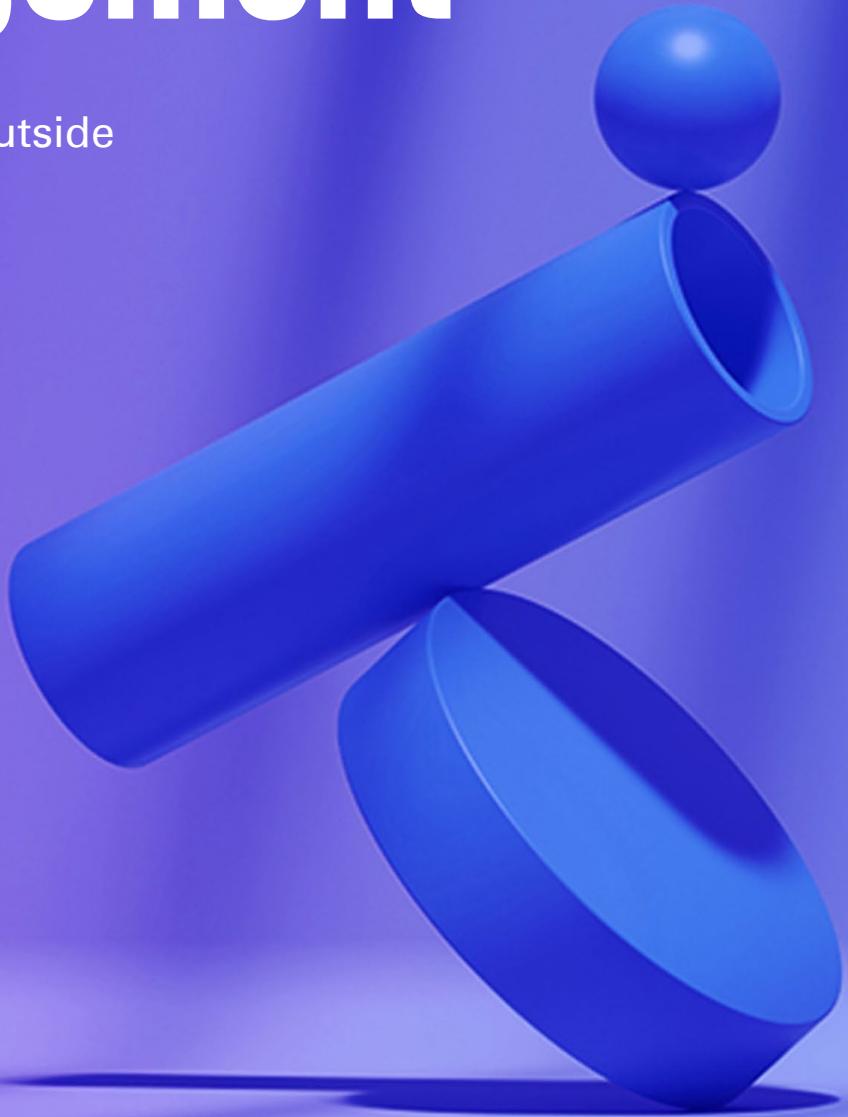




Model risk management

A prudent blueprint outside
of financial services







What is model risk?

Model risk refers to the potential for adverse outcomes stemming from models producing incorrect or misleading results. This risk originates not only from design flaws, data inaccuracies, or implementation errors but also significantly from the misuse of models. Misuse can occur when models are applied in contexts for which they were not designed, or when model outputs are interpreted incorrectly or manipulated. In the context of artificial intelligence (AI) and machine learning (ML), model risk encompasses the inaccuracies and uncertainties inherent in models that process and analyze vast data sets to make predictions, decisions, or recommendations. This risk is amplified by the complexity, opacity, and dynamic nature of AI/ML models, making it challenging to predict and quantify the ramifications of model failures accurately.



Why does model risk matter?

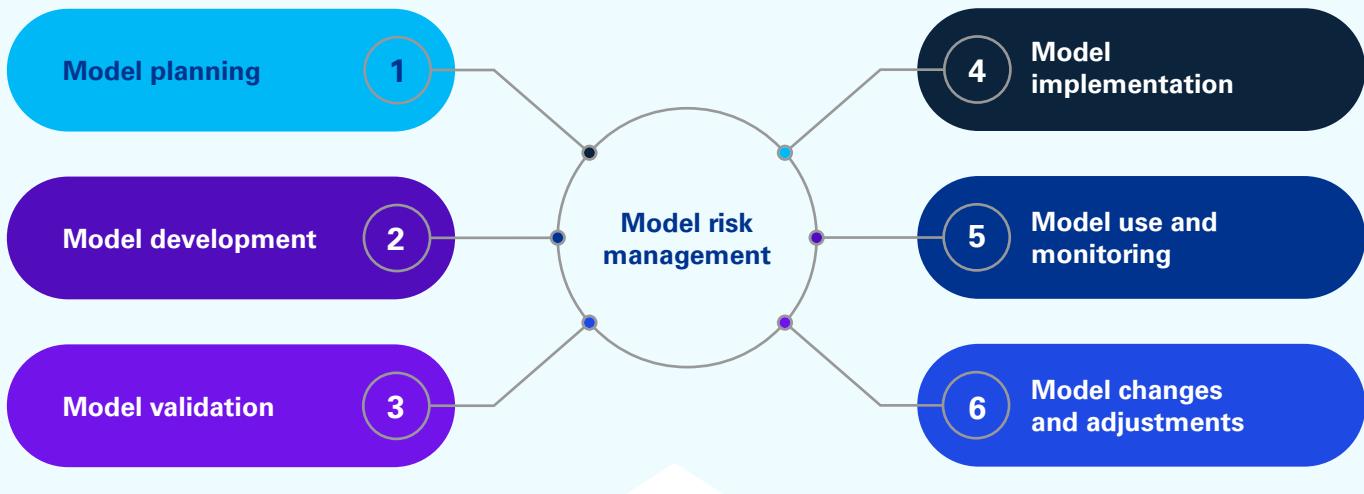
The impact of model risk can extend far beyond mere financial losses, touching on ethical, societal, and safety issues. To pull on an example many are likely familiar with at this point, in the field of automotive engineering, AI and ML models play a central role in the development of autonomous vehicles. These models must accurately interpret sensor data to make split-second decisions regarding vehicle navigation and safety. A failure in these models, such as misinterpreting a stop sign as a yield sign due to flawed training data, could lead to severe accidents, endangering passengers and pedestrians alike.

This sort of example, which can be made for many engineering problems and increasingly in the realm of healthcare, underscores the importance of managing model risk not only to prevent economic losses but also to protect public trust and ensure the ethical and safe application of AI/ML technologies.



What is model risk management?

Model risk management (MRM) is a structured, iterative approach to identifying, assessing, mitigating, and monitoring the risks associated with the use of models. It involves a set of practices designed to ensure models are developed, implemented, and used appropriately, especially in relation to their potential impact on decision-making processes. KPMG outlines a MRM lifecycle that encompasses six key stages:



1 Model planning: This initial phase involves defining the scope, objectives, and design of the model. It includes identifying the decisions the model will inform and the potential risks associated with its application, laying the groundwork for a risk-aware development process.

2 Model development: In this stage, models are built according to the specifications established in the planning phase. This includes selecting appropriate data, methodologies, and algorithms. Documentation of the development process is an expected output from this stage to facilitate both transparency to independent parties and subsequent validation efforts.

3 Model validation: The process that evaluates a model's theoretical framework, data input, output, and underlying assumptions to confirm its appropriateness for the intended purpose(s). It involves both quantitative and qualitative assessments to identify any issues in the model's design, data quality, or operational functionality. Validation is an ongoing necessity, extending beyond initial deployment to address

any changes in model use, data, or surrounding circumstances that could affect performance.

4 Model implementation: Once validated, the model is deployed within its operational environment. This stage requires integration into existing systems and processes, ensuring that the model operates as intended in real-world conditions.

5 Model use and monitoring: Models should be monitored on an ongoing basis to ensure that they continue to perform as expected over time. This includes tracking the model's output, assessing its impact on decision-making, and identifying any drift in performance or changes in the underlying assumptions that may necessitate adjustments.

6 Model changes and adjustments: The lifecycle is iterative, and models may require adjustments in response to performance issues, changes in the operational environment, or shifts in the model's objectives. This stage involves reviewing and implementing necessary changes to the model, followed by revalidation to ensure continued accuracy and reliability.



Benefits of establishing a model risk program

1

Enhanced model accuracy and reliability:

A structured model risk program involves validation and testing of models before their deployment and during their operational life. This process helps in identifying and correcting errors, enhancing the models' accuracy and reliability. For instance, continuous validation of an AI model used in predicting patient drug responses can lead to more personalized and effective treatment plans, positively impacting patient recovery rates.

2

Stakeholder confidence:

Transparent MRM practices, including comprehensive documentation and clear communication of model functionalities and limitations, build stakeholder confidence. Patients, for example, are more likely to trust and accept AI-driven healthcare solutions when there is clear evidence of their reliability and the care taken to minimize risks. Similarly, consumers' confidence in autonomous vehicles increases with transparency about the safety measures and continuous monitoring protocols in place to ensure vehicle AI systems perform as intended.

3

Liability mitigation:

By demonstrating due diligence in the development, validation, and monitoring of models, organizations can provide evidence of their efforts to anticipate and manage potential model risks. In the event of legal action, being able to demonstrate that the company had a comprehensive risk management process in place can be a powerful defense. It shows diligence in attempting to prevent harm or loss, which can mitigate liability or reduce the severity of judgments against the company.



Foundational elements of a MRM program

1 Governance structure:

Effective MRM begins with the establishment of a clear governance structure. This structure should define the roles and responsibilities of individuals involved in the model's lifecycle, from development and validation to deployment and ongoing monitoring. A well-defined governance framework ensures accountability and facilitates coordinated action in managing model risks.

2 Model inventory:

Keeping a detailed inventory of all models, including their development history, purpose, relative risk, etc., serves as the foundation for managing model risk. The inventory serves as the central system of record, enabling tracking of governance adherence, model performance, and the firm's outstanding model risk.

3

Validation and testing protocols:

Independent validation and testing protocols are at the heart of a MRM program. These protocols should include components such as performance, stability, sensitivity, and explainability testing. The goal is to ensure that models are robust, perform as expected under a wide range of conditions, and do not introduce unintended biases.

4

Documentation and transparency:

Detailed documentation for each model, including its design, development processes, and performance metrics, supports transparency and independent model validation. It serves as the foundation to build trust among stakeholders and facilitate an understanding of model decisions and limitations.

5

Ongoing monitoring and review:

Models must be regularly reviewed and monitored for performance against real-world outcomes. This ongoing process helps identify when models deviate from expected behaviors, allowing for timely adjustments or model recalibration to address emerging risks.



What should you do now?

Companies outside the financial sector using AI and ML should consider the following:

- Conduct a thorough risk assessment to understand the extent of their model risk exposure and ensure it is within your firm's risk appetite.
- Develop a MRM framework based on the foundational elements discussed above.
- Cultivate or acquire expertise in AI/ML and risk management.
- Promote a culture of risk awareness and ethical considerations in AI/ML development and application.
- Engage in collaborative efforts to stay abreast of best practices and innovations in MRM.

Broadening the application of MRM practices is increasingly important in today's technology-driven landscape. By proactively addressing model risk, companies across various industries can enhance the accuracy, reliability, and safety of their AI/ML applications, fostering public trust and ensuring the ethical use of these transformative technologies.

Contact us

Ben Harden

Managing Director

Risk, Regulatory & Compliance Services

KPMG LLP

T: 312-513-9029

E: bharden@kpmg.com

Kevin Lowery

Director

Risk, Regulatory & Compliance Services

KPMG LLP

T: 404-222-3421

E: klowery@kpmg.com

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS025144-1A