Tech Report 2021-03 , 25 March 2021, Version 1.0, ©2021 MRMIA

Right Sizing Model Risk Management for Financial Institutions Between $10-50 Billion

WORKGROUP MEMBERS

Thomas Dahlin, Chairman
Jessica Jiang
Briony Pentecost
Amy Polasek
Arun Musinipally
Blade Blevins

Background – Pervasive Use and Complexity of Models Increases Risk

Banks and financial institutions use a vast array of models to help management make decisions and set policies. These models serve a variety of different purposes within an institution: some are designed to meet regulatory requirements, whereas others are to protect the bank and its customers from fraud, and many more are used to help with the actual day-to-day management of pricing, valuations, reserve setting, stress testing, underwriting, and beyond. Within the financial industry, there is an increasing reliance on models to help perform these key functions. This can be explained simply by considering the dynamics of both supply and demand. A steady supply of bank consolidations, increasing customer base, more effective data collection processes, and greater range of modeling tools provide the foundation to readily explore relationships and project impacts. At the same time, new demands for quantification have come in the form of regulation (*e.g.,* Basel, CCAR, SR 11-7, GAAP, BSA), as well as business objectives and risk appetite.

Model development has grown from simple spreadsheets and regressions and is now moving to more complicated and integrated systems. As an example, banks traditionally used simple historical averages of losses to estimate the required reserves, but the calculation has morphed into a more sophisticated CECL construct with over-the-life predictions using new components (such as prepayment rates, curtailment, economic factors, correlation structures, and more) that each require empirical justification. Similarly, BSA modeling has moved from a series of rules to generate alerts to more advanced machine leaning systems. While these developments may seem cutting edge and meet some important objectives, they also come at a cost: increased model risk from improper use. Properly identifying and quantifying that risk requires an institution fully committed to the discipline of model risk management.

The shape and form of model risk management should be specific to the institution, as each is different, operating in a slightly different space and with varying degrees of size and complexity. Mega banks,

such as JP Morgan Chase, Bank of America, and Wells Fargo, that collectively have $6.6 trillion in assets and thousands of models, should have a very different model risk approach than smaller regional or community banks that typically have fewer than 50 models to manage. While general philosophies may overlap, their respective challenges and solutions warrant discussion. This paper is intended to present a series of model risk management practices that are well suited for smaller banks and credit unions with assets between approximately $10 and $50 billion.

Table of Contents

1. Introduction to MRMIA

Model Risk Managers' International Association (MRMIA.org) is a non-profit industry advocacy group focused on promoting best practices in model risk management. With a membership primarily from financial institutions, MRMIA seeks to provide an independent voice on model risk management that explicitly takes into account a cost-benefit analysis behind the practices being promoted. Specifically, MRMIA seeks to avoid chasing methods with diminishing returns and instead seeks to promote those practices with real benefits to model developers, model owners, and those in various risk management functions who need to oversee the process.

This document was created by an MRMIA workgroup tasked with gathering best practices from personal experience, industry interviews, and academic publications. It is expected to be a living document that will be revised as new insights and methodologies become available. The views expressed here are those of MRMIA and the authors. They do not necessarily represent the views of their employers or any specific financial institution.

2. Model Risk Management – A Discipline Emerges

Prior to 2011, there was no universal set of guidelines or model risk practices for financial institutions to adopt. However, regulators understood the need to broadly articulate an approach and further reinforce it within their existing risk management reviews. As a result, the Federal Reserve and OCC collaborated to produce the formal *Supervisory Guidance on Model Risk Management* (commonly referred to as "SR 11-7"), which was later adopted by the FDIC. The guidance covers a wide range of concepts and identifies elements that are expected to be present in an effective model risk program, including defined roles and responsibilities across the institution and commentary on model development, validation, governance review and challenge, periodic review, inventory, performance monitoring, model dispositioning, and more. While the guidance provides a comprehensive accounting of the necessary components of a model risk management framework, it does not provide a prescriptive checklist for creating or maintaining a program. There are no look-up tables that detail the requisite testing or define goodness-of-fit metrics, nor are there standards that enable an institution to gain comfort that they have meaningfully aligned with the guidance. The opacity is likely by design – since each institution and each model application area has different risks and profiles, overly prescriptive guidance would likely be improper and could

even hinder an institution's ability to properly match a program with its risk. This notion is captured as the concept of "size and complexity" referenced within the guidance. Considering these factors when designing a program can help institutions effectively manage model risk without employing unnecessary resources.

Some institutions may treat SR 11-7 and model risk in general as just another regulatory hoop to jump through, but it can actually provide value to the business when performed correctly. Model risk is a shared risk that developers, users, sponsors, validators, and management can positively influence through their diligence and understanding of models, their use, and limitations. The SR 11-7 concepts are logical and cover the areas that could lead to some form of model failure. Most pronounced are design flaws and/or data issues, but there are numerous other areas including implementation, flawed assumptions, or governance that may also contribute to a material weakness. The guidance is essentially a collection of concepts that each organization should consider incorporating within a new framework or integrating with an existing structure. Governance and data are two areas that may have some preexistence.

Central to model risk management is the validation process. It allows an organization to carefully consider and evaluate each component of a model to isolate bias and to identify potential flaws. Institutions can face serious consequences if they rely on models that result in mispricing, over/under reserving, or over/underestimating credit performance: however, a robust validation function can help prevent these adverse outcomes. Some key questions asked during a validation include: What assumptions were made that could lead to model failure in the future? Why was this proxy data used? Why this estimator? How would this perform in the past? Why were these particular variables chosen? How many alerts were missed that should have been caught? Why are these default settings used without testing? This review and challenge process can sometimes be contentious in nature between validators (as representatives of the Model Risk Management Department) and the model developers/owners who are pressed to justify key decisions, but these challenges are ultimately intended to ensure the entire modeling apparatus is thorough, justified, and reasonable.

The practices set out in this white paper are recommended for smaller size financial institutions to comply with the principles of SR 11-7, but also, to effectively right size a practice.

3. Right Sizing – Partnering with Vendor Risk Management

One fundamental difference between larger and smaller financial institutions is the prevalence of vendor models. While larger institutions tend to develop models internally,

smaller institutions are often dominated by vendor models. For a variety of reasons, it is simply not practical for a small institution to develop most models in-house. Many cannot justify the cost of a modeling staff, or they struggle to attract/retain modelers even when they do determine that the investment is worth pursuing. Name recognition, opportunities for advancement, data availability, and modeling infrastructure are just some of the attributes that influence a modeler's employment decision. These considerations tend to place smaller institutions at a disadvantage, and the typical high turnover of modelers further exacerbates the problem. As a result, these smaller institutions turn to vendors with ready-made solutions and ongoing staff to address validation queries.

Given the high dependency on vendor models, a successful model risk program should recognize the need for a close alignment and partnership with the vendor management (or third party risk governance) team. Vendor management is uniquely positioned, due to timing and access, to aid in some of the most common issues that plague vendor models. Critical information necessary to support vendor models may include:

- **technical documentation** to reflect the specific structure, equations, and theoretical rationale
- **data analysis** to address the applicability of the data used to build the model (i.e., it should have comparable qualities to the institution in which it is applied) as well as provide evidence of integrity checks used to procure the development data set
- **performance monitoring** to capture regular updates related to the model fits, back testing, and/or other indicators of effectiveness to confirm that the model continues to perform
- **implementation guidance** to detail how the model should be placed into a production environment (such as the use of "checkpoints" and testing, data requirements, setting justification, over-rides, access control points, and procedures/policies)

The key problem with the use of vendor models is securing the necessary evidence for a model validation. Unfortunately, the typical urgency to purchase and implement vendor solutions usually results in contracts and agreements that are finalized without MRM input. By the time MRM gets involved during the validations of vendor models, there is little recourse to obtain the information necessary to support a thorough review. Vendors may still provide documentation, but it is likely to be incomplete, insufficiently detailed or vague, if it is not missing altogether. Another common occurrence is receiving documentation that is oriented to marketing and fails to provide any real explanatory evidence. Most frustrating is

when vendors refuse to provide any documentation at all on the basis of proprietary or intellectual property claims, despite NDAs that are already in place. In reality, full scope documentation either never exists, is of particularly poor quality, and/or the original developer is no longer with the company. The willingness to provide responses to the numerous validation questions is then met with contractual obligations, which generally do not cover any provisions around model risk.

To avoid these pitfalls, MRM must engage and partner with Vendor Management as part of an extended model risk program. During the period of vendor model due diligence, MRM should work with Vendor Management and the model owner to determine whether the new product is a model. If MRM concludes the existence of a model, this should then trigger requisite legal language to be inserted into the agreement with the selected vendor (of which more than one should be considered). The language is should provide binding recourse when/if the vendor becomes reluctant to provide materials/evidence/availability during the validation. Additionally, a request for standard technical documentation should be made prior to the agreement to gauge how the vendor may fare in the actual validation (this could be an early indicator).

A standard MRM checklist for Vendor Management may include the following:

Document Request	Description
Vendor Model Technical Documentation	This is typically a 20-100+ page document that is a **standard "off the shelf" that details the model development process** - methodology, structure, testing, variables, key assumptions, etc.
MRM – validation questions (may be a template)	This is a set of bank specific Model Risk questions. If an answer is already provided in the above "Vendor Model Technical Documentation", a page number/paragraph may be used as reference.
Data requirements	This is the complete list of data elements needed to execute (run) the model. Clear definitions and any required functional forms should be provided.
Model Performance Monitoring	This is an **ongoing quarterly update that demonstrates what level of model degradation** has occurred since the model has been placed in production – such as stability, goodness of fit, back testing, and/or other measures.
Implementation Plan	This is typically a step by step vendor "off the shelf" document that explains how to implement the model (not a user guide). It may describe settings, reconciliations, and controls to ensure proper installation.
Third Party Validation or Certification	This is typically an independent validation conducted on the model. This becomes more relevant when/if there are aspects of the model that the vendor wishes to remain confidential, however is shared with the 3rd party.
Change Management	Any changes to the model should be recorded (not data updates).

Ideally, a prospective vendor should agree to provide the information above prior to formalizing any agreements, and specific language addressing these items should be incorporated into the final contract. If the vendor agrees with the list (and agrees to the specified language in the contract/agreement) and can provide responses to the validation questions in an appropriate time period, then MRM should allow the implementation to proceed unless there are significant concerns or outstanding queries on available technical documentation. Any deviation or hesitation could be treated as a red flag and should be considered carefully when making a vendor selection.

The right sizing aspect relates to the notion that smaller banks have proportionately more vendor models and tend to command less attention from vendors once the products are implemented. Without access to the actual developers, it is important that a rich set of evidence is agreed upon at the outset of the relationship, as opposed to the validation period. A single bank is not the only customer, so allowing time for such an interrogation can be daunting. The agreement (1) better assures (but does not guarantee) that validation will receive what is needed, and (2) appropriately sets expectations.

Summary – Right Size Recommendations for Partnering with Vendor Risk Management:

1. Request that Vendor Management augment their process/procedures to document items for model determination (key questions listed above), including requesting an initial technical document. These should be directed to MRM for dispositioning.
2. When/if a model is being considered for purchase, a checklist of items should be conveyed by Vendor Management (a sample checklist is above). If the vendor is unable to comply, it should be considered a cautionary signal.
3. If the vendor has indicated they will meet these checklist requests, it should be inserted in the contract/agreement as binding language. Again, if the vendor is unable to comply, it should be considered a cautionary signal.

4. Right Sizing – Model Identification

A key regulatory expectation for model risk management is having a robust process to identify models used in the entire organization and to generate a centralized inventory to house a variety of information specific to each model. As per SR 11-7, information that should be contained within the inventory includes:

- a description of the purpose and products for which the model is designed
- actual or expected usage, and any restrictions on use
- type and source of inputs used and underlying components
- model outputs and their intended use
- an indication of whether the models are functioning properly
- exceptions to policy
- names of individuals responsible for model development and validation

- dates of completed and planned validation activities
- timeframe for which the model is expected to remain valid

The model inventory allows MRM to both plan and manage activities, as well as to facilitate reporting to management and the Board about the nature of the bank's model universe. A comprehensive inventory allows MRM to easily identify (and report on) the total number of models, their risk ratings, how many are in use, and other dimensions that can be used to infer an overall model risk profile.

The process to identify a model can be elusive, largely because the definition of a model is not clear cut. While model owners are typically responsible for self-identifying any models in their area, there is good reason why an owner may not rush to identify – the model validation process can be both invasive and time consuming, not to mention the outcome may lead to additional pain points. However, the Model Risk Program may be deemed weak and ineffective when too many models are unidentified. For this reason, MRM (or a designated committee such as a Model Risk Management Committee, or an Enterprise Risk Management Committee) should have the ultimate authority over model designations.

In a smaller institution, the challenge to identify models may be more innocent, albeit more pervasive, than larger institutions. There tends to be an absence of internal developers, which typically leads to heavy use of vendor models, and owners may be unaware that what they perceive as tools -- operational or otherwise -- are actually models laden with model components. The same misunderstanding may exist with spreadsheets that also contain similar elements, particularly some important business-critical spreadsheets. In order to help consistently identify (and classify) models, financial institutions can start with a series of questions such as the following:

1. Does this quantification process (or product) require input data? (Yes/No/Unknown)
2. Does this quantification process result in an estimated outcome? (Yes/No/Unknown)
3. Does this quantification process use any assumptions? (Yes/No/Unknown)
4. Can the quantification process have any uncertainty? (Yes/No/unknown)
5. Is there a risk to the bank if the quantification process is not pursued? (Yes/No/Unknown)

Smaller institutions may also benefit from expanding their processes to include a wider set of activities designed to identify and capture models. System redundancy across the organization that feeds into MRM is useful. Consider the following approaches:

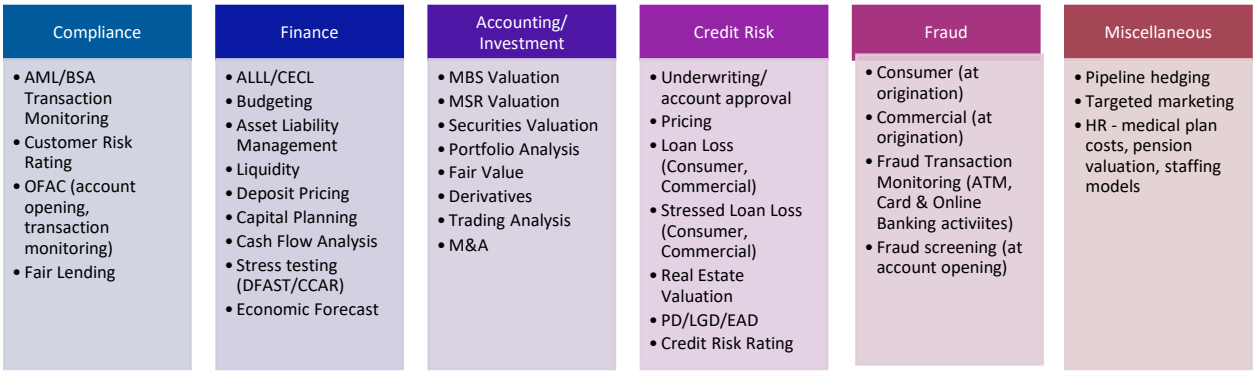
1. **Vendor Management** – Partner with existing Vendor Management functions to review new and existing systems for potential inclusion in the inventory.

a. For a lookback of existing vendor models, request full details of every vendor in the bank with a description of their product or services. A methodical approach is to progress from large/critical vendors (as classified by the respective vendor management teams) to smaller, less critical vendors. An application of the same set of questions above may be used. The owners of the products would be required to respond. All responses and details should be well documented and stored for later use and evidence.

b. For an ongoing identification of vendor models, request Vendor Management provide systematic updates of all new onboarding vendors, applying the same set of questions as described above, with direct feedback and clarification from the owners/requestors. This also should be documented and stored for future reference.

c. For further assistance, MRM may want to enlist the help of Internal Audit, as they are typically "in the field" and would have an opportunity to spot a potential model.

2. **Generally Identified Models** – Smaller institutions will typically have fewer than 50 models. A proxy list of industry-standard models (such as the one provided below) provides a reference to query the various departments on their practice.



3. **Annual Certification Process** – MRM is expected to undertake an annual review process. As part of this process, the Model Sponsors should be contacted (preferably through an automated system – *e.g.,* Logic Manager) to indicate the existence of the models within their control. Again, this should be documented.

4. **Validation Process** – An activity within the validation process should query inputs and outputs. The form of the inputs may stem from an unidentified model. Likewise, the

use of the output may also be part of a model. For example, the output of a CECL model may be used in a capital stress model. Inquiring about these flows of information has the potential of unearthing these models.

5. **New Products and Services** – A process flow within new products and services should integrate well with the MRM program, similar to the vendor management program, with key queries and responses.
6. **Training** – An ongoing training between MRM and the model community may be instrumental in bringing awareness to the owners. The concepts of model identification, components of a validation review, and the operation of MRM, including issues, provides a deeper understanding.

Summary – Right Size Recommendations for Model Identification:

1. Create or utilize a practical and consistent set of questions to establish the existence of a model. This should query on data, assumptions, projections, uncertainty, and importance/use.
2. Engage with Vendor Management to assess vendor relationships and the products they provide. This should be conducted on an ongoing basis to review all vendors. A similar practice may be embedded with New Products/Services.
3. Enlist Internal Audit to help identify potential models.
4. Establish a certification process with all model sponsors to help identify their activities and the models that may support them. Use a referenced set of models that exist in banks of similar size.

5. Right Sizing – Spreadsheet Models

Spreadsheets are potentially the most widely used business tool throughout a financial institution. Because most associates have access to Excel (or less common alternatives such as Lotus, Google Sheets, Open Office, etc.), and because any user can create a new spreadsheet, spreadsheets carry a variety of risks. These risks include flawed design, hidden cells, formula errors, entry errors, misuse, fraud, and destruction. Furthermore, without proper controls, spreadsheets can be intentionally or accidentally modified, and changes may go undetected.

Regulatory expectations indicate that spreadsheet models are not to be treated differently from any other type of system, platform, or software. However, the spreadsheet would still need to meet the definition of a model, which is defined in SR 11-7 as "…a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. Models meeting this definition might be used for analyzing business strategies, informing business decisions, identifying and measuring risks, valuing exposures, instruments or positions, conducting stress testing, assessing adequacy of capital, managing client assets, measuring compliance with internal limits, maintaining the formal control apparatus of the bank, or meeting financial or regulatory reporting requirements and issuing public disclosures. The definition of ***model*** also covers quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature."

At most financial institutions, spreadsheet software is installed on almost every computer. Identifying how each user utilizes the software, to see if their use meets the definition of a model, can be extremely difficult. To successfully manage this, consider the following best practices:

- develop and deliver bank-wide annual training (a PowerPoint presentation emailed will suffice, it does not have to be in person) in which the definition of a model is provided, along with some easy to understand examples of your current models
- set expectations for associates to self-report (say this in the training)
- partner with Internal Audit or other risk functions to help identify possible models while in the field performing audits/examinations
- partner with Information Technology and/or Training, in case they receive a request for training or support

Summary – Right Size Recommendations for Spreadsheet Models:

1. Spreadsheet models, although potentially more simplistic, are still models and thus subject to standards outlined in your policy.
2. The identification processes should have the ability to capture spreadsheet models.

6. Right Sizing – Non Model Critical Spreadsheets and Tools

6.1. Critical Spreadsheets

Most financial institutions have found that critical spreadsheets have become a topic of interest with regulators. Although it may vary from institution to institution, a critical spreadsheet can be defined as a spreadsheet that calculates data on a recurring basis and is used in one or more of the following ways:

- as a direct input to financial reporting of a material amount (materiality based on the dollar amount reported)
- as a primary factor in decision making on a material basis (materiality based on dollars involved in the decision on an individual or annual aggregate basis)
- as a primary factor in decision making within executive level governance structures (these structures are typically board level committees or executive level committees reporting directly to a board: executive loan committees, executive risk committees, asset quality committees, etc.)
- to directly assess the Bank's risk position at a material level (materiality based on the dollar amount assessed)

Materiality could then be defined as $XX million (roughly X% of INSERT YEAR pre-tax net income). Hint: if possible, consider making it consistent with the materiality definitions set by your financial institution's Accounting Department, Internal Audit Department, and/or external auditors.

Critical spreadsheets include only spreadsheets that are not being managed as models. This designation does not include applications or databases and does not consider the protection of customer information, as these items are typically addressed under Information Technology policies and procedures.

Categories of critical spreadsheets may include:

- **complex spreadsheets** – spreadsheets with complex calculations, such as algorithms, macros, logical formulas, multiple nested or conditional formulas, or formulas with cell references to multiple tabs

- **simple spreadsheets** – spreadsheets with a single data source and only simple math (*e.g.,* totals or averages) or manipulation (sorting or categorization of data)
- **aggregator spreadsheets** – spreadsheets with multiple data sources or manual input from multiple sources and with only simple math or manipulation

Critical Spreadsheets should be subjected to End User Developed Application (EUDA) standards. These standards encompass identification, protection, internal integrity, documentation, and development and testing. Controls required of critical spreadsheets are described below and will vary based on the nature and use of the spreadsheet and other types of controls in place. Complex spreadsheets will generally require more robust controls than simple spreadsheets or aggregator spreadsheets.

- Identification – Details of EUDAs should be recorded in an inventory and the inventory should be kept up to date by MRM. The inventory details of each critical spreadsheet or model spreadsheet should include, at a minimum, a description of the spreadsheet, the identity of the department/individual with primary responsibility for designing and maintaining, the individuals who use them, and the intended purposes.
- Protection – Critical spreadsheets should use password protection for entire spreadsheets, important formulas/cells, critical input data or worksheets; dependent on accessibility and complexity. These spreadsheets should reside on a secured server and not on an employee's hard drive. Only employees with a legitimate business need should have access to a critical spreadsheet; therefore, a critical spreadsheet should typically not reside in a folder on a share drive accessible by any employee, but should instead be accessible only to the department(s) using the file. Departments should also ensure that only approved versions of the spreadsheet are being used in production.
- Internal integrity – The integrity of information contained in critical spreadsheets should be assured through the first line's conducting of appropriate reconciliations, providing identification of input sources and outputs, and the application of a worksheet header/information page (providing a means for capturing critical information such as currency, units of measure, purpose of calculation, legends, and font colors).
- Documentation – There should be documented standards/procedures for the development of critical spreadsheets. These standards, although important, do not

need to reach the level of intensity of the model documentation standard/procedures for development. These standards/procedures should at a minimum cover the requirements of user training, change management, procedures for updates, and assumption details. Changes to spreadsheet logic, formulas, or references on a complex spreadsheet should have a documented review and approval by a second knowledgeable associate before the change is implemented. Each time the spreadsheet is changed it should be saved as a new file with an indicator of the new version either in the file name or within the spreadsheet. Simple spreadsheets and aggregator spreadsheets should undergo a documented periodic review within the business function to affirm calculations remain accurate. A change to the source of input on a critical spreadsheet should be verified for completeness, appropriateness, and accuracy before the change is implemented. The review should be documented and retained.

- Development and Testing – Critical spreadsheets should be subject to periodic review in accordance with the institution's MRM standards/procedures. They should be developed and tested based on the business purpose and requirements, as well as subjected to a periodic review by MRM.

A committee, preferably one assigned specifically to model risk governance, should be responsible for the oversight of critical spreadsheets, including the guidelines detailed above. Business process managers are responsible for identifying potential critical spreadsheets and reporting them to Risk Management, as well as implementing and maintaining controls over critical spreadsheets. Risk Management should be responsible for maintaining the inventory of critical spreadsheets.

Critical spreadsheets with assumptions will undergo the tool or model determination process but may fall under the requirements of a critical spreadsheet rather than a model if deemed to be a low-risk model (or not a model).
Internal Audit should test controls for spreadsheets designated as critical spreadsheets during relevant reviews throughout its normal audit plan cycle. Internal Audit may further test the integrity and accuracy of the calculations within the critical spreadsheet. Ad hoc reviews may also be conducted by the business owner or an independent function upon request by the relevant Committee.

6.2. Tools

Tools are neither models nor critical spreadsheets. They are systems that assist in business decision making but have no stochastic properties to them. Tools are generally either vendor based informational systems, or they aid in data or risk preparation for further processing. These may be used for target based marketing, loan processing, documenting, risk data procurement, or operational based efficiencies. Assumptions could be present in a tool; however, they may not be testable.

Tools will not be validated; however, they should be tracked as part of the MRM inventory. The tool owners should be queried annually by MRM to ensure the tool in question has not been subject to change that would alter the current tool classification.

Summary – Right Size Recommendations for Critical Spreadsheets and Tools:

1. Define what a critical spreadsheet is for your institution, and differentiate between models, critical spreadsheets, and tools.
2. Maintain separate inventories of critical spreadsheets and tools.
3. Develop control standards for critical spreadsheets and ensure appropriate application of said standards.
4. Establish oversight for spreadsheets and tools through light touch reviews and tool attestations.

7. Right Sizing – Model Tiering

One of the critical areas of the MRM framework is having a model classification or tiering system that corresponds to the risk posed to the financial institution. From a regulatory perspective, SR 11-7 calls for banks to develop a method of measuring model risk:

> *'Model risk should be managed like other types of risk. Banks should identify the sources of risk and assess the magnitude. Model risk increases with greater model complexity, higher uncertainty about inputs and assumptions, broader use, and larger potential impact.' (p. 4)*

Additionally, SR 11-7 also allows MRM to take a risk-based approach when conducting model validations:

> *'The range and rigor of validation activities conducted prior to first use of a model should be in line with the potential risk presented by use of the model.' (p. 10)*

The objective of the model classification or tiering is to rank order individual models by risk in comparison to the rest of the models in the bank-wide inventory. This allows MRM to properly allocate resources, to prioritize, and to determine the level of thoroughness and frequency that will be required in the model validation, monitoring, and documentation processes. This practice can be especially important for smaller institutions, as they tend to have limited resources of headcount and budget for performing model control activities. Being able to prioritize and scope the work can help smaller institutions overcome some of these challenges.

When thinking about model risk, we consider both Inherent Risk (the level of risk in absence of any actions management might take to alter the risk's likelihood or impact) and Residual Risk (the risk that remains after any mitigating controls). However, the Model Tiering exercise typically focuses on the model's Inherent Risk since it is intended to rank order individual models based on the likelihood of a model risk event occurring PRIOR to mitigation and controls. In other words, model Residual Risk is a function of the model Inherent Risk and Mitigation & Controls (see Figure 1 below). In the equation in Figure 1, *Model Inherent Risk* includes the risk of using each individual model before risk mitigation & controls (*e.g.*, higher risk comes from higher model complexity, higher input/output uncertainty, stronger interdependencies, etc.); and *Mitigation & Controls* include elements from MRM Framework such as model documentation, model validation, issue management, model performance monitoring, and change management. For the purpose of this section, we will focus on discussing the Model Inherent Risk assessment or the Model Tiering process.

Figure 1. Inherent Risk & Residual Risk of Model

Model Tiering can be a combination of both qualitative and quantitative processes. While there is no single standard, two main methodologies are widely observed in the industry[1]:

1. Scorecard Approach
2. Decision Tree Approach

7.1. Scorecard Approach

One of the widely used model tiering methodologies observed in the industry is using a score card type approach to aggregate scores of various risk factors and then classify the model into High, Medium, or Low (Tier I, II, or III) categories. With well-defined criteria, these risk factors generally take into account the risk and the impact of model failure. For example, based on a bank's risk appetite and their belief of the risk arising from using each individual model, banks may use these risk factors to evaluate their model's inherent risk: Model Reliance, Complexity, Uncertainty, Dependency, Materiality, and Visibility (see Figure 2 below). Details of each risk factor are discussed below.

Figure 2. Model Tiering Risk Factors

- **Reliance** – Reliance measures the importance of the model output (*e.g.,* Is the model output a sole driver of a business decision, or does the model provide non-essential

[1] Kiritz, N., Ravitz, M., & Levonian, M. (June 2019). Page 59. Model Risk Tiering: An Exploration of Industry Practices and Principles, *Risk Journals, Journal of Risk Model Validation*, Volume 13, Number 2, DOI: 10.21314/JRMV.2019.205.

information, and does a workaround exist if such information/model output is missing?)

- **Complexity** – Higher complexity assumes higher risk. This measures the complexity in model formulas or the methodology. It considers whether the model is statistical in nature or just uses basic arithmetic. Transparency/interpretability of development and the number of input variables may also impact a complexity score.
- **Uncertainty** – Uncertainty measures how predictable the model output is: does the model depend on a significant number of assumptions/limitations? Is the output highly uncertain/volatile/unpredictable?
- **Dependency** – Stronger interdependencies of models assumes higher risk; it considers how many upstream and/or downstream dependencies the model is known to have.
- **Materiality** – Materiality can be defined as how the errors in the model or misuse of the model would negatively impact the bank financially.
- **Visibility** – Visibility can be defined as exposure to the model output. Relevant questions include: What is the impact of the model errors and distribution of the resulting output? Would it impact the institution's reporting to third parties (*i.e.,* regulators, rating agencies, shareholders, financial reporting), multiple departments, or to only one department/area?

Depending on how the model is used and on the potential risk presented to the bank, each of the above factors can be assigned a score of 3-2-1 (or High-Medium-Low risk) to rate their risk significance. The scores for each of the factors can then be aggregated to produce an overall score that can be used to classify the model into different tiers (Tier I, II, or III) based on the bank's chosen thresholds. A sample scorecard calculation can be seen in Figure 3 below.

Figure 3. Sample Model Scorecard

Criteria	Reliance	Complexity	Uncertainty	Dependency	Materiality	Visibility
Rating	2	3	3	2	3	3

Total Model Score:	16	Model Tier:	Tier I*

* Based on bank's chosen threshold for each model tier

While the answer to some of these factors can be straightforward (*e.g., Does the model have any upstream or downstream dependencies? Will the error impact external reporting, or will it impact only one department/area?)* most of them have subjective aspects and may require qualitative expert judgment. For example, while model complexity, output uncertainty, and error materiality are important indicators of model risk, they are very difficult to measure objectively. To remain as transparent and objective as possible, some large banks may use statistical fitting of data or other quantitative analyses to derive the rating. However, this can be especially challenging for smaller institutions because they may not have the technical expertise to conduct such analyses or may not have sufficient historical data to support the studies. Another challenge for smaller institutions is that there may not be a mature bank-wide risk management program to leverage. Using the materiality risk factor as an example, large institutions with a strong risk culture may have a more matured Enterprise Risk Management (ERM) program where they may have already done a study to define the materiality dollar amount at different significance levels. If such thresholds have already been defined at the enterprise level, MRM may be able to leverage the existing thresholds to help define materiality for model risk. This, on the other hand, may be difficult for smaller institutions as those financial thresholds may have never been well defined within the organization.

7.2. Decision Tree Approach

The Decision Tree approach is another widely observed methodology used in the industry to measure model inherent risk. A simple decision tree has the advantage of being easy to understand and transparent to multiple stakeholders. In addition, when designed in a simple fashion, the decision tree approach does not require complicated algorithms or granular metrics, since a binary outcome of 'Yes' or 'No' can easily lead to the next stage of the decisioning process. However, the challenge of this approach is that if there are multiple risk factors in the evaluation process (such as the ones introduced earlier), using the decision tree alone can be complicated, overwhelming, and may lead to difficulty in interpretation, especially when different risk factors contribute different weights in impacting the risk. In addition, the visual representation of the decision can get even more challenging when multiple levels of categorical variables are introduced[2] and weighting impact is considered.

To address this challenge, some of the large institutions may build their decision tree in an application with various drop-down options. When it becomes really complicated (*i.e.,* multiple risk factors with different weights being considered), those applications may even use artificial intelligence or machine learning algorithms to process the decisions. Many people may even argue that this process alone can be a model! While large organization

[2] Kiritz, N., Ravitz, M., & Levonian, M. (June 2019). Page 60-61. Model Risk Tiering: An Exploration of Industry Practices and Principles, *Risk Journals, Journal of Risk Model Validation*, Volume 13, Number 2, DOI: 10.21314/JRMV.2019.205.

may have the resources to build a decision tree application, this approach is simply not practical for smaller institutions as most of the smaller institutions have limited models in their inventory (typically <50) and will not be able to justify the cost of purchasing a vendor application to build a decision tree tiering system.

7.3. Possible Solution

As discussed above, both Scorecard and Decision Tree approaches have their own pros and cons, and they both present unique challenges to smaller institutions. To name a few, the risk drivers used in the Scorecard Approach may be highly subjective, and it may be difficult for smaller institutions to objectively quantify the risk. On the other hand, while the Decision Tree Approach can be logical and easy to understand by both technical and nontechnical audiences, introducing multiple risk drivers in the Decision Tree approach can make the process complicated and overwhelming.

Although expert judgment plays an important role in the Model Tiering process, it is recommended that practitioners try to use objectively measurable inputs wherever practicable in order to enhance transparency and consistency. To address the challenges discussed above, one possible solution is that smaller institutions can use a combined method of both Scorecard and Decision Tree approaches to measure model risk. Figure 4 below is a sample Decision Tree combining both approaches. Using this Decision Tree as an example, the following steps can be considered:

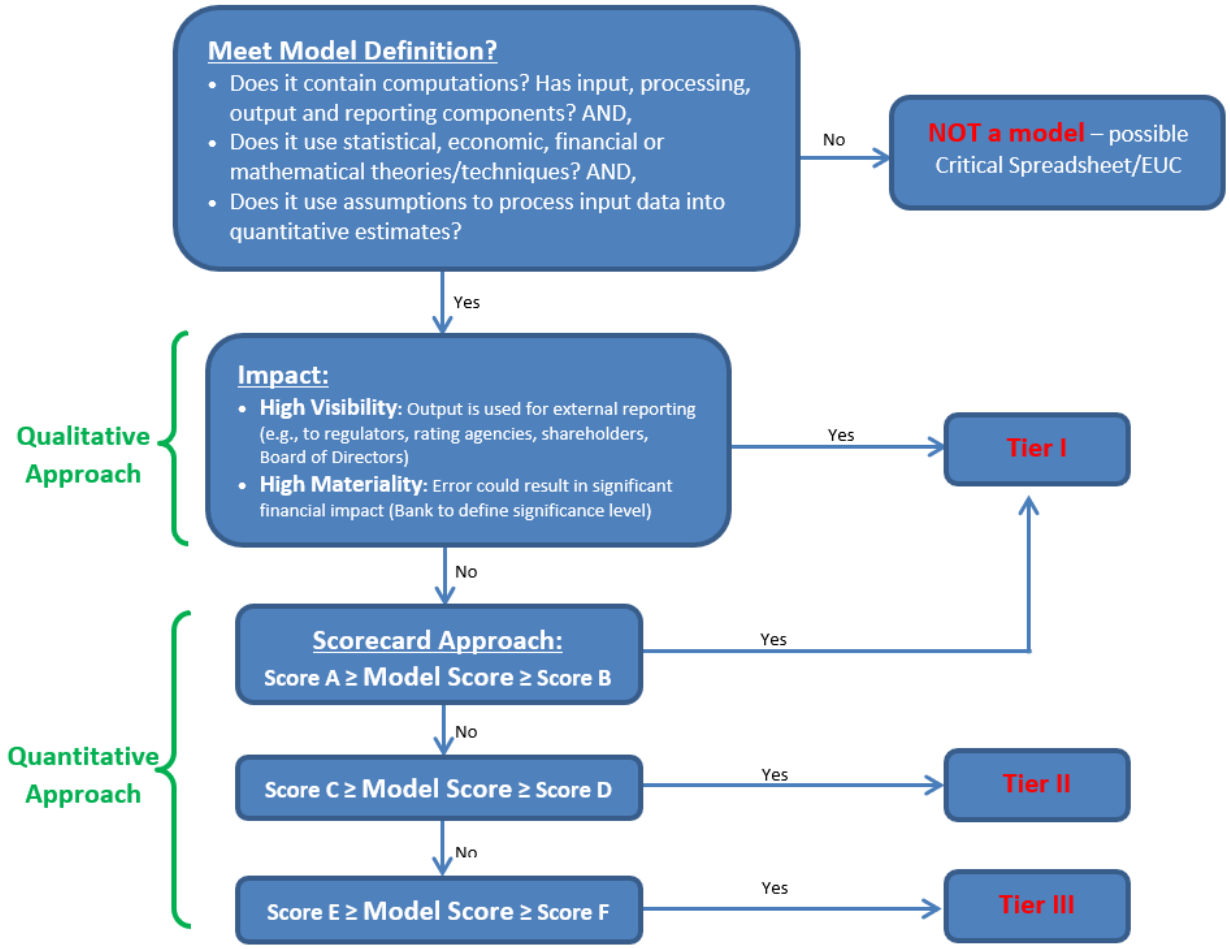
1. ***Model Determination***: When a tool is reported, the first step in MRM is to determine whether the tool meets the regulatory definition of a model. Tools that do not meet the model definition are not classified as models. However, since some of them might be used for analyzing business strategies, informing important business decisions, identifying and measuring risk, assessing adequacy of capital, and supporting external reporting, they may be classified as critical spreadsheets or End User Computing (EUC) tools. Since these tools are important to the organization, some level of reviews need to be performed to confirm computational soundness. For details of managing EUC tools, please refer to the 'Non-Model Critical Spreadsheet and Tools' section above.
2. ***Qualitative Approach***: Based on an organization's risk appetite, banks can then decide the risk factors they believe to be the most impactful from using the individual model. In the sample decision tree example below, Visibility and Materiality are selected.
    - High *Visibility* can be defined as exposure to the model output (*i.e.*, whether it is used for external reporting, such as to regulators, rating agencies, shareholders, Board of Directors etc.)

- High *Materiality* can be defined as significant negative impact from model errors or misuse of the model. The significance level can be determined based on the bank's risk appetite and can be defined quantitatively (*e.g.*, one quarter of bank earnings, certain percent of annual pre-tax income, etc.) or based on expert judgment.

If the model meets the Impact requirements from Visibility and Materiality, the model will automatically be rated as Tier I, with no additional scoring necessary.

3. ***Quantitative Approach***: If the model does not meet the Impact (defined as the combination of Visibility and Materiality) requirements, then the quantitative approach or the model scoring exercise will be performed. Based on the bank's predefined threshold, the overall model score (based on the score of the individual risk factors) can put the model into either Tier I, Tier II, or Tier III category. See Figure 3 above for suggested methodology on the scoring approach.

Figure 4. Sample Model Tiering Decision Tree



One point to note here is that the solution presented above is a suggestion and for illustration purposes only. As mentioned earlier, there are various ways of assigning model tiers in the industry. Depending on organization's size, risk appetite and the maturity of their MRM program, smaller institutions may choose to use the scorecard or decision tree approach alone or may even use simple rules based upon limited criteria, while larger institutions may take advantage of the combined approach to increase their objectivity, transparency and consistency during the model tiering exercise.

Summary – Right Size Recommendations for Model Tiering:

1. Model Tiering is used to rank order individual models in an organization's inventory by risk exposures and is intended to measure a model's inherent risk before mitigations and controls.
2. Two widely used Model Tiering approaches are observed in the industry: Scorecard Approach and Decision Tree Approach. Each approach has its own unique challenges for smaller institutions.
3. The risk drivers used in the Scorecard Approach may be highly subjective, and it may be difficult for smaller institutions to objectively quantify the risk.
4. The Decision Tree Approach can be logical and easy to understand by both technical and nontechnical audiences. However, introducing multiple risk drivers in the Decision Tree Approach can make the process complicated and overwhelming.
5. Although expert judgment plays an important role in the Model Tiering process, it is recommended that practitioners try to use objectively measurable inputs wherever practicable in order to enhance transparency and consistency. For smaller institutions, Model Tiering can be a combination of qualitative and quantitative process utilizing both Scorecard and Decision Tree approaches.

8. Right Sizing – Model Validation

Model validation is a critical component of a robust MRM framework, as it is the mechanism used to verify that models are performing as expected and are in line with their design objectives and business uses. Without a robust and independent validation function, a financial institution may fail to identify flawed assumptions or errant calculations that can result in utilizing inappropriate output for making important business decisions. Because of these adverse consequences, SR 11-7 notes that, "[a]ll model components, including input, processing, and reporting, should be subject to validation; this applies equally to models developed in-house and to those purchased from or developed by vendors or consultants."

It is easy to appreciate the importance of model validations, but it can be difficult to perform the necessary review work. Whereas large financial institutions often have large internal staffs that can leverage existing code and/or reports from similar models to conduct

validation work, smaller banks typically have fewer and/or less experienced employees at their disposal. Big banks also have the advantage of deeper pockets to fund external validation efforts, while senior management at smaller institutions may bristle at the prospect of engaging expensive consultants. Even the nature of the models themselves poses a significant challenge for smaller institutions – the vendor models they tend to rely on are generally opaque and difficult to review.

Despite these obstacles, it is important for financial institutions to maintain a robust validation framework. Regulatory guidance identifies three core elements of a successful model validation:

- Evaluation of conceptual soundness, including developmental evidence
- Ongoing monitoring, including process verification and benchmarking
- Outcomes analysis, including backtesting

While all validations should cover the points above, the actual activities may vary from model to model and institution to institution. For example, a High Risk (or Tier I) model should be subject to rigorous independent testing, while a light touch review of existing developmental evidence may suffice for a low risk model. Similarly, considerations can be made for the implementation status (performance monitoring may be limited for brand new models), validation status (repeat validations on stable models may not require extensive new testing), and type of model (underlying code may not be available for review for proprietary vendor models).

In order to ensure validation activities align with regulatory expectations and provide sufficient coverage for identifying material deficiencies, it is helpful to develop a checklist that outlines critical review activities for every model (e.g., assess the quality of the model design and construction, evaluate model assumptions and limitations, evaluate accuracy and completeness of development data, etc.). Once a generic checklist is established, it can be further customized for each individual model by identifying whether each item is in scope and what specific activities are planned to satisfy each requirement. This approach (1) helps ensure all the main validation components are covered, (2) helps define a test plan at the outset of each review, and (3) serves as documentation justifying scope.

This exercise is illustrated by the figures below. Figure 5 represents an excerpt of a potential checklist for a hypothetical High Risk, internally developed model, while Figure 6 demonstrates what the same portion of the checklist might look like for a low risk vendor model.

Figure 5. Sample Validation Scoping Checklist for High Risk, Internally Developed Model

Area of Review	Validation Requirement	In Scope? *(Yes/No)*	Justification for Scope *(if not being reviewed)*	Detailed Description of Validation Activity
Conceptual Soundness	Assess the quality of the model design and construction.	Yes	N/A	- Evaluate the quality and extent of developmental evidence. - Review empirical evidence supporting the methods used and variables selected. - Verify that model design and construction is well-informed and carefully considered. - Verify that model design and construction is consistent with published research and with sound industry practice. - Verify that model development is aligned with the intended use. - Compare the chosen approach to alternative theories and approaches.
	Evaluate model assumptions and limitations.	Yes	N/A	- Identify and assess key model assumptions. - Identify and assess potential model limitations along with any mitigation efforts. - Assess whether developmental testing conveys an understanding of model limitations and assumptions.
	Assess management judgment.	Yes	N/A	- Evaluate any qualitative information and judgment used in model development. - Ensure that qualitative/judgmental assessments are conducted in an appropriate and systematic manner. - Ensure that qualitative/judgmental assessments are well supported.
Data	Evaluate appropriateness and suitability of development data.	Yes	N/A	- Assess whether development data is consistent with the model purpose and design. - Assess the relevance of data used to build the model (should be reasonably representative of the bank's portfolio or market conditions). - Verify that all internal and external data sources are appropriate and of the highest quality available. - Verify that the timeframe of data used for development is appropriate. - Verify that any data transformations or adjustments are appropriate. - Evaluate the use of proxy data.
	Evaluate accuracy and completeness of development data.	Yes	N/A	- Perform data reconciliation between source systems and model. - Replicate development data set. - Review internal and external data for any potential errors. - Review internal and externa data for any gaps or missing information. - Confirm that any data transformations or adjustments were performed correctly.
Process Verification	Evaluate the code used to develop and implement the model.	Yes	N/A	- Review computer code implementing the model and ensure it is correct.

	Review the model's computational engine/mathematical applications.	Yes	N/A	- Verify that any mathematical theories or numerical techniques are performed correctly. - Independently recreate the model to ensure that it can be replicated. - Verify that the model's processing components successfully transform inputs into appropriate outputs.
	Evaluate the model's implementation and use.	Yes	N/A	- Confirm that the model is appropriately implemented. - Confirm that the model is being used as intended. - Verify that all model components are functioning as designed.
Outcomes Analysis	Assess final model outputs and reporting.	Yes	N/A	- Evaluate the model outputs and determine whether they are reasonable. - Review any reports presenting model outputs for accuracy and completeness.
	Assess and/or conduct model performance testing.	Yes	N/A	- *Sensitivity Analysis*: identify/evaluate any developmental testing; conduct independent analysis on input and parameter values (may involve varying inputs one-by-one or simultaneously) and confirm outputs fall within expected range or that deviations from expected results can be reasonably explained. - *Stress Testing*: identify/evaluate any developmental testing; conduct independent testing to check performance over a wide range (including extreme values) of input and parameter values; identify/verify any boundaries for the acceptable range of inputs; identify/verify any conditions under which the model may become unstable or inaccurate; confirm that any deviations from expected results can be reasonably explained. - *Benchmarking*: identify/evaluate any benchmarking performed during model development; perform independent benchmarking analysis (may include building a new model using alternative approach or comparing outputs to peer banks, historical experience, or prior model versions); confirm that any deviations from benchmark models can be reasonably explained. - *Back-testing*: identify/evaluate any back-testing performed during model development; perform independent testing by comparing model forecasts to actual outcomes; confirm that any deviations from actual outcomes can be reasonably explained. - *Additional testing*: perform individualized testing based on the model's limitations and assumptions and select/perform any additional quantitative and qualitative tests or analytical techniques based on the model's methodology, complexity, data availability, and the magnitude of potential model risk to the bank; analyze the impact of key assumptions and choice of variables on model outputs; confirm that the model performs as intended.
	Evaluate the ongoing monitoring of the model.	Yes	N/A	- Confirm that a plan for ongoing monitoring of the model is in place and being followed. - Assess the planned monitoring activities and associated thresholds. - Propose alternative measures/metrics where appropriate.
Governance	Confirm compliance with policies and procedures.	Yes	N/A	- Evaluate the appropriateness and adequacy of model governance and oversight. - Review sufficiency of policies and procedures for operating, maintaining, and updating the model.

	Evaluate access and change controls.	Yes	N/A	- Verify that access to the model is limited to relevant parties. - Confirm that only approved parties can make changes to the model. - Assess quality and change control procedures. - Confirm that all changes to the model are logged and auditable.
	Evaluate plans for model management.	Yes	N/A	- Assess the appropriateness of the model's usage horizon and plans for future updates. - Determine whether roles and responsibilities for relevant staff are defined. - Review the expertise of staff to use, maintain, and update the model.

Figure 6. Sample Validation Scoping Checklist for Low Risk, Vendor Model

Area of Review	Validation Requirement	In Scope? *(Yes/No)*	Justification for Scope *(if not being reviewed)*	Detailed Description of Validation Activity
Conceptual Soundness	Assess the quality of the model design and construction.	Yes	N/A	- Evaluate the quality and extent of developmental evidence. - Verify that model functionality is aligned with the intended use. - Compare the chosen vendor to alternative products.
	Evaluate model assumptions and limitations.	Yes	N/A	- Identify and assess key model assumptions. - Identify and assess potential model limitations along with any mitigation efforts.
	Assess management judgment.	Yes	N/A	- Assess support for the vendor selection. - Evaluate customization options selected by the bank.

Area of Review	Validation Requirement	In Scope? *(Yes/No)*	Justification for Scope *(if not being reviewed)*	Detailed Description of Validation Activity
Data	Evaluate appropriateness and suitability of development data.	Partial	Only have access to internal data.	- Assess whether development data is consistent with the model purpose and design. - Verify that all internal data sources are appropriate and of the highest quality available. - Verify that the timeframe of data used for development is appropriate. - Evaluate the use of proxy data.
	Evaluate accuracy and completeness of development data.	Partial	Only have access to internal data.	- Compare a sample of internal data to source systems. - Leverage any previous audits of source data.
Process Verification	Evaluate the code used to develop and implement the model.	No	Proprietary vendor product with no available code.	
	Review the model's computational engine/mathematical applications.	Partial	Proprietary vendor product with limited access to background functions.	- Run key model components to observe functionality.
	Evaluate the model's implementation and use.	Yes	N/A	- Review internal User Acceptance Testing. - Verify that system integration was successful. - Confirm that the model is being used as intended.
Outcomes Analysis	Assess final model outputs and reporting.	Yes	N/A	- Evaluate the model outputs and determine whether they are reasonable. - Review any reports presenting model outputs for accuracy and completeness.
	Assess and/or conduct model performance testing.	Partial	Effort required to perform independent testing is outweighed by the low impact of potential errors.	- Review developmental testing from vendor. - Confirm existence of internal performance testing.
	Evaluate the ongoing monitoring of the model.	Yes	N/A	- Confirm that a plan for ongoing monitoring of the model is in place and being followed. - Assess the planned monitoring activities and associated thresholds. - Propose alternative measures/metrics where appropriate.

Area of Review	Validation Requirement	In Scope? *(Yes/No)*	Justification for Scope *(if not being reviewed)*	Detailed Description of Validation Activity
Governance	Confirm compliance with policies and procedures.	Yes	N/A	- Evaluate the appropriateness and adequacy of model governance and oversight. - Review sufficiency of policies and procedures for operating, maintaining, and updating the model.
	Evaluate access and change controls.	Yes	N/A	- Verify that access to the model is limited to relevant parties. - Confirm that only approved parties can make changes to the model. - Assess quality and change control procedures. - Confirm that all changes to the model are logged and auditable.
	Evaluate plans for model management.	Yes	N/A	- Assess the appropriateness of the model's usage horizon and plans for future updates. - Determine whether roles and responsibilities for relevant staff are defined. - Review the expertise of staff to use, maintain, and update the model.

All validations should cover the same breadth of activities, but the depth of review may vary depending on the risk level of the model and/or its transparency. Utilizing a checklist approach can help maintain a consistent framework while still allowing for flexibility in activities. It can also help provide a road map for inexperienced analysts or for external consultants to adhere to MRM program requirements.

In addition to customizing the scope of validations based on the underlying characteristics of a model, banks can further differentiate between models by setting different validation timelines. For example, High Risk (or Tier 1) models likely warrant annual or biannual validations to ensure that they remain appropriate for use, while Low Risk (or Tier 3) models may only require a full scope review every four or five years. Financial institutions can (and should) also take other circumstances such as the number and materiality of changes, and recent performance monitoring results into consideration when determining the appropriate cadence of validations.

Overall, regulatory guidance offers financial institutions some flexibility in how they want to conduct model validations. Smaller banks in particular should take advantage of this opportunity to thoughtfully deploy resources in a manner that addresses model risk while still maintaining operational efficiency.

Summary – Right Size Recommendations for Model Validation:

1. Create a checklist of high-level validation requirements to assess models' conceptual soundness, ongoing monitoring, and outcomes analysis.
2. Carefully note whether items are out of scope (due to lack of information, no changes since prior validation, etc.) with supporting rationale.
3. Prior to each validation, complete the checklist with specific validation activities to address the generic points appropriate for the model under review.

9. Right Sizing - Reporting

Reporting on model risk is not a singular event. Regulators point out that reporting is expected at various points and across various aspects. These may be characterized across these three key and sequenced dimensions:

1. Business/Functional Purpose – This reporting is based upon output and results of individual models. Generally speaking, this reporting occurs between the model owner and their respective committee (i.e. ALCO Committee, BSA Committee, CECL Committee, Loan Committee, Fraud Committee etc.). The reporting is considered by Model Validation and may be used to evaluate the governance of the model as well as the effectiveness of model user(s). Key elements that Model Validation will expect include performance of the model, output, explanations to the changes in results (period to period), relevant assumptions, model sensitivities, and benchmark results.
2. Model Validations – This reporting is conducted specifically on each individual model. The report is from MRM to the model owners, but it is also provided to the MRMC (Model Risk Management Committee) for consideration and approval to place the model into production. The validation reports should be consistent, follow the MRM policy/framework, and should detail cited issues (and severity) across the five areas of the model validation – including model development (conceptual soundness, data, implementation, governance, and documentation). It is a best practice to provide recommendations for remediation. These validation reports provide the basis for the next area of reporting.
3. Aggregate Reporting – This reporting is MRM's aggregate view across all models related to model validations, issue management, and overall adherence to the MRM approved practices. Additionally, this reporting should include any exceptions,

overlays, and a model inventory. MRM will typically present this view to executive committee on an ongoing basis (i.e. ERC, MRMC, and Board of Directors). The reporting should enable senior management to understand the level and direction of model risk, along with sufficient supporting evidence on the drivers of that risk.

Summary – Right Size Recommendations for Reporting

The challenge of model risk reporting for smaller banks is scope. The absence of guidance with reporting on specific models, and the high dependency on vendor models, leaves operationally focused users with uncertainty on what are reportable items. It can lead to a wide range of practice. As such, it is recommended that smaller institutions consider the following as a useful practice:

1. Institute an expectation that reporting should exist across the three areas as identified above: Business/Functional Purpose, Model Validations, and Aggregate.
2. Determine the specific areas which are to be reportable. The Business area should cover output, changes of output, model performance measures, and others. The Validation report should be standardized and consistent. The Aggregate risk report should cover specific items – exceptions, model risk index, overlays, inventory, past due issues, and other higher order model risk components.

Align the reporting with the model risk framework to ensure MRM expectations are clear. Once it has been determined what exactly will be generated through the reporting, set the reporting requirement in the policy.

10. Right Sizing – Governance

Regulatory guidance related to model risk governance is an overriding principle. Even if model development, implementation, and/or use are satisfactory, overall model risk effectiveness cannot be achieved without strong governance. It should be evidenced across various activities in which the models are selected, implemented, used, monitored, remediated, and used for decisions. As such, governance should not simply be a singular form, but rather layers of control spanning from the developer to the Board. The roles and responsibilities of governance should be expressly articulated in either the Model Risk Policy and/or Model Risk Framework and should be approved by the Bank Board. Central to this function is the presence and evidence of review and challenge. Without this, there are points of failure that may arise throughout the entire lifecycle of the model and the ultimate output of the model.

There are aspects of governance that present similar challenges across all organizations regardless of size, but smaller institutions also have their own unique issues. The most commonly shared challenge is the institutional pressure to progress. This includes the need to make decisions that push the organization forward towards an objective, and on a timeline – such as bringing a product and pricing to market – to satisfy regulatory requirements (such as stress testing, pricing models, Basel parameterization, or CECL) or to stem the increase in fraud or money laundering. This institutional pressure can place managers in a difficult position of model concurrence. By the time a problematic model is requested for approval at a higher committee level, material time, costs, and efforts have incurred. There may be no immediate model alternative, and time is up. The appetite for meaningful challenge may be limited, or even non-existent. Governance may be present at this stage but can be influenced by real pragmatism.

The struggles of smaller institutions are exacerbated by the lower familiarity of statistical modeling and testing techniques, along with the heavier reliance on vendor models. This is a difficult combination. Since these vendors are in the business of selling models, they tend to focus on sales and less so on supporting evidence for the requisite validation. They typically have a self-interest in limiting publication of their model development knowledge and justification with the customer – vis-a-vie model documentation. Vendors also tend to use consortium data or pooled data for model development and testing which may limit their options for disclosure.

Vendor reluctance may be explained by either the protection of their product (*i.e.,* intellectual property), reducing an onset of numerous customer queries, recognition that the development was not exhaustive, deflecting the cost and burdensome task of documentation, or deducing that their customers are not traditional modelers, which would otherwise inquire on model-centric questions and/or evidence. None of these reasons should ever be acceptable. When the absence of complete information becomes apparent, it is extremely difficult to track down and secure. To address these various challenges, smaller institutions should consider the following:

1. Ensure well defined governance roles/responsibilities exist throughout the entire model lifecycle, and agreements related to complete evidence are provided at the earliest stage.
2. Establish heightened interface between the MRM (Model Risk Management) and the model risk community for guidance and for clarification while maintaining independence. Requesting MRM to provide a "cradle to grave" guidance through the entire process does not violate independence, but rather ensures the owners are aware of the various tasks.
3. Ensure the applicability of the model that is developed on consortium data.

The formality, structure, and scope of governance should be present through/from the following areas:

1. **Model Risk Management Committee** (MRMC) – The roles of this Committee should be clearly defined in a charter – *e.g.,* approve model overlays, exceptions to policy, approve models for use, and approve the key risk indicators for model risk aggregation. This committee should also be made aware of the MRM activities, issue remediation/closure, inventory, validation delays, and any regulatory or audit concerns. Focus of this Committee should be on the aggregate level of model risk, as well as deficiencies of specific models that have an impact on the summary profile. This committee should not be reviewing/approving statistical models, but rather obtain the final model rating recommendation from MRM and only approve on model use aspect.
2. **Business Committees (*e.g.,* BSA Committee, MRC, ERC, Loan Committee, ALCO, Fraud Committee, etc.)** – Model owners should ensure that throughout the entire model procurement, implementation, and use, governance related activities are conducted in the relevant business committees in order to prevent missteps, to ensure transparency, and to consider the appropriate use of the model. These Committees should be well informed and should decision the following:
    a. **Model selection process** – to gain an approval to purchase a specific model. Provide multiple vendors' pros and cons, together with a recommended vendor. For example, are the full data requirements and availability reconciled, are MRMs requirements sufficiently documented in the contract, is there clarity around who will run the model, who will monitor, who/when does redevelopment, are there contingency plans if issues arise? These, and more, should be provided to the Committee structure when deciding which vendor to use.
    b. **Model Assumptions** – to review/approve key assumptions necessary to run the model. These can include economic scenarios, interest rates, or other input factors that have a level of uncertainty. The vendor should explain which variables are a greater influence on the output, which in turn should be appropriately reviewed/decided by the Committee.

   c. **Model Input/Output** – similarly, the inputs/outputs of the model, as well as the performance of the model should be conveyed and approved. For example, if account volumes change or profiles of customers change, it may have a dramatic impact in fraud, approvals, or other projections. Model output, in a form of reporting, should also be reviewed/challenged with the Business Committee structures.

3. **Model Risk Management (MRM)** – should rely on the MRMC to take action when issues remain delayed and unresolved, or when model owners do not follow MRM guidelines *(e.g.*, using unvalidated models, expanding use without notification, or other out of policy activities), and/or when the aggregate level of model risk has risen to a level outside of appetite that requires further decisioning. Within MRM, all validations should be reviewed and challenged by the designated authority to ensure the validation standards are met, regardless of whether the validation was conducted internally or externally. The external validations should have an ongoing review/challenge by MRM to ensure both consistency and thoroughness are achieved.
   a. **Model Annual review –** an annual review should be conducted on all models. The annual review is to consider the model performance – when/if model degradation has occurred; business environment – when/if the environment, product, or affected model population has changed; model complexity – when/if the quantification has expanded scope or functionality; and model/spreadsheet impact and use – when/if the model/spreadsheet has broadened its use beyond that which it was validated for. The annual review may lead to a change in tier, re-validation, or escalation to MRMC for further consideration and decisioning.
4. **Audit Committee** – Reviews on the effectiveness of MRM should include a determination on whether policy, procedures, standards, inventory, validations, issues, and remediation are all present and in practice. Further, a review of the data central source systems should also be evaluated for the presence of controls as reflected in the broader data governance program. These should be the primary areas that Audit brings forward to the Audit Committee for comment and feedback.
5. **Data Governance Committee** – is to ensure that a program exists to satisfy a bank objective of complete and accurate data. This should include a framework with identified data stewards, controls and testing, standardized definitions (consistently

defined), procurement methods (collecting data), treatment (missing or outliers), integrity assurance (reconciliations), and remediation (fixing or generating data). Because model owners are ultimately customers of data, a well-defined and controlled data system is critically important for the processing of models throughout the bank. This is key evidence expected by MRM throughout the validation process.

6. **Annual Department Head or Sponsor Certification – Model Identification** - on an annual basis there should be a process in place where the head of departments/model sponsors should attest/certify that the models listed on the model inventory is the entire list and there are no other models or process operating other than those already captured within the model inventory.

Summary – Right Size Recommendations for Governance:

1. Use Model Risk Management to guide where governance should exist at each stage of the model lifecycle, and to guide the types of decisions/challenges to be made – from vendor selection to model output and review.
2. Ensure the vendor can/will comply with all the evidence necessary for a validation before the contract is finalized. It is a better practice to formalize with specific language.
3. Formalize the data governance to ensure availability, completeness, and integrity can be achieved. Identification of controls, and subsequent testing will also be critical.

11. Conclusions Related to Philosophical Practice

Right sizing regulatory guidelines on model risk management for smaller financial institutions is a practical matter that the guidance itself expects. The precept of "size and complexity" is intended for such consideration. This whitepaper was written to illustrate a set of practices that are practical and that meaningfully align to the guidance – neither ambiguous nor prescriptive. In the course of these recommendations, our shared experiences and challenges are more common than uncommon. These recommendations are to provide newcomers to model risk with a blueprint, while also providing more seasoned institutions with a common sense platform to which to migrate. The notion of right

sizing is largely about fostering a program that enables management to envelop and control model risk, set measurable assessments on model performance, and enable model owners to operate the models with sufficient clarity and input.

12. Workgroup Members

Thomas Dahlin – SVP Director Model Risk, Centennial Bank

A 25+ year international risk professional with in-depth experience in managing, developing, and reviewing models across credit and operational risk – across multiple countries. Tom has engaged with the full spectrum of stakeholders across model risk – including developers, users/owners, management, vendors, and regulators. He has led multiple banks through the quantification efforts and implementation of CCAR, BSA, AML, CECL, economic capital, loss forecasting, AMA, and stress testing models. He has led modeling teams in both large and small banks – including JP Morgan Chase, HSBC, RBS and most recently Centennial Bank. He is a Board member of MRMIA, promoting best model risk practices. Tom believes in a healthy dose of pragmatism, curiosity, and an abundance of communication to best ensure successful outcomes. Tom holds a MA.Ec from the University of Hartford, with a concentration in Quantitative Methods.

Jessica Jiang - VP Model Risk Manager, Texas Capital Bank

As a Model Risk Manager at Texas Capital Bank, Jessica leads a team of professionals managing the Bank's Model and EUC Risk Management programs. Jessica has over 15 years of experience in the financial industry. She has spent the last five years at Texas Capital Bank leading the Model Risk Management functions of model validation, model governance, committee reporting, regulatory reporting and overall Model and EUC life-cycle management. She also has leadership responsibility of directing independent validation on key bank models, including DFAST, Capital Stress Testing, CECL, ALM, Credit Underwriting, Fraud, and BSA/AML models. Prior to joining Texas Capital Bank, Jessica worked at Goldman Sachs for 10 years primarily in the Insurance Risk and Market Risk areas. Jessica received both her bachelor's and master's degrees from University of California at Davis in Agricultural and Resource Economics, with heavy focus on quantitative analysis.

Briony Pentecost - VP Model Risk Manager, Banner Bank

Briony has 10 years of experience in the financial industry. Since joining Banner Bank, Briony has designed and implemented the Bank's model risk management framework, which entailed developing policies, procedures, and templates supporting model governance, development and implementation, and validation. In her role as Model Risk Manager, she oversees the governance and reporting activities for the Bank's entire suite of models and is also responsible for performing and supervising annual reviews and model validations, including those performed by external resources. Briony previously worked in the Quantitative Services practice at Promontory Financial Group, Inc. assisting financial institutions with regulatory compliance, particularly with respect to model validation. Briony holds a Bachelor of Arts in Economics from the University of Pennsylvania and is a Certified FRM.

Amy Polasek - VP Model Risk Manager, Prosperity Bank

Amy has over 33 years of experience in banking and has been specifically focused on model risk management since 2015. As a Model Risk Manager at Prosperity Bank, Amy is responsible for tracking the model's life cycle from development through decommission. She performs an annual periodic model review of each model, facilitates model validation engagements, tracks and reports model testing and changes, and manages the bank's model inventory, critical spreadsheet listing and non-model listing. Amy received her bachelor's degree in Finance from the University of Houston.

Arun Musinipally – MBA, MSA - Deputy Director Model Risk - Centennial Bank

A seasoned risk management executive with 20 years experience in driving risk management objectives by managing, developing, and reviewing models across insurance, credit and operational risk disciplines. Arun successfully held senior executive roles and led quantification, modeling and regulatory assurance efforts in insurance and financial institutions – including Allstate Insurance Company, HSBC, RBS and most recently Centennial Bank. Arun has experience with Basel, CCAR, CECL, DFAST, AMA, Catastrophe stochastic models, Stress testing models and other financial models. Arun excels in simplifying complex statistical, financial and modeling problems to practical and results oriented business solutions.

Blade Blevins – Manager Model Risk – Centennial Bank.

Blade has nearly 10 years of banking experience, encompassing aspects of retail, lending, and model risk management. His hands on experience with model owners, vendors, and management has largely been with early, and/or first time adopters of model risk. He was

directly involved during the inception and implementation of Centennial's model risk management program and governance structure, with particular focus on controls of critical spreadsheets.