BANK POLICY INSTITUTE

April 17, 2024

Via Electronic Mail

Commodity Futures Trading Commission
Three Lafayette Centre
1155 21 Street NW
Washington, D.C. 20581
Attention: Christopher Kirkpatrick, Secretary

Re: Request for Comment on the Use of Artificial Intelligence in CFTC-Regulated Markets (CFTC Release No. 8553-24)

Ladies and Gentlemen:

The Bank Policy Institute[1] appreciates the opportunity to respond to the Commodities Futures Trading Commission's request for comment on the use of artificial intelligence in markets the Commission regulates.[2] Banking organizations have used artificial intelligence for many years[3] and have significant experience leveraging its benefits while managing its risks.

In response to the Commission's request for comment, we are submitting our recent report, *Navigating Artificial Intelligence in Banking*.[4] This report discusses banking organization's current use cases

[1] The Bank Policy Institute is a nonpartisan public policy, research and advocacy group that represents universal banks, regional banks, and the major foreign banks doing business in the United States. The Institute produces academic research and analysis on regulatory and monetary policy topics, analyzes and comments on proposed regulations, and represents the financial services industry with respect to cybersecurity, fraud, and other information security issues.

[2] *Request for Comment on the Use of Artificial Intelligence in CFTC-Regulated Markets*, Release 8853-24 (Jan. 25, 2024), https://www.cftc.gov/media/10156/AI_RFC_012524/download.

[3] *See, e.g.*, U.S. Dept. of the Treasury, *Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector* 12 (March 27, 2024), https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf ("In particular, AI tools for fraud detection, including machine learning (ML)-based tools, have been used by a wide range of financial institutions as part of risk management strategies for more than a decade, as reported by interview participants.")

[4] Brian Allen, *Navigating Artificial Intelligence in Banking*, BANK POLICY INSTITUTE (April 8, 2024),

for artificial intelligence and their corresponding legal obligations and risk management programs. We are confident this report will contribute to the Commission's understanding of artificial intelligence use and risk management by banking organizations operating in the markets regulated by the Commission.

* * * * *

The Bank Policy Institute appreciates the opportunity to respond to the Commission’s request for comment. If you have any questions, please contact me by phone at (202) 589-2534 or by email at joshua.smith@bpi.com.

Respectfully submitted,

Joshua Smith
Vice President, Assistant General Counsel
Bank Policy Institute

https://bpi.com/navigating-artificial-intelligence-in-banking/.

Navigating Artificial Intelligence in Banking

Governance and Risk Management Frameworks

April 2024

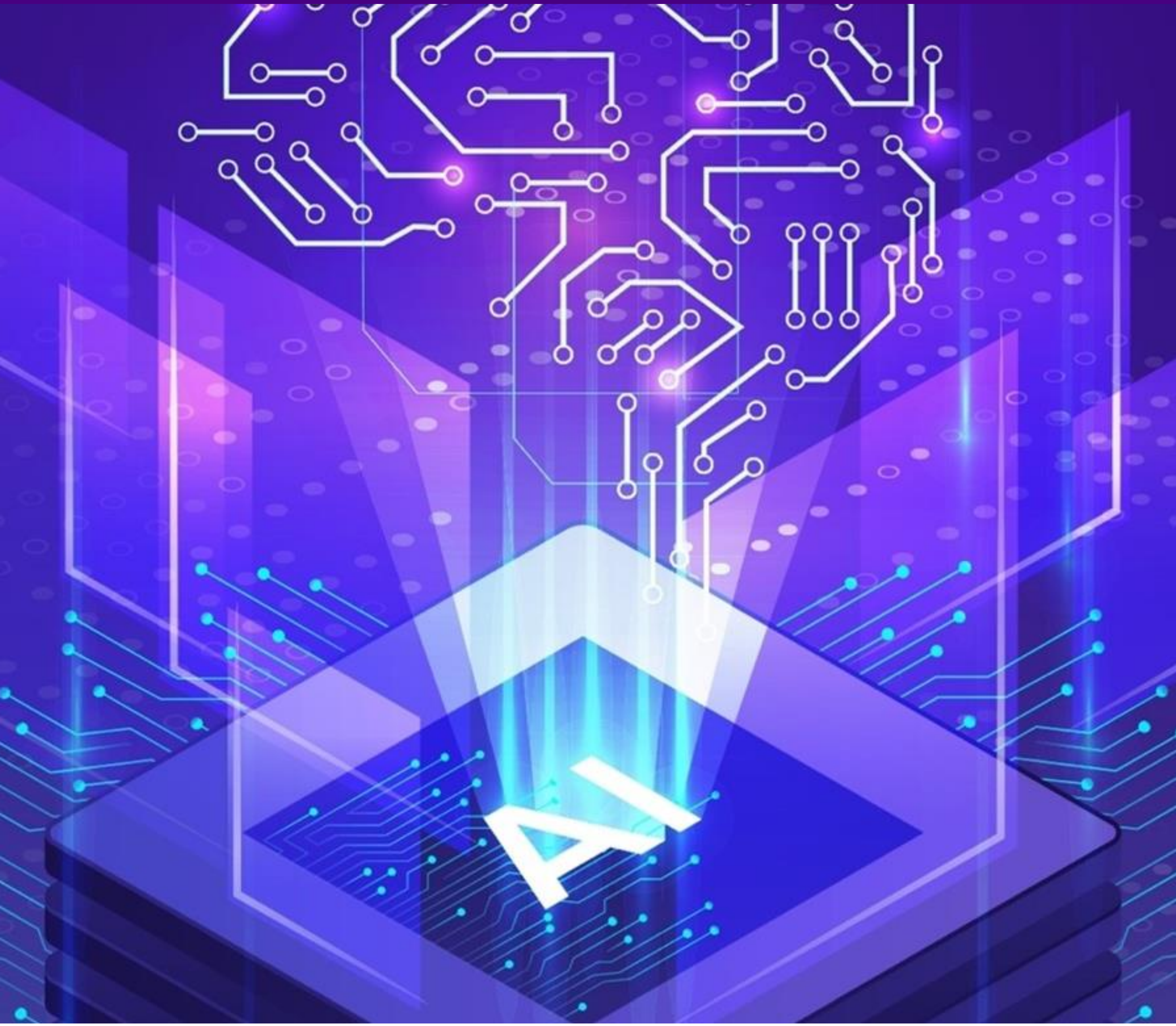

Table of Contents

I. Introduction

Banking organizations[1] have a proven track record of successfully deploying new technologies while continuing to operate in a safe and sound manner and adhering to regulatory requirements.[2] Throughout the years, banking organizations and financial institutions have digitized, gone online, transitioned to mobile services, automated processes, moved infrastructure into the cloud and adopted many other technologies, including machine learning, a form of AI. Many of these new technologies have presented new risks or amplified pre-existing risks, yet banking organizations have been able to manage these risks effectively and evolve to better serve their customers.

Artificial intelligence (AI)—or the ability of a computer to learn or engage in tasks typically associated with human cognition—has received a great deal of attention recently from the public, businesses and government officials. In October 2023, the Biden Administration issued its "Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence" (the AI Executive Order),[3] outlining the Administration's eight principles for governing the development and use of AI, which include, among other things, ensuring the safety and security of AI technology, promoting innovation and competition and protecting consumers and privacy. The AI Executive Order also directs various government agencies to take actions to promote those goals and affirms that "[h]arnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks."[4] More recently, in January 2024, the House Financial Services Committee announced the formation of a bipartisan working group

[1] This paper focuses principally on the governance and risk management practices, regulations, guidance, and supervisory expectations applicable to banking organizations. However, many of the principles discussed herein are relevant to other categories of financial institutions and the regulations and policies to which they are subject.

[2] This paper focuses predominantly on regulatory requirements applicable to U.S. bank organizations.

[3] Executive Order No. 14110, 88 Fed. Reg. 75,191 (Oct. 30, 2023)

[4] *Id.*

to “explore how [AI] is impacting the financial services and housing industries.”[5] AI has also received attention within the banking industry, with banking organizations and their regulatory agencies exploring the potential benefits and potential risks of AI and how the industry may continue to evolve in a safe and sound manner as the technology continues to advance.

Although attention to AI has increased markedly with the broad availability of relatively new technologies like large language models (LLMs), AI is not new. The conceptual foundations of AI were first articulated in scientific literature as early as the late 1940s,[6] and the term “artificial intelligence” was itself coined in 1955.[7] One of the challenges of any discussion of AI is determining the scope of what is meant by “AI.” In this paper, the terms “AI,” “AI model” and “generative AI” have the meanings used in the AI Executive Order[8] and can include a wide range of potential models, processes and use cases that incorporate AI.[9]

Banking organizations may use AI in connection with a variety of activities, including fraud detection, cybersecurity, customer service (such as chatbots) and automated digital investment advising. As with other new technologies, banking organizations have implemented and governed these and other uses of AI within existing risk management frameworks in accordance with applicable regulations, guidance and supervisory expectations. In fact, the integration of AI in the form of machine learning within the financial services sector traces its origins to the 1980s,[10] when it was primarily employed to identify and counteract fraudulent activities. It has expanded its application to a variety of use cases since.[11] This paper describes some of the guidance relevant to the use of AI, while recognizing that there is no “one-size-fits-all” approach to AI risk management. Risk management practices will vary depending on the AI technology, application, context, expected outputs and potential risks specific to the individual organization. In addition to the existing guidance, banking organizations also recognize that existing laws are applicable to the use of AI in the various contexts in which it may be employed and take those laws into account when considering particular use cases.[12]

[5] Staff of House Financial Services Committee, Press Release, McHenry, Waters Announce Creation of Bipartisan AI Working Group (Jan. 11, 2024), https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=409108.

[6] Bernadette. Longo, *Edmund Berkeley, computers, and modern methods of thinking*, IEEE Annals of the History of Computing, vol. 26, no. 4, at 4-18, (Oct.- Dec. 2004).

[7] The term “artificial intelligence” was reportedly coined in a 1955 proposal for a “2 month, 10 man study of artificial intelligence” submitted by John McCarthy (Dartmouth College), Marvin Minsky (Harvard University), Nathaniel Rochester (IBM), and Claude Shannon (Bell Telephone Laboratories). *See* http://jmc.stanford.edu/articles/dartmouth.html; https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.

[8] As defined in the AI Executive Order, AI “has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action”; “AI model” means “a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs”; and “generative AI” means “the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.” We expect the generally accepted industry definitions of these terms to continue to evolve and change as the underlying technologies continue to innovate and change.

[9] This paper does not attempt to describe the full universe of models, processes, and use cases.

[10] K. W. Kindle, R. S. Cann, M. R. Craig, and T. J. Martin, "PFPS - Personal Financial Planning System - AAAI," in Proceedings of the Eleventh National Conference on Artificial Intelligence, pp. 344-349, 1989.

[11] Ubuntu, "Machine Learning in Finance: History, Technologies, and Outlook," Ubuntu Blog, [Published/Updated Date], https://ubuntu.com/blog/machine-learning-in-finance-history-technologies-and-outlook, (accessed Aug. 23, 2023).

[12] The banking agencies have emphasized the applicability of existing laws to the use of AI. Federal Reserve Board Vice Chair for Supervision Michael Barr recently noted that the Federal Reserve is “technology agnostic” when examining firms on compliance with laws such as the

II. Harnessing AI: Governance and Risk Management for Resilience and Innovation

AI is one of the latest of many technologies that have been, or are in the process of being, implemented by banking organizations. AI has a wide range of potential capabilities, is rapidly evolving and may be incorporated in numerous and highly diverse use cases, creating both opportunities and potential risks for banking organizations. This paper outlines the governance and risk management principles already established by the banking agencies that provide an overarching framework for banking organizations to implement AI in a safe, sound and "fair" manner. The comprehensive approach to risk management required by the banking agencies allows banking organizations to utilize their risk management practices to address evolving technologies and associated potential risks. This is particularly important in the AI context given the speed at which AI technologies are developing. Banking organizations must be able to act quickly to identify, evaluate, monitor and manage risks posed by emerging AI technologies, and use currently available risk management processes to do so.

This paper discusses that (1) while AI's applications will differ based on the nature of the AI and the applicable use case and business context, banking organizations' existing governance and risk management principles provide a framework for consistency, coordination and adaptability in the face of the opportunities and potential risks posed by AI, and (2) given the dynamic nature of AI and the potential use cases, continued partnership with the banking and financial sector agencies is necessary to ensure that the sector's approach to AI remains both responsive and aligned with regulations, guidance and the broader objectives of financial markets safety and soundness and consumer protections.

Responsible implementation of AI benefits from a deliberate approach from regulators and other stakeholders as all parties continue to learn how best to address challenges and take advantage of opportunities in this space. That approach must balance the opportunities and potential risks presented by AI, as well as the need of banking organizations and regulators to consider evolving circumstances. It is in everyone's best interests for AI tools to be implemented in a safe, sound and fair manner, enabling banking organizations and their customers to benefit from new AI capabilities while appropriately mitigating risks. Those goals are best served by banking organizations and regulators working together to share information and identify benefits and risks, as well as appropriate mitigation strategies. BPI[13]

Community Reinvestment Act. *See* Ebrima Santos Sanneh, Regulators Say They Have the Tools to Address AI Risks, *supra* note 19. In addition, fair lending laws (*e.g.*, the Equal Credit Opportunity Act, Fair Housing Act, and their implementing regulations and related guidance) require explanations for adverse decisions as a means of ensuring fair treatment, and the Consumer Financial Protection Bureau has issued a number of circulars addressing financial institutions' obligation to provide specific and accurate explanations to customers when their decisions to take adverse actions with respect to credit involve algorithms, such as AI models. *See* CFPB, Circular 2023-03: Adverse Action Notification Requirements and the Proper Use of the CFPB's Sample Forms Provided in Regulation B (Sept. 19, 2023), https://files.consumerfinance.gov/f/documents/cfpb_adverse_action_notice_circular_2023-09.pdf; CFPB, Circular 2022-03: Adverse Action Notification Requirements in Connection with Credit Decisions Based on Complex Algorithms (May 26, 2022), https://files.consumerfinance.gov/f/documents/cfpb_2022-03_circular_2022-05.pdf.

[13] The Bank Policy Institute is a nonpartisan public policy, research, and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks, and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

and its technology policy division known as BITS[14], looks forward to continuing to work with its members, the federal banking agencies and other U.S. government offices to facilitate future collaboration and consultations as the AI landscape evolves.[15]

To lay a common groundwork for future conversations, this paper highlights some elements of enterprise risk management (ERM), including risk governance, model risk management, data risk management and third-party risk management, that provide a framework within which banking organizations can identify, assess, manage and monitor the potential risks that may be posed by emerging AI technologies. Through these frameworks, banking organizations have the tools to effectively manage risks posed by AI, even while AI, its use cases and the application of these frameworks to AI are evolving.

III. Embracing Emerging Benefits and Understanding Potential Risks

Integrating AI into the banking sector offers potential benefits, including processing information and detecting patterns with greater efficiency and effectiveness by augmenting human capabilities. The ability of AI to analyze vast, complex datasets can reveal trends and anomalies beyond human detection, enhance decision-making and potentially reduce bias are some of the many new and or advanced outcomes that AI provides. AI tools employing machine learning (ML) have the ability to continuously learn and adapt, improving their pattern recognition capabilities. Even so, AI also has the potential to exacerbate biases within a model or data set which can produce inaccurate or misleading results. Further, the opacity of certain AI models' methods can present challenges for users to identify and correct for inaccuracies or biases.

The adoption of any new technology requires consideration of its risks and rewards, and banking organizations rely on their robust governance and risk management practices to do so. As BPI has noted in connection with the implementation of other emerging technologies, managing risk is fundamental to the business of banking and it is imperative for banking organizations to assess and manage possible risks and benefits in all aspects of their businesses.[16] Responsible implementation of AI in the banking sector hinges on many factors, including integrating established risk management practices, such as

[14] BITS – Business, Innovation, Technology, and Security – is BPI's technology policy division that provides an executive-level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud, and improve cybersecurity and risk management practices for the nation's financial sector.

[15] BPI and its members have already been engaging in advocacy with respect to the safe and sound adoption of AI in the financial services industry. *See, e.g.*, BPI, Letter re Response to OSTP RFI: National Priorities for Artificial Intelligence (July 7, 2023), https://bpi.com/wp-content/uploads/2023/07/OSTP-RFI-BPI-Response-7.7.23.pdf ("We are committed to the responsible use and development of AI technologies, underpinned by strong governance, oversight, and risk management. The banking industry's foundational adherence to, and experience with, robust risk management practices, including model risk management, IT risk management, cyber risk management, enterprise risk management, operational risk management and resilience, data security, and privacy, can be effectively leveraged to assist in establishing a framework designed to allow for the responsible use of AI within the financial services sector."); BPI and Covington & Burling LLP, Artificial Intelligence: Recommendations for Principled Modernization of the Regulatory Framework (Sep. 14, 2020), https://bpi.com/wp-content/uploads/2020/10/Artificial-Intelligence-Recommendations-for-Principled-Modernization.pdf; Greg Baer and Naeha Prakash, Machine Learning and Consumer Banking: An Appropriate Role for Regulation, BPI (Mar. 14, 2019), https://bpi.com/machine-learning-and-consumer-banking-an-appropriate-role-for-regulation/.

[16] Paige Paridon and Joshua Smith, Distributed Ledger Technology: A Case Study of The Regulatory Approach to Banks' Use of New Technology, BPI (Feb. 1, 2024), https://bpi.com/distributed-ledger-technology-a-case-study-of-the-regulatory-approach-to-banks-use-of-new-technology/.

model risk management, risk governance and third-party risk management. This approach to risk management can help to confirm that AI's performance and outputs meet expectations and allow banking organizations to adapt to evolving risks.

Certain of these established risk management practices, including validation protocols, thorough testing of modeled outputs and ongoing monitoring of AI tools for continuous assessing of model quality, drift in performance and robustness will all play an important role in light of the unique characteristics of certain AI tools. For example, the validation process for an AI tool may benefit from additional or modified human input or intervention. "Human in the loop validation" is useful to validate many AI tools, and is especially important in the specific context of generative AI due to its inherent ability to hallucinate, or produce false or misleading information presented as fact. AI performance can also be evaluated through metrics, including those that measure performance over time, precision, recall and accuracy, among other things. Such metrics will be evaluated by automatic evaluation, human evaluation or a combination of both. Explainability must be considered in applying risk management principles, especially for generative AI technology. Fundamentally, explainability refers to the capacity to discern how outputs are generated in a consistent and understandable manner. Many AI models, especially those employing complex algorithms like deep neural networks, generate outputs where neither the user nor the developer can easily or comprehensively discern the basis for why one or more of the outputs were generated. Practices around data input, decision-making criteria and weighting of those criteria, assurance review and others are being developed to ensure that validation processes keep pace with technology. Likewise, the field of explainable AI, which aims to demystify AI models and make their operations more transparent and understandable, is in its early stages and continuing to develop.[17] This includes developing methodologies to trace how AI models process inputs into outputs and to understand the states of the models before and after processing. This would include, but not be limited to, model evaluation with a primary focus on overall LLM performance and system evaluation with a primary focus on the effectiveness of LLMs in specific use cases.

IV. AI and ERM: Maturing a Cohesive Risk Management Strategy in Banking

As banking organizations consider new uses of AI, including generative AI, the federal banking agencies continue to evaluate and monitor the use of AI within the banking industry. For example, in its Fall 2023 Risk Perspective (Fall Risk Perspective), the Office of the Comptroller of the Currency recognized that "[a]lthough existing guidance may not expressly address AI use, the supervision risk management principles contained in OCC issuances provide a framework for banks that implement AI to operate in a safe, sound and fair manner."[18]

[17] *See, e.g.*, Defense Advanced Research Projects Agency, Explainable Artificial Intelligence (XAI), https://www.darpa.mil/program/explainable-artificial-intelligence.

[18] OCC, Semiannual Risk Perspective from the National Risk Committee: Fall 2023 (Dec. 7, 2023), https://www.occ.treas.gov/publications-and-resources/publications/semiannual-risk-perspective/files/semiannual-risk-perspective-fall-2023.html.

Indeed, the Fall Risk Perspective noted that banking organizations need to "identify, measure, monitor and control risks arising from AI use as they would for the use of any other technology."[19] Similarly, in its 2023 Annual Report, the Financial Stability Oversight Council noted that "[e]xisting requirements and guidance also apply to AI, despite the rapid development and evolution of technology. These include general risk management requirements that would apply to any technology used by banking organizations, plus domain-specific use cases like fair lending that already have established rules to which AI (and any other approach used) must conform."[20] The Board of Governors of the Federal Reserve System and OCC also have noted both the benefits and risks of new AI technologies and that the banking agencies are working to ensure their supervision keeps pace with the technology.[21]

The banking agencies have issued regulations and guidance relating to banking organization risk management.[22] Informed by these regulations and guidance, banking organizations have in place ERM frameworks, including governance structures and third-party risk management and model risk management practices and related policies, within which any use of AI should be evaluated and governed.[23] ERM has been described as "an integrated approach to identifying, assessing, managing and monitoring risk in a way that maximizes business success. It involves the practices and processes the board and management use to define their business model and strategy, prioritize the associated risks and identify ways to mitigate them, use that analysis to make effective decisions and create an organization that anticipates and adapts to the changing internal and external environments."[24] This comprehensive and integrated approach provides a framework for banking organizations to manage risks appropriately and consistently across the organization.

[19] *Id. See also* Speech of Lael Brainard, Governor of the Federal Reserve, What Are We Learning about Artificial Intelligence in Financial Services? (Nov. 18, 2018), https://www.federalreserve.gov/newsevents/speech/brainard20181113a.htm ("Our existing regulatory and supervisory guardrails are a good place to start as we assess the appropriate approach for AI processes.... [W]e would expect firms to apply robust analysis and prudent risk management and controls to AI tools, as they do in other areas, as well as to monitor potential changes and ongoing developments."). Similarly, Federal Deposit Insurance Corporation ("FDIC") Chairman Martin Gruenberg has observed "[w]hatever the technology – including artificial intelligence – that is going to be utilized by a banking organization, that has to be utilized in a way that is in compliance with existing law, whether it's consumer protection, safety and soundness or any other statute.... Our agencies currently have authority to enforce those laws over the technology." Ebrima Santos Sanneh, Regulators Say They Have the Tools to Address AI Risks, American Banker (Jan. 19, 2024), https://www.americanbanker.com/news/regulators-say-they-have-the-tools-to-address-ai-risks#:~:text=WASHINGTON%20%E2%80%94%20Bank%20regulators%20said%20on,consumers%20or%20the%20financial%20system.

[20] *See* Financial Stability Oversight Counsel, Annual Report 2023 (Dec. 14, 2023), https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/studies-and-reports/annual-reports.

[21] *See, e.g.*, Speech of Michael S. Barr, Vice Chair of the Federal Reserve, Furthering the Vision of the Fair Housing Act (July 18, 2023), https://www.federalreserve.gov/newsevents/speech/barr20230718a.htm ("While [AI and machine learning] technologies have enormous potential, they also carry risks....Through our supervisory process, we evaluate whether firms have proper risk management and controls, including with respect to those new technologies."); Speech of Michael J. Hsu, Acting Comptroller of the OCC, Tokenization and AI in Banking: How Risk and Compliance Can Facilitate Responsible Innovation (June 16, 2023), https://www.occ.gov/news-issuances/speeches/2023/pub-speech-2023-64.pdf ("For banking, the potential benefits of more widespread adoption of AI are significant, but so are the risks....[The OCC is] committed to being agile and credible on financial technology developments so that we can balance prudence with innovation and growth.").

[22] *See, e.g.*, 12 C.F.R. Part 252 (Reg. YY); OCC, OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations, 79 Fed. Reg. 54,518 (Sept. 11, 2014), https://www.govinfo.gov/content/pkg/FR-2014-09-11/pdf/2014-21224.pdf (codified at 12 C.F.R. Part 30 App. D) (the "OCC Heightened Standards").

[23] OCC, Comptroller's Handbook on Corporate and Risk Governance, Version 2.2 at 55 (July 2019), "ERM helps the board and management view the bank's risks in a comprehensive and integrated manner." https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/corporate-risk-governance/index-corporate-and-risk-governance.html.

[24] Remarks by Carolyn G. DuChene, former OCC Deputy Comptroller Operational Risk, at the Bank Safety and Soundness Advisory Community Bank Enterprise Risk Management Seminar (Oct. 22, 2012), https://www.occ.treas.gov/news-issuances/speeches/2012/pub-speech-2012-150.pdf.

The Federal Reserve requires a bank holding company with total consolidated assets of $50 billion or more to maintain a global risk-management framework that is commensurate with its structure, risk profile, complexity, activities and size.[25] The risk management framework must include "policies and procedures establishing risk-management governance, risk-management procedures and risk-control infrastructure for its global operations; and processes and systems for implementing and monitoring compliance with such policies and procedures[.]"[26] The banking agencies have long recognized that "properly managing risks has always been critical to the conduct of safe and sound banking activities and has become even more important as new technologies, product innovation and the size and speed of financial transactions have changed the nature of banking markets."[27] The banking agencies generally require regulated entities to employ a risk-based approach in identifying, measuring, monitoring and controlling risks. A risk-based approach considers factors such as the size of the institution and the scope, nature and materiality of the proposed activities or related risks. Banking agency risk management regulations and guidance generally do not impose specific prescriptive requirements,[28] but rather articulate principles that may be applied as appropriate for a particular institution or a particular risk. This, in turn, affords banking organizations appropriate flexibility in applying their existing frameworks to new risks and opportunities.

Because an institution's risk management processes are expected to be risk-based and "are expected to evolve in sophistication, commensurate with the institution's asset growth, complexity and risk,"[29] there is no one-size-fits-all approach to risk management. Each banking organization's ERM and supporting implementation throughout the organization will look and operate differently in certain respects. Accordingly, the manner in and extent to which the aspects of risk management and risk management processes described in this paper are applied take into account various factors such as the characteristics of the institution, the technology at issue, the proposed use, the materiality of that use and the potential risks to the enterprise that may result.

Risks associated with the use of AI technology should be addressed through a banking organization's ERM framework, whether the AI technology is developed at the institution itself or through a third party providing AI-related services used by a banking organization. Within a banking organization's overall ERM framework, various underlying frameworks, processes and policies may be relevant to evaluating and using AI, including risk governance, model risk management (MRM), data risk management and third-party risk management (TPRM), each discussed in more detail below. Further, these underlying

[25] 12 C.F.R. §§ 252.22(a)(2) (bank holding companies with total consolidated assets of $50 billion or more); 252.33(a)(2) (bank holding companies with total consolidated assets of $100 billion or more). The OCC also expects national banks and federal branches of foreign banks with total consolidated assets of $50 billion or more to maintain risk governance frameworks that satisfy the standards established by the OCC. *See* OCC Heightened Standards.

[26] 12 C.F.R. §§ 252.22(a)(2); 252.33(a)(2).

[27] Federal Reserve, SR Letter 95-5, Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies (Nov. 14, 1995; rev. Feb. 26, 2021), https://www.federalreserve.gov/boarddocs/srletters/1995/sr9551.htm.

[28] For example, in the recent interagency guidance regarding climate-related risks, the banking agencies stated that "[e]ffective risk management practices should be appropriate to the size of the financial institution and the nature, scope, and risk of its activities." *See* Federal Reserve, FDIC, OCC, Principles for Climate-Related Financial Risk Management for Large Financial Institutions, 88 Fed. Reg. 74,183, 74,184 (Oct. 30, 2023), https://www.govinfo.gov/content/pkg/FR-2023-10-30/pdf/2023-23844.pdf.

[29] Federal Reserve, SR Letter 16-11, Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than $100 Billion (rev. Feb. 17, 2021), https://www.federalreserve.gov/supervisionreg/srletters/SR1611a1.pdf.

frameworks, processes and policies do not operate in silos; instead, they operate together and may, in some respects, complement one another or include elements that overlap. In the AI context, this may be particularly true given the myriad of possible uses of AI that could be employed throughout a banking organization and subject to its ERM framework. For example, MRM and TPRM may overlap when it comes to models developed by third parties. The banking agencies have recognized this overlap. In addition to interagency TPRM-specific guidance issued by the banking agencies (Interagency TPRM Guidance),[30] the agencies' Supervisory Guidance on Model Risk Management (SR 11-7)[31] addresses TPRM. The OCC Comptroller's Handbook on Safety and Soundness: Model Risk Management (Comptroller's Handbook on Model Risk Management) also discusses how third-party models should be incorporated into both TPRM and MRM.[32]

The following sections of this paper discuss four aspects of risk management within an institution's ERM framework that are particularly relevant to managing the risks associated with AI technologies: risk governance, MRM, data risk management and TPRM. Banking organizations are using their experiences with their current ERM processes to address risks relative to new AI technologies and continue to consider and develop best practices for integrating oversight of AI into the various risk frameworks on an ongoing basis. This paper discusses some of the ways in which existing frameworks are equipped to address AI, even though they may not have originally been developed with AI in mind.

A. General Risk Governance Practices

Banking organizations are required to have well-established risk governance practices and processes, which include reporting and committee structures, which allow boards of directors to oversee the risk management of a banking organization and allow senior management to stay informed of risks and make risk-based decisions about the day-to-day operations of the institution. Banking organizations apply these risk governance practices and processes to AI today, and the flexibility of these processes means they may be readily adapted to new and evolving technologies.

Boards of directors are primarily responsible for oversight of banking organizations, including reviewing and approving strategy and risk appetite, while day-to-day implementation and operational decisions are the responsibility of senior management. As Federal Reserve guidance states, "[a]n effective board oversees and holds senior management accountable for effectively implementing the firm's strategy, consistent with its risk appetite, while maintaining an effective risk management framework and system of internal controls."[33] Similarly, OCC guidance states that "a covered bank's board of directors should

[30] Federal Reserve, FDIC, OCC, Interagency Guidance on Third-Party Relationships: Risk Management (June 7, 2023), https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf.

[31] The Federal Reserve and OCC jointly issued the Supervisory Guidance on Model Risk Management, and the FDIC later issued the same guidance as well. Each of the agency's publications is cited, and we refer to the guidance as "SR 11-7" throughout the paper for convenience. *See* Federal Reserve, SR 11-7, Supervisory Guidance on Model Risk Management (Apr. 4, 2011), https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf; OCC, Bulletin 2011-12, Supervisory Guidance on Model Risk Management (Apr. 4, 2011), https://www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf; FDIC, FIL22-2017, Adoption of Supervisory Guidance on Model Risk Management (June 7, 2017), https://www.fdic.gov/news/financial-institution-letters/2017/fil17022.pdf.

[32] OCC, Comptroller's Handbook on Safety and Soundness: Model Risk Management Version 1.0 (Aug. 2021), https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/index-model-risk-management.html.

[33] Federal Reserve, SR Letter 23-1 / CA 21-1, Supervisory Guidance on Board of Directors' Effectiveness (Feb. 26, 2021), https://www.federalreserve.gov/supervisionreg/srletters/SR2103.htm.

actively oversee the covered bank's risk-taking activities and hold management accountable for adhering to [its risk governance framework]."[34] Boards of directors delegate management oversight and day-to-day operations to executive officers. The OCC Heightened Standards provide that a risk governance framework, which should be approved by the board of directors or its risk committee, "should include delegations of authority from the board of directors to management committees and executive officers as well as the risk limits established for material activities."[35] Oversight of an organization's risk management activities will look different depending on the organization's approach to risk and particular activities or risks in question.

Governance practices with respect to AI may include the incorporation of a cross-functional working group at the management level, which may be referred to as a steering committee, advisory forum or strategy council, among other names, with key stakeholders from across the organization, such as privacy, legal and compliance, cyber, enterprise architecture, model risk management, technology and other support functions, to ensure multiple perspectives. This type of group can enable managers and other experts across the organization to coordinate and manage the organization's use of AI on a day-to-day basis. This structure allows senior management to have increased visibility into and engagement with AI strategies and risk considerations and can be an effective supplement to the overall risk management framework discussed herein. This type of group may be responsible for several day-to-day actions or decisions, such as reviewing and recommending for approval specific AI use cases following technology, cyber, model risk, legal, third-party and potentially other reviews to ensure considerations from each relevant discipline are considered. This group may consider strategic alignment, opportunities, challenges and emerging risks and it may also be responsible for establishing or executing to a risk tolerance for a particular use case within the broader risk appetite and escalating any risks appropriately. These forums can complement other formal or informal governance structures, such as working groups or Centers of Excellence that banking organizations have created for AI. Such forums may facilitate top-down communication of enterprise priorities and align resources across lines of business and supporting functions to set enterprise-wide, high-level expectations in advance of any particular business line or function championing specific use cases under established processes that govern the introduction of any new products or services. In doing so, they may help organizations align on terminology, frameworks and platforms to help evaluate, implement and scale solutions. Leadership direction from effective working groups can be operationalized at either the enterprise level or by individual lines of business through the established governance processes discussed below.

Banking organizations have in place established governance processes that are designed to reasonably ensure that risks are effectively identified, measured, monitored and controlled by management and that those activities are properly overseen by the board. For example, banking organizations often utilize a three lines of defense framework for risk management, according to which the client-facing businesses and certain enterprise functions that support them are the first line of defense against potential risks, the second line of defense is the banking organization's independent risk management function and the third line of defense is the internal audit function. Reporting requirements allow the

[34] OCC Heightened Standards at 54,537.

[35] *Id*. at 54,574.

board of directors to stay informed of the risks facing the banking organization and monitor management's risk-taking within the risk appetite the board has established.[36] These processes should be applied to potential uses of AI, taking into account a variety of factors, such as the institution's business and business plans, materiality of the risks and risk appetite. Existing risk governance principles guide banking organizations in determining what types and levels of oversight may be needed for potential uses of AI, both at the board and management levels.

Banking organizations are supportive of the National Institute of Standards and Technology (NIST)[37] AI Risk Management Framework (AI RMF 1.0). The AI RMF notes that "maintaining organizational practices and governing structures for harm reduction, like risk management, can help lead to more accountable systems."[38] The "govern" function is one of four "core" functions of NIST's AI RMF 1.0. Similar to the concept of an ERM framework, MRM framework or other governance frameworks already in use in the banking industry that are applied across an organization, the AI RMF 1.0 notes that "[g]overnance is designed to be a cross-cutting function to inform and be infused throughout the other three functions."[39] The AI RMF 1.0 also allows for a principles-based approach that can include many of the same factors that banking organizations already consider in their overall risk governance frameworks. For example, "[g]overning authorities can determine the overarching policies that direct an organization's mission, goals, values, culture and risk tolerance. Senior leadership sets the tone for risk management within an organization, and with it, organizational culture. Management aligns the technical aspects of AI risk management to policies and operations."[40]

B. Model Risk Management

For decades, banking organizations have used models to achieve numerous objectives and have developed MRM frameworks aligned with the banking agencies' risk management standards and the guidance for models, including SR 11-7 and the Comptroller's Handbook on Model Risk Management. MRM frameworks are informed by experience, including experience with examiner expectations. As models have proliferated and become more complex over time, MRM frameworks at banking organizations likewise have evolved.

Similar to other banking agency guidance, SR 11-7 is risk- and principles-based and allows banking organizations to create MRM frameworks that are adaptable and complementary to other aspects of the organization's risk management framework. SR 11-7 acknowledges that "the extent and

[36] *See, e.g.*, OCC Heightened Standards at 54,528 ("[The three lines] … should establish an appropriate system to control risk-taking. These units should keep the board of directors informed of the covered bank's risk profile and risk management practices to allow the board of directors to provide credible challenges to management's recommendations and decisions."). *See also* FDIC, Risk Management Manual of Examination Policies, Section 4.1; Basel Committee on Banking Supervision, Review of the Principles for the Sound Management of Operational Risk at 4 (2014), https://www.bis.org/publ/bcbs292.pdf.

[37] BPI supports the work NIST has been doing with respect to AI and has been engaging with NIST to share the perspective of the banking industry. *See, e.g.*, BPI, Letter re Comments on the Four Principles of Explainable Artificial Intelligence (Draft NISTIR 8312) (Oct. 15, 2020), https://bpi.com/wp-content/uploads/2021/01/2020.10.15-BPI-Comments-on-the-Four-Principles-of-Explainable-Artificial-Intelligence-NISTIR-8312.pdf.

[38] U.S. Dept. of Commerce, NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0) at 16 (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[39] *Id*. at 20. See also *id*. at 22 ("Govern is a cross-cutting function that is infused throughout AI risk management and enables the other functions of the process…. Attention to governance is a continual and intrinsic requirement for effective AI risk management over an AI system's lifespan and the organization's hierarchy.").

[40] *Id*. at 22.

sophistication of a bank's governance function is expected to align with the extent and sophistication of model usage,"[41] which is consistent with general principles of risk management that require tailoring based on various factors, such as materiality, criticality to the business and risk appetite. For instance, where a particular AI model's use is "less pervasive and has less impact" on the financial condition of a banking organization, the approach to MRM may not need to be as complex.[42] The inverse is also true. SR 11-7 states that MRM overall "should include disciplined and knowledgeable development and implementation processes that are consistent with the situation and goals of the model user and with bank policy," even as the "appropriate selection of inputs and processing components" may vary based on the particular model at issue.[43]

MRM frameworks are important for the implementation of AI and are top of mind both for banking organizations and banking agencies. In some cases, AI technology may not obviously fit within the definition of a "model" for purposes of SR 11-7.[44] However, banking organizations, as well as the banking agencies, recognize that the guidance's risk-based principles to address new types of models could apply, even where the form of the models was not originally contemplated when the guidance was finalized. The Comptroller's Handbook on Model Risk Management recognizes that certain models or tools may not meet the formal definition of a model, but provides that these models and tools should still be subject to sound risk management principles, including effective risk identification and controls.[45] Controls, including with respect to model validation, training and usage, should be risk-based and the applicable controls may differ based on the model and use case. SR 11-7 emphasizes the need for "systematic procedures for validation [that] help the bank understand the vendor product and its

[41] SR 11-7 at 16.

[42] *Id*. at 5.

[43] *Id*.

[44] *Id*. at 3. *See also* BPI, Letter re Joint Agency AML and Sanctions RFI (June 11, 2021), https://bpi.com/wp-content/uploads/2021/06/BPI-Letter-re-Joint-Agency-AML-and-Sanctions-MRM-RFI-2021.06.11.pdf (citing FRB, FDIC, OCC, Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance (Apr. 9, 2021), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20210409a2.pdf).

[45] Comptroller's Handbook on Model Risk Management at 13. ("Sound risk management should be applied to models and tools not meeting the definition of a model described in [SR 11-7]. Risk management of AI, as with any other innovative technology, should be commensurate with the materiality and complexity of the model or tool and the activity's risk or business process that the AI is supporting. Sound AI risk management typically includes:

- appropriate due diligence and risk assessments as AI is implemented.
- sufficiently qualified staff to implement, operate, and control the risks associated with AI.
- an inventory of AI uses.
- identification of the level of risk associated with each AI use.
- establishment of clear and defined parameters governing the use of AI.
- effective processes to validate that AI use provides sound, fair, and unbiased results.
- effective technology controls, such as system and data access, identity and authorization, system integration, separation of duties, configuration management, vulnerability management, encryption, malware controls, business resilience, system change control, monitoring and logging, data management, and other similar controls.")

Likewise, in the BSA/AML context, the banking agencies have recognized that not all of the systems banks use for BSA/AML compliance may meet SR 11-7's definition of a model. *See* Federal Reserve, FDIC, OCC, Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance at 3 (Apr. 9, 2021), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20210409a2.pdf. However, they note that, while "there is no specific organizational structure required for oversight by the bank," SR 11-7 "provides principles that may be helpful in managing the BSA/AML compliance program." *Id. See also* Ebrima Santos Sanneh, Regulators Say They Have the Tools to Address AI Risks, *supra* note 19 (Vice Chair for Supervision Barr "noted that firms that utilize newer techniques of artificial intelligence like large language learning models need to make sure that the tech complies with the agencies' model risk management expectations.").

capabilities, applicability and limitations."[46] While the specific validation procedures may vary with AI, the general risk practices can be applied, and the guidance provides a framework for banking organizations to rely on as specific procedures continue to develop alongside technological advancements.

SR 11-7 provides certain guidance that should be applicable to the development, validation, implementation and use and governance of many models, including many AI tools, and banking organizations should consider all controls available to them to address SR 11-7 concerns when assessing the risk of AI models in a particular use case. For example, with respect to model validation, SR 11-7 sets out three key elements of an effective validation framework: (1) evaluation of conceptual soundness, (2) ongoing monitoring and (3) outcomes analysis.[47] These elements should generally apply to many AI tools, even if their practical application may vary depending on the technology or use case.

Banking organizations are aware that the application of MRM guidance to certain AI tools presents unique challenges, in comparison to its application to models that more obviously fit within the scope of SR 11-7. Generative AI or other AI tools based on deep learning or neural network architectures are not easily evaluated using traditional validation techniques. For example, many such models have a large number of parameters and are designed to operate on a wide range of potential input data, which makes it difficult to validate these models under every scenario. Some AI models, such as LLMs and other generative AI tools, may be trained on massive amounts of data that is of uneven quality, and the exact nature of the training data used may not be available to a banking organization in the case of proprietary third-party models, as discussed below. This can pose different validation challenges than models with limited input data and specific outputs. The use of Small Language Models (SLMs) specifically trained and or fine-tuned on bank-specific data can help mitigate potential risks. The flexible principles of SR 11-7 provide guidance that may be applied even to these new types of AI tools, such as LLMs. The banking industry may leverage these principles as it has to manage other developing technologies, even if the validation and testing techniques required for generative AI and LLMs may be different.

These flexible principles are relevant for considering explainability, which is also an important consideration in applying MRM principles to AI tools (depending on the use case) and will likely require different techniques than those applied to traditional models to explain how or why AI tools generate specific outputs in response to given inputs. Indeed, the Comptroller's Handbook on Model Risk Management indicates that a bank's model risk assessment methodology should consider explainability for AI models, and notes that, while "[t]ransparency and explainability are key considerations that are typically evaluated as part of risk management regarding the use of complex models . . . [t]he appropriate level of explainability . . . depends on the specific use and level of risk associated with that use."[48] As banking organizations work to address these challenges, in some cases, SR 11-7 provides flexibility to address challenges with respect to MRM within the broader ERM framework, whether or not an AI tool would constitute a model under its definition. For example, SR 11-7 explains that if it is

[46] SR 11-7 at 16.
[47] *Id.* at 11.
[48] Id. at 40.

not "feasible to conduct necessary validation activities prior to model use because of data paucity or other limitations, that fact should be documented and communicated in reports to users, senior management and other relevant parties. In such cases, the uncertainty about the results that the model produces should be mitigated by other compensating controls."[49] This flexibility permits the use of compensating controls to address the limitations of traditional validation techniques when applied to AI tools. Compensating controls institutions may employ include testing, performance monitoring, red teaming, outcome analysis, benchmarking and appropriate documentation of the limitations of the validation performed. In addition, banking organizations evaluate the use of AI in a risk-based manner that varies based on the use case through the processes established as part of their ERM frameworks.

Ultimately, as the Comptroller's Handbook on Model Risk Management notes, "Regardless of how AI is classified (*i.e.*, as a model or not a model), the associated risk management should be commensurate with the level of risk of the function that the AI supports."[50] As the OCC recently observed in the Fall Risk Perspective,[51] banking organizations can apply their MRM frameworks developed in alignment with existing guidance and regulations, including SR 11-7, as a component of their risk management of AI when and as appropriate as one of many frameworks that enables successful implementation of AI. While some of the specific mechanisms of model validation may be subject to further consideration, particularly in the context of generative AI, they are supplemented by the broader ERM framework which helps ensure a cohesive approach to risk throughout the organization.

C. Third-Party Risk Management

The implementation of AI by banking organizations may use and build upon or involve the engagement of third parties for, among other things, the provision of the AI models and the cloud services through which AI models are accessed or used. Internally, banking organizations may also develop proprietary AI models or employ open-source AI models that are generally publicly available and freely modifiable. In either case, AI models may be trained on data provided by the developer of the model, third-party data sourced by the developer of the model or the banking organization that uses the model, publicly available data or a combination of any or all of these sources. In the case of generative AI models, such as LLMs, the most sophisticated models are currently proprietary to third-party vendors such as OpenAI/Microsoft or Google.[52] In addition, third-party service providers may employ AI to facilitate the services they provide to banking organizations, even if those services are not directly related to AI.

Banking organizations have developed robust TPRM governance processes for assessing and managing the risks associated with third-party relationships. The banking agencies' guidance on this subject has

[49] SR 11-7 at 10.

[50] Comptroller's Handbook on Model Risk Management at 4.

[51] Fall Risk Perspective at 23.

[52] In a recent speech, Securities and Exchange Commission Chair Gensler pointed out that "we've already seen affiliations between the three largest cloud providers and the leading generative AI companies." SEC Chair Gensler, AI, Finance, Movies, and the Law Prepared Remarks before the Yale Law School (Feb. 13, 2024), https://www.sec.gov/news/speech/gensler-ai-021324#_ftn7.

also evolved, culminating in the Interagency TPRM Guidance that was released in June 2023.[53] The Interagency TPRM Guidance discusses sound risk management principles for banking organizations when developing and implementing risk management practices for all stages in the life cycle of a third-party relationship, from planning and due diligence through contract negotiation and ongoing monitoring and, eventually, termination.

The Interagency TPRM Guidance also provides guiding principles for solutions where it is not possible to obtain all desired due diligence information from a third party. In that case, the TPRM Guidance provides that a banking organization should identify and document the limits of its due diligence, understand the risks from such limitations and consider alternatives as to how to mitigate the risks.[54] It also provides that a banking organization in such a position may, for example, "obtain alternative information to assess the third party, implement additional controls on or monitoring of the third party to address the information limitation or consider using a different third party."[55] First, the Interagency TPRM Guidance emphasizes the importance of conducting diligence and ongoing monitoring on a third-party service provider, both during the contract negotiation stage and on an ongoing basis over the course of the relationship.[56] However, the Interagency TPRM Guidance acknowledges that it is not always possible to obtain the desired due diligence information from a third party.[57] Although the Interagency TPRM Guidance does not explicitly discuss AI or other technologies, this challenge may be particularly acute for banking organizations seeking to implement third-party AI models into their businesses. For example, the third party may not be willing to disclose sufficient information about its proprietary model, or the banking organization may not have sufficient expertise to fully understand the model. In addition, banking organizations may face "nth party" risk where the chain of risk dependencies extends beyond the third-party vendor with which the banking organization has a relationship, especially if a model is trained on data that the third party has obtained from a different source.[58]

To mitigate these risks, banking organizations should establish suitable compliance and monitoring standards or consider avoiding these risks entirely. These standards would include existing TPRM frameworks, plus contractual provisions such as indemnification, and would warrant serious consideration before onboarding an AI model where the information or representations and warranties provided by a third party, or nth party, does not permit a banking organization to validate the appropriateness of a model for a particular use case.

According to the Interagency TPRM Guidance, ongoing monitoring typically includes "relevant audits, testing results, and other reports that address whether the third party remains capable of managing

[53] The Interagency TPRM Guidance follows the banking agencies' principles-based approach and requires each financial institute to make its own assessment of the relevant risks. "[A]s part of sound risk management, it is the responsibility of each banking organization to analyze the risks associated with each third-party relationship and to calibrate its risk management processes, commensurate with the banking organization's size, complexity, and risk profile and with the nature of its third-party relationships…. Banking organizations have flexibility in their approach to assessing the risk posed by each third-party relationship and deciding the relevance of the considerations discussed in [this] guidance." Interagency TPRM Guidance at 37,923.

[54] *Id.* at 37,929.

[55] *Id.*

[56] *See id.* at 37,929.

[57] *Id.*

[58] *See id.* at 37,925.

risks and meeting contractual obligations and regulatory requirements." A banking organization's ongoing monitoring of a particular provider may need to be adapted to adequately monitor the risks posed by the third party's provision of AI technology. The challenges in monitoring the relevant third party may be particularly significant for third-party proprietary LLMs and other generative AI models, for which model architectures, the data used to train the models, and the approach used by the third party to mitigate risks associated with the models may be proprietary information that is not fully available to the banking organization employing these models.

The Interagency TPRM Guidance emphasizes the importance of evaluating the third party's legal relationship with the banking organization, as well as its legally binding arrangements with subcontractors and other parties. At the same time, the Interagency TPRM Guidance also recognizes the difficulty that banking organizations may encounter when they have limited negotiating power. This difficulty may be heightened for banking organizations wishing to procure AI services from third parties in the current environment because of the overwhelming demand, both on the part of organizations and consumers, for such services and the limited number of providers. In situations where banking organizations lack negotiating power, the Interagency TPRM Guidance emphasizes the need for banking organizations to understand "any resulting limitations and consequent risks," noting that if a contract is unacceptable to a banking organization, it may consider other approaches, such as employing other third parties or conducting the activity in house, or negotiating contracts as a group with other organizations.[59] As noted above, today's most sophisticated LLMs are proprietary to third-party vendors, and generally there are a small number of such vendors, which may exacerbate this risk or limit the other approaches that are available to banking organizations.

Publications regarding emergent technologies that rely on third-party vendors also address challenges that banking organizations face when applying certain TPRM principles. For example, many of the examples in the U.S. Department of the Treasury's report entitled The Financial Services Sector's Adopting of Cloud Services (Treasury Cloud Report)[60] are relevant to AI, and a number of those echo some of the difficulties discussed in the Interagency TPRM Guidance, including the level of transparency needed to support due diligence and monitoring and dynamics in contract negotiation,[61] as discussed above. The Treasury Cloud Report highlights a potential for concentration risk, which is also relevant in the AI context because the current market for AI services (like the market for cloud services) is concentrated in a limited number of providers. Thus, many banking organizations could be exposed to those providers, and a single incident (*e.g.*, an outage at a particular AI services provider) could affect multiple banking organizations.

Concentration risk could be a concern for individual banking organizations, as a banking organization may have to rely upon a single service provider for the provision of all their AI services the institution utilizes, leaving parts of the banking organization exposed to the effects of an incident at that service provider. This can heighten the risks posed by the third-party relationship, affecting how the banking

[59] Id. at 11.
[60] U.S. Department of the Treasury, The Financial Services Sector's Adopting of Cloud Services (Feb. 8, 2023), https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.
[61] *Id.* at 6 –7.

organization manages the relationship within its TPRM framework. However, concentration risk could extend beyond individual banking organizations if a large number of institutions rely on a small number of technology providers.[62] Banking organizations have been navigating these challenges in connection with the implementation of other technologies or similar services and are able to use insights from past experiences to help inform third-party risk management with respect to AI.

D. Data Risk Management

In each application of AI technologies, effective data governance and risk management are pivotal. Existing laws, regulations, principles and regulatory expectations outline how banking organizations should manage and govern data risk, including data risk related to the use of AI technology. These include, but are not limited to, the Basel Committee on Banking Supervision standard 239 (BCBS 239),[63] the Federal Financial Institutions Examination Council's Architecture, Infrastructure, and Operations examination handbook (AIO Booklet),[64] SR 11-7, and the Gramm-Leach-Bliley Act (GLBA)[65] and similar data protection obligations. Through data risk management frameworks, banking organizations manage and govern end-to-end data flow, including risks that arise from inaccurate data or the inappropriate use, dissemination, or understanding of data.

BCBS 239 principles include expectations that data is and should remain accurate, complete, timely, available, adaptable and fit for purpose. Fitness for purpose and other use case assessments and evaluations determine whether the proposed use of the data is restricted by contract, law or other data management risk principle or regulatory expectation. Data risk management and governance includes data capture controls, data lineage and data tracing evaluations, data defect management, data use assessments and requirements documentation and data quality metrics.

The AIO Booklet has outlined additional risk-management considerations including the establishment of a Chief Data Officer and a data management and data governance program. The Chief Data Officer has many responsibilities, including but not limited to developing and maintaining data-related policies, data life cycle management, data asset management, oversight of compliance with applicable laws and regulations and conformance with data management industry practices.[66] In addition, the Chief Data Officer should provide governance of the use of data as an asset and assist in protecting that data and deriving maximum value from it.

Data protection risk, including data privacy risk, is an additional type of data risk. Data protection obligations for banking organizations are similarly well established under the GLBA, the Fair Credit Reporting Act (the FCRA),[67] and similar data protection requirements. Established data protection laws, regulations, and guidance compel banking organizations to embed security, data minimization, purpose

[62] *See, e.g.*, Id. at 7 ("[C]oncentration could expose many financial services clients to the same set of physical or cyber risks (e.g., from a region-wide outage), and addressing such risks may necessitate action on the part of each financial services client.").

[63] Basel Committee on Banking Supervision, Principles for Effective Risk Data Aggregation and Risk Reporting (Jan. 2013), https://www.bis.org/publ/bcbs239.pdf.

[64] Federal Financial Institutions Examination Council, Architecture, Infrastructure and Operations (June 2021), https://ithandbook.ffiec.gov/media/ywfm2ftz/ffiec_itbooklet_aio.pdf.

[65] Gramm-Leach-Bliley Act, Pub. L. No. 106-102 (codified at 12 U.S.C. § 1811 *et seq.*).

[66] AIO Booklet at 9.

[67] 15 U.S.C. § 1681 *et seq.*

specification, use limitation, transparency, and choice principles into their overall data strategy. Although the GLBA and FCRA are primarily designed to protect consumer data, additional data protection obligations exist for processing commercial and employment-related data.

As reliance on third-party data providers (including third-party model providers and their increasingly sophisticated technology) evolves, so too do data management programs. Additional requirements placed upon third-party data providers could help banking organizations obtain greater transparency, comfort, and reliance on the "big data" being provided so that banking organizations can rely on such data and adequately perform their established data management processes (*e.g.*, fitness-for-purpose evaluations). As an example, under the FCRA, a third-party consumer reporting agency is held to a "maximum possible accuracy" standard that banking organizations can rely on, and consumer reporting agencies achieve this standard, at least in part, due to consumer notice, access and correction rights.

Banking organizations largely have been able to apply their established data risk governance programs to manage data risk. The efficacy of these data management and governance frameworks and industry standard practices is reflected in the policies, procedures, and programs seen across banking organizations. These established data risk management programs speak to the positive impact that existing regulatory expectations and requirements have created in the banking sector.

V. Sample Use Cases

As noted above, banking organizations have used AI for many years in connection with a wide variety of activities and are continuing to explore many more possible use cases. Current and potential use cases vary among banking organizations from customer service to cybersecurity, fraud, anti-money laundering and back-office management, as BPI has previously advocated.[68] For illustrative purposes, below we provide a brief summary of two use cases for AI: mitigating cybersecurity and fraud risks and enhancing Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance.

1. ***Cybersecurity/Fraud Prevention.*** In many cases, banking organizations are using, or are considering using, AI tools to address emerging risks to their businesses that are driven by external actors using similar technologies. For example, AI models, including generative AI tools, are being evaluated or piloted to enhance operational efficiencies and risk mitigation in the cybersecurity and fraud prevention contexts. In those contexts, ML tools are currently being used by some banking organizations to automate labor-intensive tasks in fraud and cybersecurity risk management, such as responding to spam/phishing attempts and enhancing threat awareness. However, as the technology becomes more sophisticated, there may be opportunities for an increasingly important role in other areas of fraud prevention such as anomaly detection and behavior analysis.

[68] *See, e.g.*, BPI Letter regarding Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning (Docket No. OCC-2020-0049; OP-1743; RIN 3064- ZA24; CFPB 2021-0004; NCUA 2021-0023) (June 25, 2021), https://bpi.com/wp-content/uploads/2021/06/BPI-Comment-Letter_Interagency-RFI-on-AI_Final-06.25.2021.pdf.

2. ***BSA/AML.*** Many banking organizations also use AI tools to enhance existing processes that facilitate compliance with BSA/AML and sanctions legal requirements and banking agency expectations. Some of these tools flag potentially suspicious activity, such as suspected money laundering, or potential sanctions concerns. These tools have the potential to improve the detection of suspicious activity, quickly process complex patterns in data and possibly improve reporting times.[69]

Adoption of AI tools in these areas is particularly important, given the bad actors who employ AI to perpetrate crimes.[70] The need for speed and agility in combatting these threats is not a concept unique to the implementation of AI, but rather is a consistent theme in the banking sector's response to other technological advancements and adversarial tactics. This approach is rooted in past experience coordinating with banking agencies to enable banking organizations to be forward-thinking and resilient in the face of ever-evolving threats. Even with these aggressive pressures by bad actors constantly changing tactics and employing emerging technologies, banking organizations generally adopt a measured, risk-based approach to integrating AI into their operations. This approach carefully balances the risks associated with rapid technology implementation against the risks of moving too slowly or not adopting new technologies at all. The ability to use AI tools to combat AI-driven threats may prove essential to promoting safety and soundness.

VI. Conclusion

The banking sector and government agencies agree that the safe and sound implementation of AI technologies is in everyone's interest. An ongoing dialogue with regulators and other stakeholders is vital to addressing the complexities of AI, particularly as evolving technologies introduce or increase potential challenges, such as accuracy and explainability. Collaboration within the industry and reliance on comprehensive, principles-based frameworks within a broader ERM framework are key for banking organizations to integrate new AI tools such as generative AI tools safely, soundly and fairly into their operations. This approach will enable them to capture the benefits of AI while minimizing its potential risks. As AI and other technologies advance, it is crucial to leverage ongoing conversations that draw on the experiences and expertise of both banking organizations and banking agencies.

The financial industry has a history of responsibly adopting emerging technologies, including ML, by employing mature governance and risk management practices. Similarly, the industry is now approaching the implementation of generative AI to drive innovation following the same risk-based approach. Given the rapid pace of technological evolution, navigating the complex landscape of regulation, collaboration and transparency is imperative.

To this end, there are four critical areas where focused discussions can lead to meaningful outcomes:

1. **Explainability**: All stakeholders could benefit from dialogue around expectations and standards for generative AI models and new, multi-modal forms of AI, as traditional concepts of

[69] *See* BPI Letter regarding Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning, *supra* note 68.

[70] https://bpi.com/distributed-ledger-technology-enhancing-the-current-regulatory-approach/

explainability and transparency may pose particular challenges when it comes to the validation of AI tools. Although these challenges may raise concerns about accountability and fairness, collaboration on expectations around risk management practices can make it possible to achieve interpretable and trusted outcomes. Similarly, engagement on testing and ongoing monitoring of AI may be beneficial, especially as AI models increasingly change or update themselves based on data or user feedback.

2. **Application Commensurate with Risk:** As best practices around AI use continue to develop, further discussion should consider distinguishing more complex AI tools or models, or those that are applied to more complex or critical use cases, from simpler AI applications. For example, credit underwriting decisions and traditional spreadsheets may both use tools that are considered AI, but the complexity of the tools and the potential impact differ significantly depending on their use and expected outcomes. Similarly, it is critical that working definitions for models and AI are precise enough to clearly identify what is in scope and subject to governance and risk management practices. MRM and AI governance practices should mesh effectively to ensure a risk-based approach and appropriate oversight given the potential risks.

3. **Third-Party Risk Management**: As reliance on third-party AI models and solutions grows, transparency and accountability issues become increasingly significant. Establishing clear expectations around transparency with third-party AI providers, especially regarding the operation of their products, is essential. Focused discussions can uncover strategies to enhance due diligence and ongoing monitoring processes for third-party AI model providers, aiding banking organizations in maintaining compliance with regulatory standards and managing the complexities of certain AI models.

4. **Model Validation**: AI tools may not meet the definition of a model under SR 11-7 and may require different validation techniques than those used to validate models that do meet that definition. As these techniques continue to be developed, collaboration between the banking agencies and industry will be necessary to determine how the techniques fit into the existing MRM guidance. In addition, while the banking agencies have acknowledged that SR 11-7 provides principles that may be applied to tools that do not meet its definition of a model, further consideration of which principles may be most useful in the context of AI may be beneficial.

By adhering to mature governance and risk management practices and addressing these areas with a proactive and collaborative approach, we can harness the potential benefits of AI technologies while navigating the complexities that often accompany emerging technologies.