MRMIA
MODEL RISK MANAGERS' INTERNATIONAL ASSOCIATION

The Role of an Audit Practitioner with Model Risk

Written by Tom Dahlin,

Chief Model Risk Officer, Centennial Bank

Approved by MRMIA – 3/15/2023

Table of Contents

1. Background

Internal audit has an important role in the assessment of the model risk. Within its assessment, it should conduct a comprehensive review and testing specific to the compliance of model risk policy and procedure. Any significant findings resulting from audit should be reported to the Board.

A wide range of Audit practices currently exist within the space of Model Risk, and across the banking industry. This may be largely explained by the absence of either directive and/or unambiguous language within the model risk guidance –i.e. SR 11-7. Consequently, audit sometimes either misses aspects that should be reviewed, or conversely, improperly conducts model risk specific activities – such as validations. This may otherwise be permissible when no MRM exists, however, it should be temporary. Internal Audit should assess the model risk framework as it pertains to all model stakeholders – including line of business, data governance, model validation, and the respective committees with purview over models.

The following principles have been presented, approved, and endorsed by the MRMIA Board as a standard practice for Internal Audit to follow. These activities are scoped with the intention of enabling Internal Audit to meaningfully access on model risk effectiveness and policy adherence.

2. Regulatory Requirements – Guidance on Model Risk Management

The Federal Reserve Bank has established guidelines for model risk management by issuing SR 11-7. It states that a guiding principle for managing model risk is "effective challenge" of models, that is, critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate changes. Competence is a key to effectiveness since technical knowledge and modeling skills are necessary to conduct appropriate analysis and critique.

Model risk staff performing model validation should have the requisite qualification, knowledge, skills, and expertise. A high level of technical expertise may be needed because of the complexity of many types of models, both in structure and in application. Validation activities should continue on an ongoing basis after a model goes into use, to track known model limitations and to identify any new ones.

Internal audit should verify that approved policies are in place and that model owners and control groups comply with those policies. Internal audit also has an important role in ensuring that validation work is conducted properly, and that appropriate effective challenge is being carried out. Audit should evaluate the objectivity, competence, and organizational standing of the key validation participants, with the ultimate goal of ascertaining whether those participants have the right incentives to discover and report deficiencies.

Internationally, the Bank of England has issued SS1/23 – Model Risk Management Principles for Banks, that outlines model risk management requirements regarding financial reporting and external auditors.

The expectations in this SS are relevant to models used for financial reporting purposes. The PRA considers that the effectiveness of MRM for financial reporting is relevant to the auditor’s assessment of, and response to, the risk of material misstatement as part of the statutory audit, including its understanding of a firm’s processes for monitoring the effectiveness of its system of internal controls and its understanding of a firm’s control activities. The PRA (Prudential Regulatory Authority) expects firms to ensure a report on the effectiveness of MRM for financial reporting is available to their audit committee on a regular basis, and at least annually. To facilitate effective audit planning, the PRA expects firms to ensure that this report is available on a timely basis to inform their external auditor’s assessment of, and response to, the risk of material misstatement as part of the statutory audit.

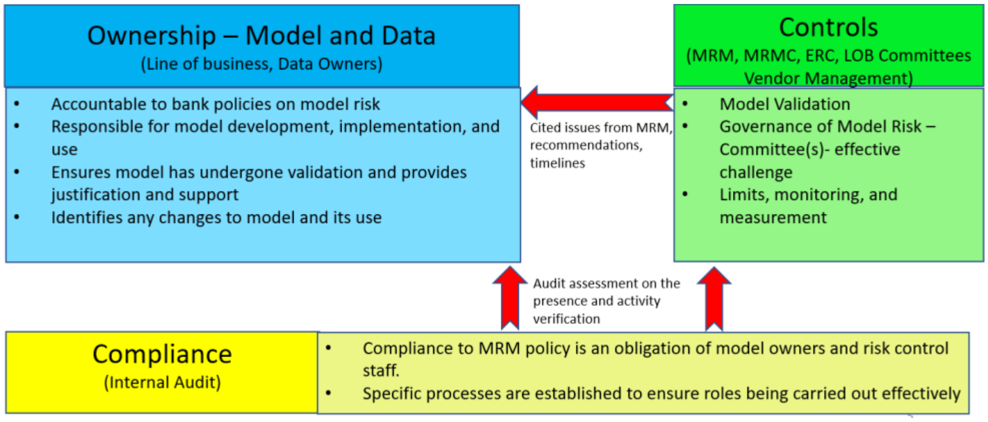
3. Roles Across Model Risk – Compliance, Controls, and Ownership

Effective model risk structures encompass at least 3 roles; ownership, controls, and compliance. These functions should be well defined throughout the organization as well as clearly documented/evidenced.

Ownership refers to the owning and possession of the model and data. This is typically the line of business and/or data owner (ie. business intelligence, data curator, etc.) The ownership role is responsible for adhering to bank policies regarding model risk, appropriate model development, implementation, issue remediation, and use, ensuring the model has undergone validation and providing support, and identifying changes to the model or its use.

The control function is usually made up of a combination of the Model Risk Management department, governing bodies (MRMC, ERC, LOB Committees, etc.) and potentially vendor management/third party governance departments or functions. The control arm of this relationship directly overlooks the ownership arm through model validation, effective challenge, and reviewing limits, monitoring, and measurements.

Internal Audit resides in the compliance role of model risk and is responsible for overseeing and providing assessment on both control and ownership functions as they relate to MRM policy compliance and process effectiveness. See the graphic below that illustrates this relationship.



Ownership – Model and Data
(Line of business, Data Owners)

- Accountable to bank policies on model risk
- Responsible for model development, implementation, and use
- Ensures model has undergone validation and provides justification and support
- Identifies any changes to model and its use

Controls
(MRM, MRMC, ERC, LOB Committees Vendor Management)

- Model Validation
- Governance of Model Risk – Committee(s)- effective challenge
- Limits, monitoring, and measurement

Cited issues from MRM, recommendations, timelines

Audit assessment on the presence and activity verification

Compliance
(Internal Audit)

- Compliance to MRM policy is an obligation of model owners and risk control staff.
- Specific processes are established to ensure roles being carried out effectively

4. Audit Scope – 3 Phased Approach

Effectively scoping the MRM audit is fundamental. Internal Audit has the responsibility to ensure the scope of the MRM audit is both effective and efficient. A 3-part approach can be adopted, encompassing planning, evidence, and testing.

Planning – Determine the existence of a MRM program plan and how is this plan intended to be achieved. This encompasses the presence of MRM Policy, Framework, Charters, Procedures, Standards, etc.

Evidence – Assess the evidence that the MRM program is following this plan. For MRM specifically, review the management of inventory, validations, issues, aggregate risk, governance, and challenge.

Testing – This may include the schedule of validations, methodology of risk aggregation, timing of past due issues, validation rating system, and model ID process. Testing should also include internal data systems used for the models are tested and certified.

5. Ownership – Model Owner and Data Source Systems

Model owners are required to have a procedure to provide descriptions of how models will be used. Decisions made based upon a model's outputs that depart from its stated use between validations should not occur.

Audit verification and testing should include:

- The policy/procedures of the model are updated, well documented, and used. Access controls should be verified and tested. A previous period of results may be reviewed that no judgment or discretion was exercised (unless otherwise documented).
- The status of the model can be verified – for example, the stated model is consistently used in production, and no manual process is inserted or substituted.
- The use of the model has not gone beyond its stated purpose. For example, a model was designed for one type of product, but was subsequently used for other products or segments.
- Thresholds or settings of the model have not been changed or modified with notification to MRM, which may otherwise trigger a new validation.
- Contingency plans may be reviewed and tested. If the vendor code is in escrow, verification should be made available.

A model overlay may result from a combination of items, such as historical underestimation, changes in business strategy, uncertainty, model limitations, or other. Overlays should be well supported and justified. Review and challenge of an overlay should occur in the 1st and 2nd lines of defense, specifically MRM.

Audit verification and testing should include:

- Audit may verify that the 1st line of defense has challenged and approved the overlay, with any repeated use following the same review process.
- Audit may verify that overlays were reported to the stated risk committees for review and approval.
- Audit may verify that MRM either supported/opposed the overlay, and adjusted the aggregate risk reporting accordingly.

The data used in any of the models will be assessed as part of the model validation. It will include the variable selection process, proxy data, data applicability, treatment, procurement, and testing. NOT included in the model validation are the internal data systems, which is an Internal Audit function. This includes the internal data integrity process to ensure the model owner can rely on the systems available to them. Internal Audit should review and test the Data Governance program.

Audit verification and testing should include:

- Review and verify the Data Governance program for policy and framework.
- Verify the presence of a data dictionary for all critical data elements; as defined by data variables used in the models.
- Certification of data used in the models.
- Review data mapping of the critical data elements.
- Review and verify identification of data owners, or stewards, responsible for reconciliation and treatment.
- Verify that the critical data element with identified issues (not reconciled, aberrant, missing, etc.) has a work plan for remediation.
- Verify that the Data Governance Committee is informed, reviews, and challenges the data source issues and recommendations.

6. Controls – Model Governance, Vendor Management, and Validation

Internal Audit should begin with a request for the organization's current approved MRM practices – this should include policy, frameworks, and committee charter. This is to ensure regulatory alignment as well as internal consistency.

Model Risk Policy – This specifies the firm's high-level objectives of measuring and managing model risk. This is reviewed and approved by the Board on an annual basis. The policy specifies model identification, model inventory, model attestation, requirements to conduct model validations, exceptions, model approval process, and MRM updates to the specified governance structure.

Audit verification and testing should include that:

- A policy exists and has been approved by the Board on an annual basis.
- The policy includes the necessary elements that should enable Model Risk to be effective.
- Each of the elements in the policy is conducted in practice, and well evidenced. For example, Audit may test any required approvals, and be supported by minutes.

Model Risk Framework – this is an extension of the policy, such that greater details are provided on how exactly adherence to the policy will be achieved. Its design and implementation will be influenced by the size and complexity of the organization. It should be reviewed and approved annually by the Board of Directors. The framework covers the roles and responsibilities of various the model risk stakeholders and participants, including model validations, governance updates, exception approvals, critical spreadsheets, inventory approval, overlays, limitations, and model approvals. Additionally, it will specify how and where model risk training is provided to model owners and ensure that training requirements are satisfied.

Audit verification and testing should include:

- A framework exists, and has been approved by the Board on an annual basis.
- The framework includes all the activities necessary for a functional MRM program. For example, the role of MRM is to give updates to MRMC on schedules, validations, aggregate risk, inventory, past due issues, and overlays.
- Each of these activities is conducted per the framework – for example, are past due issues and/or exceptions being reported regularly to MRMC? Are validations being conducted within the specified time that the model tiering dictates? Are training materials available and are the requirements met?

Model Risk Management Committee Charter (MRMC) – outlines the role and responsibilities of the committee responsible for overseeing model risk and its reporting structure. The MRMC's should encompass reviewing and approving the Model Risk Management (MRM) Policy and Framework, assessing aggregate risk, monitoring key risk indicators (KRIs), evaluating model exceptions, overseeing model usage, managing the model inventory, and handling model retirements. Additionally, the Committee charter should specify the process for reviewing the model validation schedule.

Audit verification and testing should include that:

- A charter exists and has been approved by the Board on an annual basis.
- The charter includes specific activities of the Committee – including model approval, exceptions, and retirement, as well as updates on validations, aggregate risk, inventory, past due issues, and overlays. Minutes should be requested.
- Verify that each of these decision points and activities are being conducted per the charter – for example, is each model approved by MRMC for use? Are past due issues escalated? Is there evidence and support for every exception?
- Decisions and approvals from the MRMC are strictly adhered to, and managed to keep within stated risk appetite.

Vendor Management – Requirements should be specified within the MRM framework – with processes to identify vendor models or tools and ensure that contract language and MRM requirements are set throughout the engagement.

Audit verification and testing should include:

- A review of Vendor Management policy and/or procedures for the notification to MRM of a new vendor.
- A review and test that new contracts, including renewals, are conveyed from Vendor Management to MRM for model identification.
- Verification that model identification queries are complete and sourced to the responsible party in the LOB.
- Verify the presence of an MRM model or tool final determination, with requisite approvals.
- Verify that all new vendor contracts, that have been MRM deemed as a model, include requirement setting language necessary to conduct a model validation.

Audit should ensure that vendor management has a well-controlled process to aid model identification and MRM validations.

Qualifications – Model risk staff doing model validation should have requisite knowledge, skills, and expertise. A high level of technical expertise is often needed due to the complexity of the models, both in structure and application. (Source: SR 11-7 Section 5 Model Validation). As such, resumes for the Model Validation team should be made available to verify the following:

- Education – For all individuals who are involved in the validation process. Validators should be trained in quantitative methods, specifically modeling techniques involving predictive and other statistical/mathematical techniques. A validator's background should include graduate-level higher education, e.g. a Masters degree or higher in statistics, mathematics, economics, data science, etc.
- Experience – model development experience is important. Typically, experience enables the validators to assess which modeling approaches are reasonable in imperfect conditions, such as incomplete or troublesome data.
- Where education is at Masters level, or experience is five or more years, it may be concluded that requisite qualifications are sufficiently met. When it is less, managers overseeing the validation must have met the requirements. Auditors themselves should self identify if they are not sufficiently qualified to validate models.

Audit verification and testing should include:

- Verify that the resumes of all staff have the requirements necessary to conduct validation(s) – as outlined above.

Model inventory – is where all models and their characteristics are captured and is a core reference for MRM. Characteristics to be included are the model's purpose(s), owner, sponsor, risk tiers, key inputs, implementation date, last validation rating, model status, and timing of the next validation.

The model inventory will be a central source through which the model risk can be determined in aggregate – combining ratings, unvalidated models, past due issues, and models with limitations.

Audit verification and testing should include:

- A model inventory exists, complete with the appropriate model characteristics, and summary totals to cross check against governance documents that describe the inventory – i.e. number of models.
- Controls – Audit may test and/or verify that access to the inventory is limited to current MRM personnel only. Additional control testing may include model status (i.e. retirement), model determination (MRM or owner), and schedules.
- Testing – platform appropriateness – Audit may conduct benchmark assessments on the use of Microsoft Excel for the inventory, or the use of Logic Manager, GRC (or other systematic tool).

MRM Procedures – there are multiple procedures that MRM will create and use in the course of their activities. These will include

- model identification – this describes the step-by-step approach(s) used to register a model.
- model validation- the is the generalized procedures to validate a model, and the controls used to ensure internal consistency.
- critical spreadsheet review -
- Annual review of models
- creation of the reported KRIs and KPIs -

Audit verification and testing should include:

- MRM procedures exist, including model identification, model validation, critical spreadsheet review, and creation of KRI and KPIs. Controls – Audit may test and/or verify controls to ensure that access to the inventory is limited to current MRM personnel only. Additional control testing may include model status or model determination.
- Testing – KRI and/or KPI replication – with the procedures to generate KRIs and KPIs, Audit may use the inventory, ratings, and audit issues to re-create and verify the values.

MRM Validation – the process and procedure for model validation will be generalized, as models will be different, requiring slightly different approaches. However, the validation principles should be evident, such that the model validator will assess 5 key areas: Model Documentation, Implementation, Model Development, Data, and Governance. Model Monitoring may be included as part of the Model Development.

Audit verification and testing should include:

- A validation report exists for each model.
- Each validation category, including Model Development, Data, Governance, Documentation, and Implementation is assessed.
- Issue – Audit may verify that any resulting issue has support and/or is referenced in the validation report. For example, in either the work-papers, validation testing, or explicit validator determination.
- Recommendations are provided by an MRM validator for each of the cited issues.
- Ratings – Audit may assess the ratings' consistency, such that the specified number and type of issues, as outlined and approved in the framework, lead to the stated rating.
- Validation review and challenge – Audit may test whether the validation has been reviewed and effectively challenged. This may be evidenced through version controls, internal challenge, and final approval for model use in the MRMC.

Audit must NOT conduct a validation. Internal Audit's role is not to duplicate Model Risk Management activities. Rather, it is to evaluate whether Model Risk Management is comprehensive, rigorous, and effective (Source SR 11-7). Adherence to the framework is evidence of such a threshold.

MRM Validation Issues – as part of the validation process, MRM will cite any deficiencies as issues. They may be major, significant, moderate, or minor. The issues influence individual model risks and the aggregate level of risk within the organization. Each issue type should have a time limit within which to address them. Further, MRM, through the validation, should also provide a recommendation for how the issue should be closed.

Audit verification and testing should include:

- Each validation report specifies identified issues, with a risk designation (i.e. significant, moderate, etc).
- Each identified issue should have a validator's recommendation to close the issue. This should be implicitly/explicitly approved by the Head of Model Validation.
- Submitted for review – when the issue has been submitted for MRM review, a decision should be made by MRM to reject, close, or downgrade the issue which should be evidenced. That which has been submitted to MRM should not age beyond the stated framework or be conveyed to MRMC.
- Past due issues - Audit may verify that past due issues are escalated to MRMC.

Model Limitations– models may have limitations for a variety of reasons that should be documented in either policy, framework, or procedure. This may include a model with an overlay or an exception to policy – such as unresolved past due issues, delayed validation, or an unvalidated model. In some cases, a model limitation may preclude its use only under certain conditions.

Audit verification and testing should include:

- The policy/framework/procedure has criteria for model limitation.
- The models that meet this criteria are properly designated as having limitations.
- Verify when models have limitations, and that their use is adhered to.
- The aggregate risk calculation incorporates the model limitation as a component.
- Model limitations are regularly reported to the MRMC.

Model owners are responsible for providing the necessary evidence to support the validation and should be aware of MRM's expectations. Internal Audit should determine the presence of model risk standards and training.

Model Risk Standards- these standards should be documented and available to all model owners. This includes development, documentation, implementation, and performance monitoring. All models will be measured against these standards when validating. When or if these are found to be deficient in the model validation, they may lead to an identified issue. Audit should verify that MRM defines these standards and makes them available to the model owners.

Model Risk Training – mandatory training for the model owners and sponsors. It should include high level model risk concepts and the minimum expectations necessary for the model owner to undergo a validation. There may be a variety of methods to deliver the training, however, it should have audit capabilities necessary to determine that the specified owners took the training, and successfully passed.

Audit verification and testing should include:

- Model risk standards exist and are accessible to all model owners – including implementation, documentation, development, and model monitoring.
- Audit may verify that all model owners have taken and passed the MRM designed training and testing – within the required timeframe.

7. Pre-approved Audit Scope

Before performing a model risk audit, a scope document should be provided by the audit team to ensure all stakeholders understand the depth of review. Depending on the maturity of the program, the scope may either be narrowly focused or widely focused with specific testing across different areas. The expectation of maturity should be a function of asset size, the number of years in MRM operation, and the complexity of the organization.

Audit scope should include the degree of each of these items, and specificity, that will be reviewed/tested:

- MRM Policy, Framework, Procedures – presence, alignment to SR 11-7, and adherence to stated practice.
- Model Identification Process – presence and adherence, including Vendor Management, with contract MRM specification.

- Model Inventory – presence, comprehensive characteristics, tiering, descriptions, validation timing, ratings.
- Exceptions, Limitations, and Overlays – well defined, escalated, and approved.
- Model Validation – conducted across model inventory, within stated timelines, with identified issues, and recommendations.
- Model Risk Issue Management – presence, remediated, closed, and/or escalated as appropriate.
- KRIs and Aggregate Model Risk – conducted in accordance with stated procedures.
- Governance – presence of review and approval of all requisite model risk activities and reporting.
- Data Source System – presence of policy/procedures of critical data elements, data mapping, reconciliations, and treatment.
- Model Owners – presence of model procedures, training, use control, access controls, elevation of output and monitoring.

Each item within the scope should be explained thoroughly, including its purpose, and the criteria to satisfy the requirement. Specific testing is to be done.

8. Conclusion

Audit has an important role in the assessment of model risk, with a focus on the presence of and adherence to the stated practice. To achieve this, audit should generate a scoping document for an engagement – detailing coverage, specific testing, and adjusted for model risk maturity. Audit must be certain to not conduct model risk activities or prescribe which specific validation activities should be performed. Auditors should remain independent from validators, exactly as validators should be independent from developers. Otherwise, this precludes their ability to effectively audit MRM. A wider view of model risk should be taken – including LOB, Vendor Management, Committees, and Data Governance; being mindful that Model Risk Management measures the risk, it does not own it. Testing should be performed across various areas, replicating KRIs, Aggregate risk, issue aging, model identification testing, and verification of necessary use and access controls.