

T

## INDUSTRY INSIGHTS

# Supervisory Expectations on Model Risk Management—Key Considerations and Practical Implications for Banks

By Kishore Ramakrishnan

Given the increasing reliance on the use of internal models (IM) and scenario analysis to assess risk, it is not surprising to note the supervisory authorities are working overtime to come out with clear and prescriptive guidelines on the use of IMs focusing on the model governance and model risk management (MRM) frameworks.

European Banking Authority (EBA) issued a consultation paper back in March 2023 proposing changes to the bank use of market risk model with particular focus on the governance of the market risk model, internal risk measurement approach, and assessment of the internal default risk model.

Back in June 2022, Prudential Regulation Authority (PRA) had outlined 5 principles (CP 6/22) that firms should refer to in order to establish a robust MRM framework. Building on those principles, PRA's May 2023 policy statement (PS 6/23) proposes certain changes that have far reaching implications to banks, including on the usage of Artificial Intelligence (AI) / Machine Learning (ML) models, vendor models, post model adjustments, financial reporting, and accountability of the senior management function. PRA's MRM PS 6/23 will go live in a year's time (i.e., May 17, 2024), which means that firms have approximately 12 months from obtaining permission to use IMs for the first time after the publication of PS 6/23.

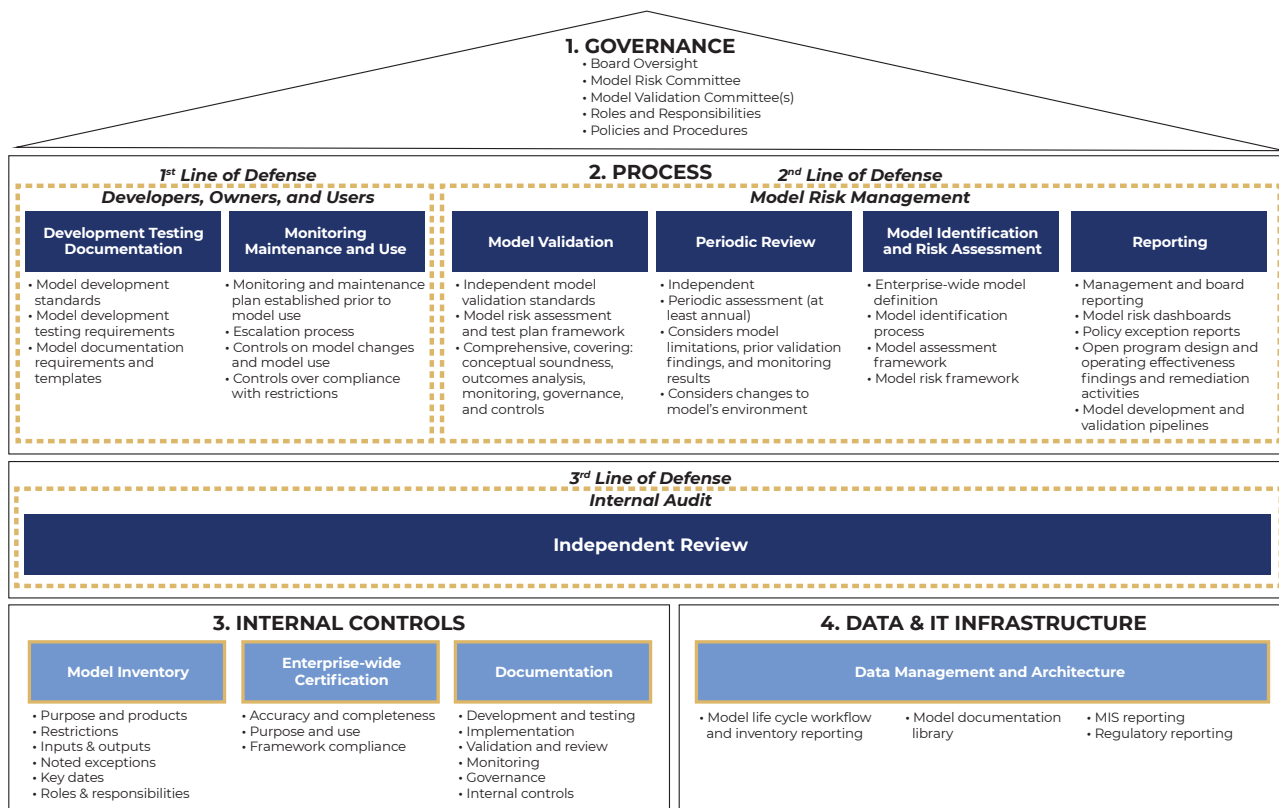
All the consultation papers and policy statements from the supervisory authorities underscore the importance of banks needing to identify and prioritize actionable steps to fulfilling the regulatory expectations around the model risk management ranging from

- Conducting an annual self-assessment against the MRM framework.
- Ensuring the bank's governance arrangements support effective oversight of their MRM framework.
- Embedding the firm's own assessment into the wider supervisory assessment.
- Identifying synergies with the Basel 3.1 model approval submissions for credit and market risk.
- Building a robust MRM policy addressing PRAs expectations around regulatory reporting and oversight of regulatory models.
- Building a strong remediation framework to addressing the PRAs Skilled Persons reviews.

When it comes to the overarching governance expectations on the MRM, the board of directors and senior management of the banks are on the hook for enforcing a robust MRM that encapsulates the five principles set out by the PRA.

1. **Model Identification and Model Risk Classification** – It is recommended that the banks work towards compiling a company-wide inventory of IMs including third party and external vendor models. In doing so, it is important to capture the information on model owners and model users with appropriate lifecycle statuses such as “under development”, “in-production”, “decommissioned”, “outdated” etc., The inventory should be supported with detailed documentation outlining the intended use of the model data dependencies etc.
2. **Governance** – At the outset, it is important for the banks to have a well-documented MRM policy and designate an accountable individual who takes on the responsibility of implementing the MRM framework aligned with the model risk appetite that needs to be reviewed at least annually. Firms need to consider the use of analytical tools that automate the process of analyzing the end-user developed models to mitigating the model risk in detecting the possible errors and dependencies on other models / data sets. These analytical tools should be able to deal with the data’s sensitivity to errors or absence of variables. The senior management function should ensure the relevant processes and procedures are embedded within the MRM framework covering both the internal, external, and vendor models. MRM governance requires seamless coordination and interaction with the stakeholders representing the 1st, 2nd, and 3rd lines of defense alongside leveraging the data and technology infrastructure of the bank in an appropriate manner.
  - a. The 1<sup>st</sup> line of defense is responsible for the model development. They should have complete ownership of the model risk as an exposure class and should be involved in rigorous testing of the models during the implementation phase.
  - b. The 2<sup>nd</sup> line of defense should be focused on model validation as opposed to model development with particular focus on enforcing stricter controls and documentation standards.
  - c. The 3<sup>rd</sup> line of defense is less focused on the model theory / model mathematics and instead should focus on the process and controls alongside documenting and reporting the audit findings to the senior management and the board.

**Model Risk Management Governance Framework – What Good Looks Like**



- 3. Model Development, Implementation, and Use** – Banks are expected to have a robust model development process with supporting documentation outlining the intended use of the model and its limitations, mathematical theory, underlying model assumptions, calculation methodologies, design principles, output calibration approach, model adjustments, testing approaches, supporting technology infrastructure, etc. This needs to be supplemented with appropriate data quality checks and controls for completeness, accuracy, timeliness including handling of incorrect or missing data.
- 4. Independent Model Validation** – Banks need to demonstrate that models are independently validated prior to implementation and when (1) the risk rating of a model changes, (2) there is a significant change to the model or the operating environment, (3) the bank detects performance deterioration in the model, or (4) third-party reviewers identify concerns. The frequency of validation ranges depending on the size and complexity of the bank and inherent risks thereof. The model validation should encompass both qualitative (i.e., process and the underlying data quality) and quantitative elements such as stress tests, benchmark tests, sensitivity tests, source code tests, actual vs estimation analysis, discriminatory power, stability tests, etc.
- 5. Model Risk Mitigants** – In order to ensure the bank constantly operates within the boundaries of its risk appetite, model risk mitigants play a pivotal role to assessing the model health and model materiality. The model risk mitigants should be centered around identifying areas where measurement uncertainty and model deficiencies are known to exist, according to their materiality.

In the future, the PRA seeks to rationalize existing references to MRM under a single overarching policy framework, where the proposed broad expectations would be applicable to all model and risk types including:

- **Capital models** covering credit, counterparty, and market risk models which includes IRB, IMM, and IMA approaches.
- **Operational management models** including AML, AI / ML and new technology, Anti-fraud, trade surveillance, etc.
- **Risk management** covering stress testing, risk pricing, valuation, trading algorithms, ICAAP, and Pillar 2 models.
- **Provisioning and other balance sheet** items such as IFRS9 (ECL) models, etc.

It is indeed welcoming to note that PRA has outlined a “proportionality framework” whereby the rigor of model risk management, including frequency of model validation, application of risk controls, performance monitoring, etc. will be commensurate with the firms’ size, business activities, and complexity and extent of their model use.

---

An abbreviated version of this article was published as an [op-ed in Banking Risk & Regulation](#).



#### **Kishore Ramakrishnan**

Kishore Ramakrishnan is Managing Director, Capital Markets Advisory at Treliant. He has over 24 years of global industry and consulting experience across the banking, capital markets, asset, and wealth management businesses. Kishore is a trusted advisor and respected thought leader in the risk, regulation, and compliance domains covering multiple asset classes including cash equities, fixed income, and listed and OTC derivatives. [kishore.ramakrishnan@treliant.com](mailto:kishore.ramakrishnan@treliant.com)