks.

Supervised financial institutions face a variety of cyber 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.

The Board should ensure that it works effectively with its partner federal financial regulators to determine whether financial institutions and their IT 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 their financial stability. In 2025, the Board announced plans to reduce its staffing by the end of 2026. Additionally, the Board's Division of Supervision and Regulation announced new supervisory operating principles. According to the division, these new principles seek to focus supervision on identifying and taking timely, proportionate action to address the most important risks to the safety and soundness of banking organizations. Amid these changes, the agency should ensure that supervision staff continue to monitor evolving risks and adapt their supervisory approaches accordingly. 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.

Additionally, financial institutions supervised by the Board have been increasingly exploring or pursuing new activities and technologies. For example, some banking organizations are engaging in crypto-related activities and technology-driven partnerships with nonbanking organizations. In addition, artificial intelligence (AI) technologies continue to evolve, and financial institutions are increasingly using AI for new purposes. Financial institutions are also relying more on third-party service providers to support their operations. Supervision staff will need to assess the risks associated with these activities, technologies, and arrangements and whether institutions and providers have sufficiently mitigated the resulting risks.

Further, effective supervision requires coordinating and collaborating with other state and federal regulators. Accordingly, the Board should maintain strong cooperative relationships with other agencies to coordinate supervisory activities; leverage the work of other supervision staff, as appropriate; and collaborate, as necessary, on 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 Infrastructure Effectively Meets Mission Needs

The Board has undertaken significant, multiyear renovation and capital improvement projects, including the ongoing $2.4 billion building renovation project. These initiatives are not always a part of the Board's core regulatory and policy competencies and present risks related to size, complexity, contractor oversight, cost management, and governance. Several of our prior reports have highlighted issues managing these types of initiatives.

Over the past decade, the Board has supplemented its owned space with leased space to accommodate staff growth and staff displaced by renovation projects, with a stated overall goal of creating one campus for all employees that will allow for improved collaboration and communication. These renovation projects are multiyear efforts that involve significant resources. The William McChesney Martin, Jr., Building renovation was completed in 2022 for $454.4 million. As of August 2026, the construction phase of the renovation of two additional buildings, the historic Marriner S. Eccles Building and the 1951 Constitution Avenue building, is scheduled for completion in December 2027. The Board of Governors' approved budget for the renovation project is $2.4 billion—a $1.1 billion increase from the projected initial cost of $1.3 billion in 2020. In addition, the Board will develop a maintenance and repair plan in 2026 for its New York Avenue building.

In response to a request from the former Board chairman, we recently issued a report on the Board's oversight of its Eccles-1951 renovation project. Our review identified project management, governance, and oversight concerns. Notably, the Board did not effectively execute its key contracts and repeatedly deviated from the cost-management provisions in its "construction manager at risk" contract. Although the Board may not immediately undertake future building projects like its previously planned New York Avenue building renovation, the Board is planning a significant, multiyear initiative that could create similar cost and schedule risks as the Eccles-1951 renovation project. The Board of Governors approved a $500 million economic forecasting and modeling modernization effort in 2024. The initiative is no longer reflected in the Board's multicycle budget because the Board is in the process of contracting with a third party to get a comprehensive cost estimate. However, concerted project management efforts with schedule and budget discipline, as well as appropriate governance and oversight, will be critical to the success of this project as well as future endeavors that present similar risks.

Modernizing Information Technology Systems, Services, and Operating Models

IT plays a critical role in enabling the Board to effectively conduct its mission, including developing economic policy, making monetary policy decisions, and achieving transparency obligations to Congress and the public. To better ensure that IT investments support mission needs, the Board has developed a technology strategy to modernize its IT operating model, workforce, 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 economic forecasting, modeling, and data analytics.

In support of its IT modernization efforts, the Board has developed a large-scale, multiyear investment plan to reduce existing and emerging operating risks and modernize its current processes through the forecasting and modeling modernization effort. This effort is essential to the Board's ability to meet its mission as it modernizes the processes and systems that directly inform Federal Open Market Committee decisions and public communications. The Board and the System are also continuing a significant initiative to migrate IT systems and workflows to the cloud. Together, these initiatives represent a significant expenditure for the Board.

To ensure that it achieves an effective return on its investments, the Board should mitigate several risks, including those related to IT governance and financial management, human capital, change management, and information security. In addition, effective cybersecurity processes, including supply chain risk management, will be critical to protect the Board and its systems, data, and personnel. The Board should also mitigate the risk posed by interdivisional initiatives that have multiyear implementation schedules. Historically, those types of projects have frequently exceeded expected budgets and durations. For example, the forecasting and modeling modernization effort has already experienced a 1-year extension from its original 2029 completion date. Actual expenditures have also fallen behind the year-one baseline projections—a variance that management attributes to a 2025 hiring freeze—indicating that performance against established benchmarks remains off track. As these systems support mission-critical policy outputs relied on by policymakers and the public, delays or changes in costs present not just financial risks but also risks to the Board's ability to deliver timely, accurate economic analysis to inform monetary policy decisions.

Sustaining Mission-Critical Functions While Streamlining the Workforce

Agencies must carefully navigate workforce changes to execute their mission and maintain a qualified, agile workforce. In May 2025, the former chairman directed Board divisions to consolidate functions, modernize business practices, and reduce the agency's workforce while ensuring that the Board meets its statutory mission. In response, the Board offered a voluntary resignation program and restructured certain divisions.

As the Board's streamlining efforts continue, the full effect has yet to be realized. For example, staffing reductions have resulted in a significant number of vacancies in important positions not anticipated by leadership. Given the recent reductions to the Board's workforce, divisions are using the Board workforce planning team's services more frequently, focusing on issues such as organizational design, span of management control, and skill gaps. However, divisions are not required to use these tools, and their implementation has remained informal and ad hoc. These efforts are particularly important with 71 percent of the Board's officers eligible for full or early retirement by the end of 2029.

While the Board is downsizing, it is also undertaking significant capital investment projects to modernize its data and technology environment. These modernization efforts may require particular technical, managerial, and leadership skills.

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. Specialized expertise is needed for the agency to compete with the private sector for resources. The Board must continue to monitor the effects of ongoing workforce reductions, address any job family and workforce gaps—especially involving the performance of core Board functions and emerging technology—and actively implement workforce strategies to meet future needs.

Evolving with Financial Sector Innovations

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

In July 2023, the System launched its domestic, real-time payment and settlement system, FedNow, which operates 24 hours a day, 7 days a week. Since the launch, the System has focused on increasing participation rates and maturing its services, such as increasing the transfer limit to $10 million and enhancing fraud mitigation tools. As of February 2026, over 1,600 of the 9,000 U.S. banks and credit unions were participating. Progress has been gradual among institutions sending instant payments primarily because of concerns about fraud risk. The System should continue to develop fraud prevention and detection tools, including the use of AI, to strengthen trust in FedNow.

The System also modernized its wholesale payment system, Fedwire, in July 2025 by adopting a global financial messaging standard that allows for more comprehensive data, improved fraud detection, and enhanced interoperability with international payment systems. While Fedwire allows for cross-border payments, it does so using intermediaries, which increase fees and cause delays. With the increased demand for instant payments, the System is exploring the business case and associated risks of enabling participants to make international payments through FedNow, supporting faster and more accessible cross-border commerce. In October 2025, the Board announced it will expand Fedwire's operating hours to 22 hours a day, 6 days a week by 2028 or 2029, allowing time for technological, operational, and industry readiness. As the Board continues to enhance FedNow and Fedwire, it should assess the need to maintain two infrastructures that offer comparable services.

In December 2025, the Board requested public input on a potential limited-purpose account designed to give legally eligible institutions with new business models limited access to the Federal Reserve's payment systems. While the Reserve Banks have always had the authority to limit the privileges of traditional master accounts, the Board is considering establishing a standardized, tailored account for Reserve Banks to offer. In March 2026, after consulting with the Board, a Reserve Bank approved for a 1-year term a limited-purpose account for a legally eligible institution with a nontraditional business model under terms consistent with the Board's December request for information. As the Board continues to evaluate establishing limited-purpose accounts, it will need to consider the risks that these accounts present to the financial system.

In addition to these initiatives, the System is exploring other reforms and innovations. Specifically, the Board is researching the future of the Reserve Bank's check-clearing services because of the increase in instant and other electronic payments, declining check usage, and high fraud rates with checks. It is also researching AI and machine learning, as well as stablecoins and tokenized assets, to better understand the implications of these private-sector developments. We will continue to monitor and assess the Board's response to new technologies as they are introduced into financial ecosystems.

Using Artificial Intelligence to Enhance Mission Delivery

AI presents significant opportunities for the Board to enhance mission delivery, but, if not managed carefully and effectively, also potentially serious risks. These risks include unauthorized access, model manipulation, exposure of sensitive information, and algorithmic bias from untrustworthy data, as well as cost considerations. While AI, and particularly generative AI, has the potential to transform how Board and System employees work, effectively leveraging AI to improve operations and mission delivery will require robust governance and risk management practices.

The Board has taken steps to develop governance and risk management practices for evaluating and adopting AI. It has designated a 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 Board has established a program team and a working group that consists of members from across the agency and developed a policy to guide the evaluation and use of AI technologies. Further, the Board has made strategic investments and expanded a generative AI pilot program to evaluate the benefits, drawbacks, and guardrails related to employees' day-to-day use of generative AI. The Board now allows agency and System employees engaged in Board-delegated functions to use two internal AI tools and several coding assistants. In addition, the Board has invested in a multivendor, multimodal strategy that the agency believes can absorb shifts in the AI landscape. While the Board's platforms are flexible, processes and staff will need to complete testing and evaluate results in the event of significant shifts in the AI landscape. Further, robust governance and risk management practices will be needed to further operationalize AI use cases on multiple platforms to enhance mission delivery.

The Board has also 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 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. It should also monitor for employees' use of unapproved models, including on Board mobile devices. Maturing these processes will help the Board respond effectively to the continuously changing AI technology landscape while recruiting and retaining talent to support the Board's AI efforts.

The Board should continue to refine its approach to governing AI within its existing IT 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. As the Board scales its AI tools and platforms, to include agentic implementation in the future, and integrates

them into more business workflows, it must develop and adapt risk assessment, threat modeling, and vulnerability assessment methodologies to address security and privacy risks that AI systems are susceptible to. The Board must also account for the cost implications of AI scaling, as providers bill by tokens—units representing the computational work (server processing, memory, and energy) required to process text. This usage-based billing model means costs scale directly with the volume and complexity of AI interactions, making financial monitoring essential as the Board expands AI capabilities.

Abbreviations

AI	artificial intelligence
IT	information technology



Hotline

Report fraud, waste, abuse, and mismanagement involving the programs and operations of the Board or the CFPB.

oig.federalreserve.gov/hotline

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

1-800-827-3340

General Contact

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

202-973-5000

Media and Congressional Inquiries

oig.media@frb.gov