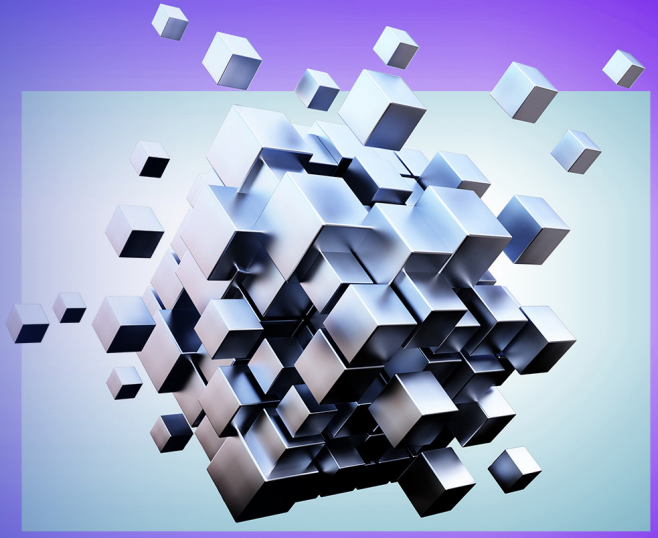
Artificial Intelligence and Model Risk Management



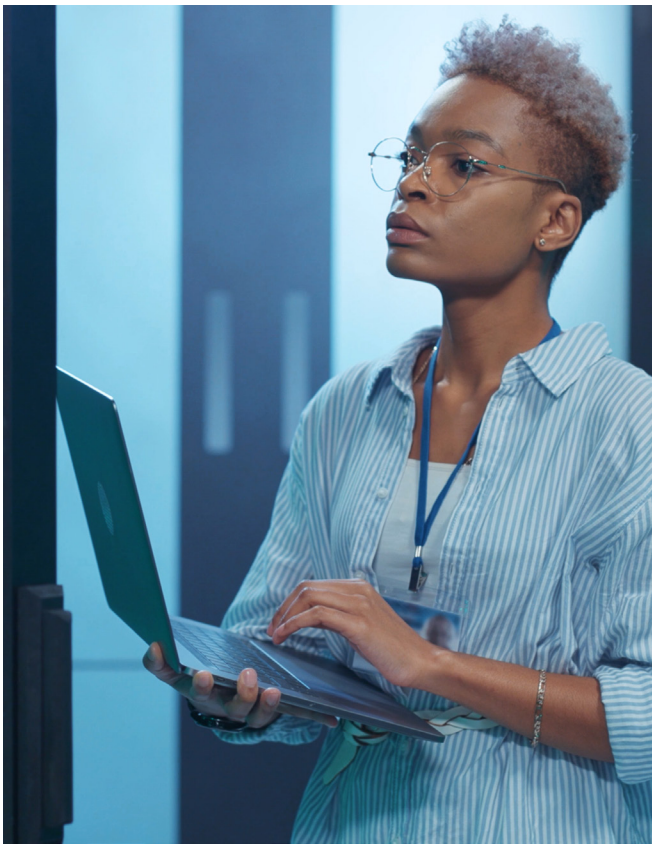
With increasing availability of data, enhancements to computational power coupled with growing interest in Artificial Intelligence (AI) and Machine Learning (ML), AI/ML adoption in financial services is expected to continue to increase and play a more prominent role. While regulators around the world are actively pursuing safe, sound, and responsible ways for this adoption, it is critical to strike a balance that fosters innovation without compromising model risk management (MRM).

One of the first questions financial institutions should ask themselves when building and implementing AI/ML technology is whether it meets the organization's definition of a model. More times than not, the answer is yes given the conventional components of a model (input, calculation, and output).

While there is wide debate about whether AI/ML technology should be managed through the existing MRM framework, existing MRM prudential guidelines (e.g., FRB SR 11-7/OCC 2011-12, FHFA AB 2013-07, etc.) offer a strong foundation for managing the key risks associated with AI/ML models and thus should serve as the starting point for governing these models. Discussions with the top ten largest banks in the US by asset size asserts that this is indeed the way the industry is approaching the adoption of AI/ML.

Recent developments in the European Union, the United Kingdom (UK), Canada, and Singapore provide insight into how global regulators are expecting financial institutions to manage AI/ML model risk. The Bank of England (BoE) states that the proposed principles and expectations in their MRM framework cover all elements of the model lifecycle and are applicable to all types of models, including AI/ML models (DP5/22, CP6/22). The new rules from the BoE are more prescriptive with performance testing on models that dynamically recalibrate or change autonomously in response to new inputs. The definition of a model is also much broader, which will likely increase financial institutions' model inventory and cover AI technology that may not have previously fallen within the MRM framework.

Despite the evolving challenges presented by AI/ML models, the existing MRM guidelines provide a robust foundation for tacking these issues. In the following discussion, we outline our perspective on how the current MRM framework, as detailed by SR 11-7, can be further strengthened to effectively address key challenges related to AI/ML models.



1 Governance

The importance of strong governance, policies, and controls that is commensurate with the complexity, materiality, and purpose of a model is clearly outlined in the SR 11-7 MRM framework. Financial institutions must promote enterprise-wide oversight at the highest levels of leadership, with the objective of ensuring that the level of model risk is effectively understood, managed, and within their tolerance.

The additional challenges that arise in AI/ML models due to interpretability & explainability, modeling techniques, and model monitoring require strong, holistic governance that promotes a culture of responsibility and accountability around the use of AI/ML within an organization. While MRM will play a lead role, it is also imperative that other stakeholders play key roles such as operational risk (model misuse) and compliance (potential model bias).

2 Interpretability & Explainability (Transparency)

AI/ML models are often perceived as "black boxes" due to the opaque model training process and challenges deciphering marginal effects. Interpreting and explaining the model can be a significant challenge. SR 11-7 mandates that the model methodologies and processing components that implement the theory, including the mathematical specification and the numerical techniques and approximations, should be explained in detail with particular attention to merits and limitations. The guidance also underscores the importance of subjecting the model to effective challenges regarding its conceptual soundness as a key aspect of independent validation. By following SR 11-7, we believe approaches such as feature importance analysis, local and global interpretability can be employed to address issues related to interpretability and explainability.

3 Model Monitoring

The performance of AI/ML models may change over time due to "data drift", "feature drift" or "model drift" and thus requires close monitoring. SR 11-7 underscores ongoing monitoring as a fundamental component of the model validation process, confirming that the model is appropriately implemented and performing as intended. We believe many of the suggested tests outlined in the guidance for ongoing monitoring, such as sensitivity analysis and benchmarking, are applicable to AI/ML models. The guidance is broad enough to state that monitoring should be commensurate with the model's purpose and ongoing usage. As AI/ML models scale in complexity and frequency, the framework expects that monitoring would effectively identify model limitations, performance deterioration, or risks.

Other Considerations

While the current MRM framework serves as a good starting point for governing AI/ML models, we believe there are areas that are not covered by the existing framework and thus should be considered by the financial services industry.

Data Lineage & Security: Data related risks can amplify risks in AI, and therefore the importance of strong data controls, policies, and governance around collection, lineage, and quality is critical. Financial institutions should have proper management and controls that enforce consent, privacy, protection, and security of personal data.

Consumer Protection: AI has the ability to derive complex patterns and understandings of consumers, which could lead to (improper) exploitation of biases or discrimination, vulnerabilities, and improper personalization and exclusions from certain products (see CFPB's recent guidance on fair lending).

Competition: AI systems may increase the cost of entry into a market, hindering competition. AI could also potentially create collusive business strategies that create harmful scenarios for markets.[1]

Financial Stability and Market Integrity: Financial stability and markets could become vulnerable to manipulation and volatility through things like algorithmic trading, opaqueness of third-party vendors, and unclear objective functions and reinforced learning.

Ethics: AI ethics can be defined as a set of values, principles, and techniques that employ widely accepted standards of right and wrong to guide moral conduct in the development and use of AI technologies.[2] Financial institutions should ensure that the use of AI tools do not conflict with ethical economic and societal objectives.

[1] Calvano, Emilio and Calzolari, Giacomo and Denicolo, Vincenzo and Pastorello, Sergio, April 1, 2019. "Artificial Intelligence, Algorithmic Pricing and Collusion", *SSRN*.

[2] Leslie, D.: Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute. (2019)

Conclusion

While AI/ML technology is new and emerging, the existing US MRM framework provides a solid foundation for addressing the distinctive challenges presented by this evolving technology. This perspective aligns with the majority of financial services organizations in the US. Although enhancements to the current framework are imperative to ensure comprehensive coverage for AI-related risk management, it is not productive to discard the existing structure and start anew.

Should you have any questions, need additional information, or would like to discuss the contents of this white paper in greater detail, please feel free to contact:

Anthony Sepci
Partner, KPMG LLP
E: asepci@kpmg.com

Adam Levy
Principal, KPMG LLP
E: adamlevy@KPMG.com

Paul Fagone
Principal, KPMG LLP
E: paulfagone@kpmg.com

Hanzhao Xing
Director, KPMG LLP
E: hxing@kpmg.com

Sean Sexton
Director, KPMG LLP
E: smsexton@Kpmg.Com

kpmg.com/socialmedia