On the 2026 board agenda

A banking and capital markets perspective

January 2026

Drawing on insights from our conversations with directors and business leaders, and incorporating specific considerations for the financial services sector, we highlight five items to keep in mind as boards consider and carry out their 2026 agendas:

- **Reassess the board's engagement in strategy**
- **Understand the company's AI strategy, including the related risks and opportunities**
- **Consider the adequacy of the company's data governance framework and processes**
- **Assess whether the company's cybersecurity governance framework and processes are keeping pace**
- **Revisit board and committee responsibilities.**

> "Disruption, volatility, and uncertainty will continue to test bank boards in a dynamic 2026, elevating their crucial role in providing big-picture context—from business model disruption to the impact of AI—for company direction. To strategically navigate this evolving landscape, boards are prioritizing robust data and cybersecurity governance, understanding AI's risks and opportunities, and proactively refining their oversight responsibilities to foster resilience and capture new growth."
>
> **—Peter Torrente**
> US Sector Leader, Banking & Capital Markets
> KPMG US

Reassess the board's engagement in strategy

Disruption, volatility, and uncertainty will continue to test boards in 2026. Monetary policy, a changing regulatory landscape, advances in artificial intelligence (AI), elevated cybersecurity risk, geopolitical tension, among others, will add to the challenge. In this volatile operating environment, demands for greater disclosure and transparency, particularly around the oversight and management of the company's strategy and risks, will continue to intensify. The pressure on management and boards will be significant. The board's role in helping provide big-picture context—from business model disruption risk to the impact of AI on the workforce—will be more important than ever to the company's decisions and direction.

For financial services entities, this means preparing for, withstanding, and recovering from "shocks" while quickly adapting to longer-term change. Successful strategies will require a balanced approach combining alignment with evolving supervisory priorities, capital efficiency, and digital enablement. Scenario planning for merger and acquisition (M&A) opportunities maintains its importance, especially given the current appetite for M&A from regulators and the current administration. Challenges will also arise in capturing growth opportunities, which may result in embracing new products or businesses such as private credit lending, stablecoins, and fintech partnerships. The board can provide credible challenges and insights to management as they navigate strategic planning and new growth opportunities.

Understand the company's AI strategy, including the related risks and opportunities

As companies forge ahead with AI and generative AI (GenAI) initiatives, it's imperative for boards to stay current on the related opportunities and risks, including how GenAI and AI agents are being deployed, and how the company is managing and mitigating the risks. Boards of financial services companies should closely monitor the governance structure of AI and GenAI deployments as well as understand the talent and workforce impact of the use of this technology.

Financial institutions are advancing AI strategies and are deploying AI use cases to areas of the organization such as loan origination, fraud prevention, systems development, and customer retention. Collaboration with partners is accelerating AI adoption across the industry. Boards are focused on understanding management's AI strategy and the processes in place and governance over AI decisions and use cases, including the consideration of return on investment, which may take various forms depending on the AI use. Boards may also monitor the regulatory impact or reputational risks involved with using these technologies when engaging with customers.

Consider the adequacy of the company's data governance framework and processes

The explosive growth in the use of AI is prompting more rigorous assessments of companies' data governance framework and processes. In its oversight of data governance, the board should insist on a robust data governance framework that:

- Makes clear what data is being collected; how it is stored, managed, and used; and who makes decisions regarding these issues
- Identifies which business leaders are responsible for data governance across the enterprise, including the roles of the chief information officer, chief information security officer (CISO), and chief compliance officer (or those performing similar functions)
- Determines which vendors and third parties may have access to company data and their obligations to protect it.

For financial services companies, the quality of organizational data, data privacy concerns, and the lack of robust risk and governance processes remain significant barriers and risks. Modernizing data and leveraging AI/analytics are key for driving personalization, smarter decision-making, and operational efficiency. Building a unified cloud-based data platform is also a priority for launching targeted AI use cases. The board plays an important role in considering whether the company's data governance framework supports their strategic initiatives, including AI governance and processes.

Assess whether the company's cybersecurity governance framework and processes are keeping pace

While management teams and boards have devoted substantial time and attention to addressing increasingly sophisticated cyber threats, companies must continue to upgrade their defenses against fast-moving AI-driven and quantum computing threats.

Financial institutions face a uniquely challenging and evolving cybersecurity landscape, driven by rapid technological advancements and heightened regulatory expectations. Boards should oversee the balance between technological innovation and robust risk management to build enterprise-wide resilience. AI is being integrated into security operations centers to automate tasks like threat detection, vulnerability management, and incident response, allowing cybersecurity teams to focus on more complex threats. Governance and accountability are being elevated, with increased responsibility placed on CISOs and boards to oversee cyber risk, extending to managing outsourcing complexities and ensuring rigorous security across the supply chain and digital ecosystem. AI security and data protection are paramount, requiring robust governance to secure AI models, ensure data privacy, and protect expanding data assets from leakage and misappropriation. Implementing Zero Trust architecture and AI-enhanced threat detection, including resilience drills and updating third-party risk protocols, are critical. Boards are positioned to provide oversight around robust security and governance for AI systems and oversee preparation for the cryptographic threats of quantum computing.

Revisit board and committee responsibilities

Refining board and committee risk oversight responsibilities requires diligence. The increasing complexity and fusion of risks requires a holistic approach to risk management and oversight.

For banking and capital markets, risk and regulatory issues are top of mind. Risk and compliance professionals are leveraging technology to transform compliance, manage regulatory complexity, and evolve risk assessment methodologies to address emerging risks. Boards should monitor potential changes to existing regulations and regulatory practices, such as stress testing requirements and recovery planning guidelines. They should also prepare for a more flexible regulatory approach to technological innovations and products.

To support the board's governance over emerging technology and deployment, financial institutions are creating board technology committees to focus on overall technology strategy, data security, and investments in technology, including AI. Board members with technology experience—either as a former chief information officer, experience at a large technology company, or as a founder of their own technology company—are being counted on in technology committees to bring expertise and new perspectives to the boardroom.

Digital assets present a unique set of risks that banks are not accustomed to managing, including interaction with public blockchains, management of private keys, and Know Your Customer/Anti-Money Laundering/Know Your Transactions (KYC/AML/KYT) requirements. Banks will need to perform comprehensive risk assessments and update their risk taxonomies before incorporating digital assets into their business models. Establishing a comprehensive governance model that helps identify risks and controls around digital assets and interacting with public blockchains is crucial. As the board considers oversight of these activities, establishing which committee will oversee these developments will help ensure that management's strategy, goals and incentives, and governance structure are properly aligned.

> With the widespread adoption of AI, it has become imperative for bank boards to champion strong technology governance and uphold stringent data integrity standards. An emerging trend we see is the development of dedicated technology committees, which are an effective way to diligently oversee AI-related risks, fortify data governance frameworks, and conscientiously propel technological innovation within their financial operations.
>
> **—Karen Silverman**
> National Industry Knowledge Leader
> KPMG US

Contact us

Peter Torrente
US Sector Leader,
Banking & Capital Markets
KPMG US

Chris Seaman
Partner, Audit
KPMG US

Karen Silverman
National Industry Knowledge Leader
KPMG US

Andrew Ellis
Banking Consulting Leader
KPMG US

Agnel Kagoo
Capital Markets Consulting Leader
KPMG US

Nadia Orawski
US Deal Advisory & Strategy Banking Leader
and Financial Services Strategy Leader
KPMG US

Stephanie S. Petruzzi
Capital Markets Deal Advisory Leader
KPMG US

Mark Price
National Tax Industry Leader
KPMG US

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**