ProSight™

Model Risk Framework for Medium-Sized and Small Banks

RMA & BAI:
Together we're ProSight

ProSightFA.org

About ProSight Financial Association

ProSight Financial Association empowers financial services leaders to strengthen and advance our industry. Formed through the merger of BAI and RMA, trusted organizations with rich histories and deep expertise in risk, compliance, and retail and commercial banking, we are here to support you during times of great change, guide you towards new opportunities for growth, and help you act with confidence. As ProSight, we've enhanced our ability to support you at a time when the industry is challenged to meet changing customer needs, adopt new technologies, and manage more complex risk and compliance issues. Our work creates positive ripple effects throughout financial services organizations and our industry—and ultimately helps consumers, businesses and communities thrive. Learn more at ProSightFA.org.

Acknowledgments

The ProSight Model Risk Framework for Medium-Size and Small Banks has been reviewed and approved by ProSight's Model Validation Consortium, and is published by ProSight Financial Association.

ProSight would like to recognize the work of its current Model Validation Consortium Advisory Board.

Advisory Board Chair:
Aaron Benson, Zions Bancorp, Salt Lake City, UT

Members:
Jeff Broecker, Forbright Bank, Potomac, MD
Adam Chin, TowneBank, Portsmouth, VA
David Clatfelter, Mechanics Bank, Walnut Creek, CA
Steven Crowe, Busey Bank, Champaign, IL
Mike Dudgeon, Park National Bank, Newark, OH
Angela Jenkins, ANBTX, Terrell, TX
Jessica Jiang, Texas Capital Bank, Dallas, TX
Kole Kostic, Atlantic Union Bank, Richmond City, VA
Nikolai Kukharkin, MUFG Bank, New York, NY
Dori Luli, Western Alliance Bank, Phoenix, AZ
Tony Mieloch, Bremer Bank, Saint Paul, MN
Arnold Pashi (Events Chair), First Citizens Bank, Raleigh, NC
Bri Pentecost, Bank of Hawaii, Honolulu, HI
Trevor Woolley, Berkshire Bank, Pittsfield, MA

Please direct inquiries to Katie Williams at rmaxchange@rmahq.org.

Design by Christopher Santoro.

July 2025

©2025 ProSight Financial Association. All rights reserved, including the right to reproduce this report or portions thereof in any form whatsoever.

Table of Contents

Introduction

It has been more than 14 years since the publication of *Supervisory Guidance on Model Risk Management*, issued jointly by the Federal Reserve in SR 11-7 and the Office of the Comptroller of the Currency in OCC (Bulletin 2011-12). In that time, the largest banks have dramatically improved their model risk management (MRM) programs by increasing the number and skill sets of those involved in model risk management, enhancing policy and procedure, and improving technology to make model risk management more efficient.

Progress has been slower and more difficult at smaller institutions and community banks, even though the use of models at these institutions continues to grow rapidly. This rapid growth is driven by the many opportunities models bring, for example in the form of more efficient and repeatable processes. However, these opportunities carry risk as well, which needs to be effectively managed. For this reason, the FDIC in 2017 adopted the Fed's Supervisory Guidance on Model Risk Management for all banks with assets greater than $1 billion, definitively requiring these institutions to bolster their MRM practices. This paper describes the key components of a sound model risk management program, with a focus on smaller institutions, where the struggles to stand up a solid program are distinct from the larger national or multinational institutions.

To that end, we provide a guide for banks to develop a model risk management program, including: a governance framework, a model identification process, model risk rating, a model inventory, a model development process, model validation, an ongoing model monitoring program, and finally a risk appetite statement. We start by exploring model governance and the concept of a model governance framework.

Model Governance

When tasked with building out a model risk management program, many banks find it difficult to know where to start. That is where the notion of a model governance framework comes into play. Once the framework is established, the process of assigning roles and responsibilities followed by the development of policies and procedures becomes easier. Developing this framework, educating model owners and users about their roles and responsibilities related to the framework, and reviewing it on a regular basis leads to strong, sustainable model governance.

Developing a Framework

How does an institution go about putting together a framework? The first step is determining one's objective(s). Next, we need to determine what it takes to achieve those objectives. Finally, we need to assess what it takes to make those achievements sustainable.

As described on the following , governance is the tool used to ensure we achieve and sustain our objectives. This is very similar to how the U.S. Constitution serves to achieve and sustain the objectives of forming "a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense," etc.

The bank's model risk objectives can and should be placed in a risk appetite statement where the firm's appetite (and capacity) for model risk are prescribed. Once these objectives are initially solidified a governance framework should be developed to achieve those objectives and make them sustainable.

Model Risk Management Framework

Making this more concrete for a bank in a model risk management context, a framework could look like the following:

1.

Objectives:

a. Identify all models used at the bank.

b. Assess the risks associated with those models.

c. Assess the firm's aggregate model risk profile and appetite.

d. Manage risk within the firm's appetite.

2.

Plan to Obtain Objectives:

a. Develop a model identification process.

b. Develop a risk assessment process for individual models and in aggregate.

c. Determine how much model risk the firm is comfortable with.

d. Develop a plan to reduce or retain risk within the firm's risk appetite.

3.

Plan to Make Objectives Sustainable:

a. Development/revision of process to ensure objectives are sustainable.

b. Policies regarding roles in developing objectives and ensuring they are achievable and sustainable

c. Governance: review of framework execution, assessing performance of individuals and groups in relation to policies and procedures, and making recommendations for refinements.

Model Risk Management Governance

This can be a problematic scenario for many institutions, particularly smaller banks with budgetary constraints. Ultimately, it is the responsibility of everyone at the institution – starting with the Board of Directors, extending to Senior Management including Business Heads that are the owners of the models and the users of the models, and naturally the risk management function and audit. They each have roles and responsibilities in a properly functioning governance framework. However, the Chief Risk Officer needs to play a central role in designating someone as the "Head of Model Risk Management" for the bank. That individual(s) may have additional titles and responsibilities depending on the size of the model inventory and the complexity and risk of the models. However, as a centralized role, the head of MRM works for the bank (including the business) to ensure that policies and procedures are developed, that they are commensurate with the risk footprint and risk appetite of the firm, and that the Head of MRM has the authority to implement these policies. Note that we emphasize that the Head of MRM works for the bank. The bottom line is that strong model risk management is not only about policies and procedures, but also encompasses revenue retention and, in some cases, revenue enhancement.

A strong governance structure should provide reporting structure, approval authority, dispute resolution, and escalation procedures and set the enterprise model risk profile and tolerances within the stated risk appetite of the Board. It is important that the Board of Directors be the driving force behind a strong MRM governance structure, as the Board is ultimately responsible for the success or failure of the firm. As FIL 17-022 states:[1]

"As part of their overall responsibilities, a bank's board and senior management should establish a strong model risk management framework that fits into the broader risk management of the organization. That framework should be grounded in an understanding of model risk – not just for individual models but also in the aggregate. The framework should include standards for model development, implementation, use, and validation."

1 https://www.fdic.gov/news/news/financial/2017/fil17022a.pdf Supervisory Guidance on Model Risk Management, SR 11-7, Federal Reserve Board April 4, 2011.

Risk Appetite Statement

Risk Appetite Statement Banks large and small should have a risk appetite statement, approved by the Board, that lays out the objectives of the MRM program and will, in fact, guide its development and sustainability. It does not have to be perfect at first. The statement will evolve as the bank evolves, so don't let best be the enemy of good. Something as simple as the following is a good beginning

Identify all models utilized or to be used at the bank, assess their risk to the institution and manage these risks within the bank's appetite. This entails at minimum ensuring that all models are validated prior to first use with limited and time-constrained exceptions; ensuring models are revalidated on a regular basis commensurate with the risk of the models; resolving issues identified in the model validation process in a timely fashion; monitoring the performance of all models and taking prompt corrective action when model performance deteriorates below acceptable thresholds; ensuring models are properly documented and users know the appropriate use of any model they utilize; ensuring model changes are properly managed and reviewed; and ensuring model dependency is understood and properly managed.

This simple risk appetite statement lays out the broad objectives of the MRM program to be developed. The first objective in our risk appetite statement is the identification of all models utilized at the firm. To do this, our governance framework must have a definition of a model. We tackle that next.

Model Definition

To identify models, you must have an idea of what you are looking for. So the next step is to define what a model is. It is reasonable to start with a definition utilized in SR 11-7 or the FDIC's 2017 guidance:

"Model refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates."[2]

Though this is a good place to start for your MRM governance document, it is useful for all banks, in particular smaller banks, to augment the model definition with so-called "walking around questions." These can be used to help potential model owners and users know the key differentiators between End User Computing Tools (EUCTs) or simply "calculators" and models.

The guidance goes on to say that a model consists of three components: an information input component, which delivers assumptions and data to the model; a processing component, which transforms inputs into estimates; and a reporting component, which translates the estimates into useful business information.

Though this is a good place to start for your MRM governance document, it is useful for all banks, in particular smaller banks, to augment the model definition with so-called "walking around questions." These can be used to help potential model owners and users know the key differentiators between End User Computing Tools (EUCTs) or simply "calculators" and models.

The questions below tackle three parts of a model and begin to clearly delineate between what could be a model and what may be a EUCT. Many calculations performed in the finance group fall short of being a model when viewed in light of these questions. For example, depreciation calculations which are mandated by finance accounting rules do not require assumptions (e.g., possibly one-time accounting choices) and any firm would calculate the same depreciation on a piece of equipment purchased at the same time for the same amount with the same accounting regime. That is, there are no assumptions, no choices in the combination of the data, and no uncertainty in the outcome.

We observe, very importantly, that these questions (and the definition) do not say anything about where the tool is implemented. It is the concept that makes a model, not where it is implemented. So, a model can be implemented in Excel or nowhere at all! If a person uses pencil and paper every time they "run" the model, it is still a model.

Now that we have ironed out the definition of a model, to meet our next set of risk appetite statement objectives we must identify and risk-assess (or rate) the models of the bank.

The questions are the following:

1. In addition to data, does the tool require assumptions as a key input? Could a different individual, business unit, or bank have different assumptions?

2. Are those assumptions involved in combining the data? Are there various choices in the combination of the data or processing component that could vary from person to person or firm to firm?

3. Is there uncertainty in the output of the tool? That is, if it produces a (proposed) decision or a number, could someone starting with the same data arrive at a different decision or a different outcome?

2 https://www.fdic.gov/news/press-releases/2020/pr20091a.pdf One key componentis the requirement to "conducting ongoing monitoring to identify and report suspicioustransactions," which may result in CTRs andSARs. For many institutions this analysis isin large part performed by 3rd-party modelswhich are also utilized in fraud detection.

Is The Tool A Model?

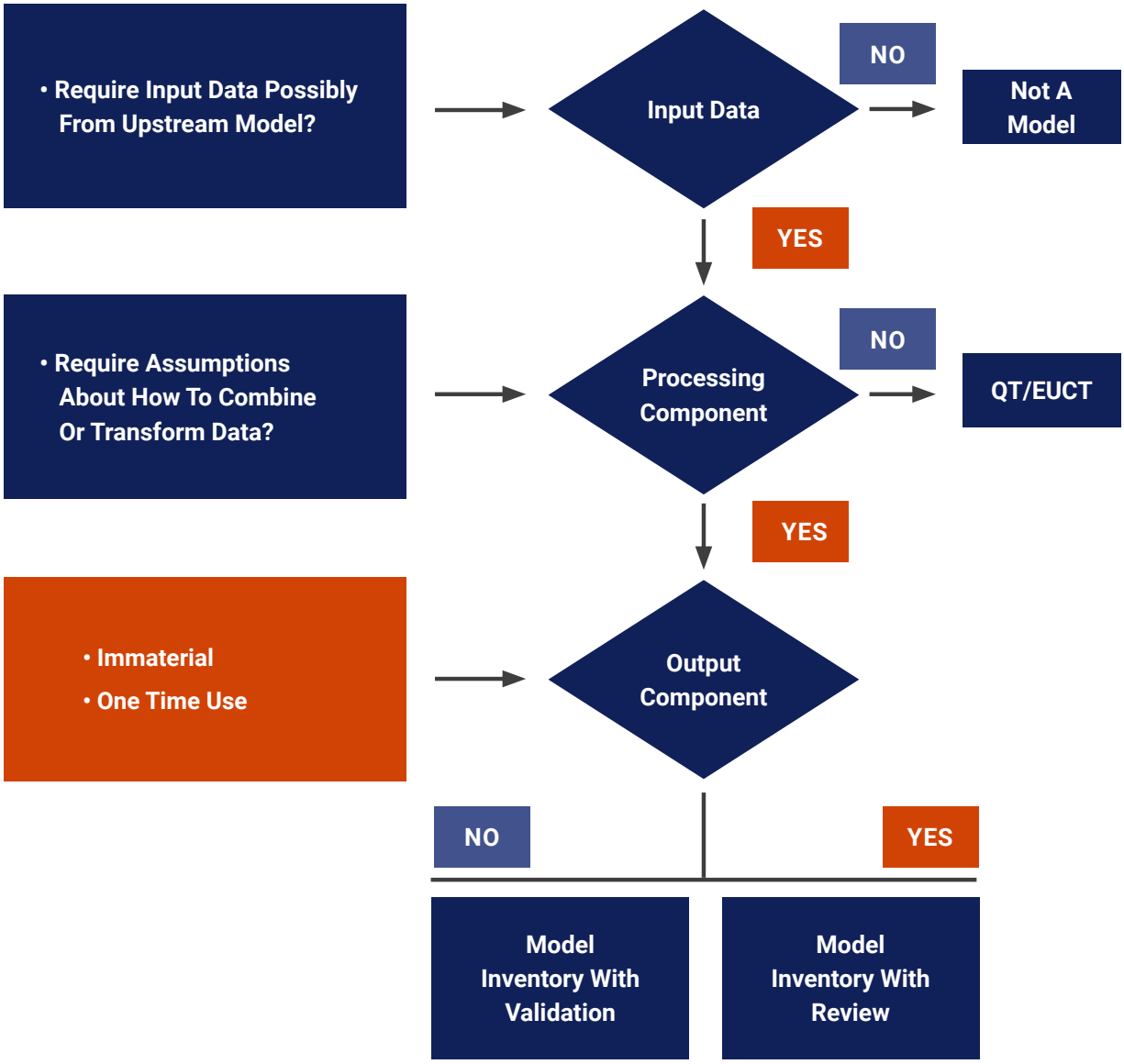

Figure 1

Model Identification and Risk Rating

Model Identification Process

Model identification is the important starting point in the model lifecycle. In this stage, banks of all sizes establish the process to identify all models (and nonmodels) at the institution. This process should be done firm-wide at least annually and when a potential model is planned to be developed or purchased.

Let's take each of these in turn, with model inventory having a section of its own to be discussed later. First, we discuss roles and responsibilities. An identification policy should at minimum define roles broadly across three groups: "Enterprise Risk Management," "Model Owners," and "Model Users." Best practice is to include a fourth group: Internal Audit. The roles and responsibilities (R&R) assigned to these four groups at minimum should include the following:

- **Enterprise Risk Management:** Develops the model definition and provides training on MRM including the model identification and risk rating process. Reviews and approves identified models and tools determined to be non-models. The head of MRM will also maintain the Model Inventory.
- **Model Owners:** Ensure models are properly identified, risk rated, validated, and used for their intended purpose. Compliance with the MRM policy is achieved by presenting tools to be assessed and assigning model users and competent individuals that will ensure the model remains in compliance with policy.
- **Model User(s):** Are responsible for the appropriate use of the model and the escalation of any performance degradation. Additionally, they share responsibility to ensure the model is validated on a timely basis in compliance with this policy.
- **Internal Audit:** Reviewing the model identification approach designed and executed by MRM to ensure it meets requirements set out by the bank's policies and it aligns with regulatory requirements.

These R&Rs can also be associated with the three lines of defense framework. However, this can often be confusing, in particular at small institutions where individuals wear many "hats" depending on their dayto- day activities and they are not sure which line they are in! It is often clearer if they consider R&R in terms of the four principle players outlined above: Model Owner, Model User, Model Risk Management, and Audit.

It is useful to note that the Model Owner and Model User are the risk takers, therefore they are the first line of defense. A key to community banks (and really all banks) having an effective model identification process (and more broadly an effective MRM program) is not focusing on whether individuals are in a certain "line of defense" at the start of the exercise. The focus should be on the roles and responsibilities they need to play in the MRM process from a Model Owner, Model User, Oversight, and Audit perspective. The rest will sort itself out.

Keys to developing a successful process

1. Clearly established roles and responsibilities.
2. Training
3. A good questionnaire covering model identification and potential risk ratings (remember Voltaire!).
4. A method for retaining and utilizing the information (a model inventory).

Model Risk Rating

Once a tool is identified as a model by the institution it is important to identify the risk of the model to the bank. Like any other product used or distributed by the bank, the use (or lack thereof) of models comes with risk that needs to be understood, ranked-ordered as best as possible, and mitigated to conform with the risk appetite of the bank. SR 11-7 defines model risk as "the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports. Model risk can lead to financial loss, poor business and strategic decision making, or damage to a bank's reputation".

We start by defining the components, Inherent, Intrinsic and Residual risk, and then illustrate how they can be utilized to rank-order model risk in the spirit of (1).

The guidance goes on to state that two primary sources of model risk are due to:

1. The model may have fundamental errors and may produce inaccurate outputs when viewed against the design objective and intended business uses.
2. The model may be used incorrectly or inappropriately.

A good starting point to rank-ordering model risk is to consider:

1. A simple three-tier approach – for example high, medium, and low-risk models.
2. Separating (individual) model risk into three components: Inherent, Secondary(Intrinsic), and Residual risks.

Inherent Risk

Inherent model risk, as per its name, is risk that is difficult to change or mitigate due to the ”nature” of the model. This difficulty may be due to the use of the model or the type of model, but the two largest components of Inherent risk are typically:

- The model’s role in critical decision making.
- Financial exposure.

Inherent risk is also commonly thought of risk before controls are established, for instance monitoring or testing. Models that are used in critical decision making have the potential for high Inherent risk. These are models that are used to make credit decisions, for pricing, to manage interest rates or the balance sheet, that have client impact, or are used to meet regulatory reporting requirements, to mention some of the potential critical decision making situations.

Financial exposure is typically defined in terms of the size of the potential loss either due to direct financial loss (e.g., mispricing of credit) or in terms of poor business or strategic decision making (e.g., capital allocation). This is most often the largest consideration in the Inherent risk category and can be categorized by the dollar exposure of the portfolio, products, or clients the model is used to manage.

Bank A:

Uses vendor Consumer Credit Approval Model in an automated fashion to review and decision consumer loans. The process is completely automated to have “borderline” declines reviewed by a credit officer for further review and potential approval.

Bank B:

Uses vendor Consumer Credit Approval Model as one component of Credit Officer Review process for each loan application. The officer looks at 10 risk factors where the model output is one of the equally weighted factors, with most of the other factors expert-judgment driven.

In these two very real examples the financial and reputational impact of the same model is vastly different based on its degree of use in critical business decisions.

It is also important to take into account the impact and degree of the model's importance in critical decision making to assess its true financial exposure. Even when models are used to manage risk for very similar portfolios at different banks, the risk to the bank can vary depending on the role in the decision making process of that model. The example above illustrates how the risk for two identical models can dramatically affect their "exposure" or materiality to the bank.

It is worth noting that, increasingly, banks are considering the knock-on effect of reputational damage, which could have long-term earnings impacts. In fact, reputational impacts from the misuse of models could present some of the most serious challenges to community banks going forward. For example, recently, the reputational issues due to regulatory fallout from poor BSA/AML models or fair-lending practices have been problematic for institutions large and small.[3] In some cases, these problems have even led to the regulatory-enforced delay of growth activity, like acquisitions.[4] This is not to say that reputational impact should be the largest factor in determining the amount of risk associated with a model, but that it should not be forgotten in the process.

For these reasons, banks also frequently consider two additional factors in the Inherent risk category:

- Non-financial exposure (including reputational risk).
- Regulatory Risk.

3 A mid-tier bank was forced to delay an acquisition for over three years after regulators unearthed BSA issues. Four years after the Fed issued its agreement to address compliance problems, it freed the bank from its enforcement action. https://es.kaufmanrossin.com/news/big-banks-continue-to-struggle-with-bsa-aml-issues/

4 https://www.fdic.gov/regulations/examinations/supervisory/insights/sise16/si-se2016.pdf

Intrinsic (Secondary) Risk

Besides Inherent risks, models have what is known as Intrinsic risk. The term can be defined slightly differently by market practitioners, but there is increasing recognition at smaller institutions that the management of Intrinsic risk is critical to successful model risk management. Some of the items commonly considered in model Intrinsic risk are the following:

- **Data or Inputs:** Quality, stability over time, inclusive of output from upstream models and their risk tier.
- **Complexity:** Is this model wellknown? Has it been peer-reviewed and used in the industry for years? Or not? Does the model rely on several different assumptions, each of which must tie together to make a logical whole? Or is it based on one relatively simple principle?
- **Theory:** Is the underlying theory well-known or intuitive? This also could have a "maturity" aspect. Has the model theory been in practice in the industry for a long time?
- **Performance:** Has the model proven accurate (predictive) in the past or in back testing? Have the results had wide dispersion?
- **Implementation:** Is the model easy to implement and run? Is it implemented in a system that has several control features, ranging from approved users, change controls, etc.?

Often these two components (Inherent and Intrinsic) are combined into a single risk score which may collectively be called the risk ranking or rating. In either case, for many institutions this exercise leads to the final risk rating for the model. We will talk about how it is implemented in a moment, but we will first discuss Residual risk and how that is utilized at some institutions to either derive a final risk ranking/score or used to complement the risk ranking.

As just noted, the amount of risk associated with a model, without incorporating any mitigating controls is referred to as either the model risk rating or score or, more correctly, as the sum of Inherent risk and Intrinsic risk. As noted earlier, most of a model's Inherent risk comes from its exposure to financial loss. However, a model which has a large exposure may be more or less risky than a comparable model with similar exposures due to other factors, including input or data quality (including reliability) issues, model complexity, or implementation of the model (Intrinsic risk). Many of these Intrinsic (or Secondary) risks can be "nurtured" or mitigated to reduce the total model risk. The net effect after mitigating these Intrinsic risks is a lower Residual model risk. That leads us to our final component definition.

Residual Risk

Even when model risk is large due to Intrinsic risk factors, there may be controls that reduce the overall risk of the model. What's left when these controls are introduced and properly implemented is known as Residual risk. Most controls are placed around the Intrinsic risk factors but (dynamic) exposure controls can be utilized as well to reduce the Inherent risk at times. Typically, all these controls fall under the broad heading of governance. If there is a strong governance framework for models this, by its very nature, decreases model risk individually and collectively. Below we list the usual controls that are typically utilized to reduce Intrinsic risk:

- **Data/Input:** Review and cleansing of input data, including the definition, review, and removal and monitoring of the frequency and degree of outliers.
- **Performance Monitoring:** Clear guidelines related to good performance versus bad performance (or questionable performance). This is usually developed during model development and implemented to guard against performance degradation. Models with large exposure (Inherent risk) that have large performance variance need to be monitored more frequently to minimize Residual risk.
- **Usage Monitoring:** Inappropriate use is one of the risk factors identified in SR 11-7. Appropriate monitoring of usage and changes of usage with appropriate review before those changes take place can mitigate usage risk.
- **Reporting:** The appropriateness, ease of use, and interpretation of the model outcomes in reporting are critical to appropriate and risk-controlled use.
- **Exposure Control:** In some cases, exposure can be dynamically decreased based on risk factors both internal and external.
- **Governance Framework:** At most institutions, the existence of a sound governance framework is recognized as a risk mitigant for some or all models.

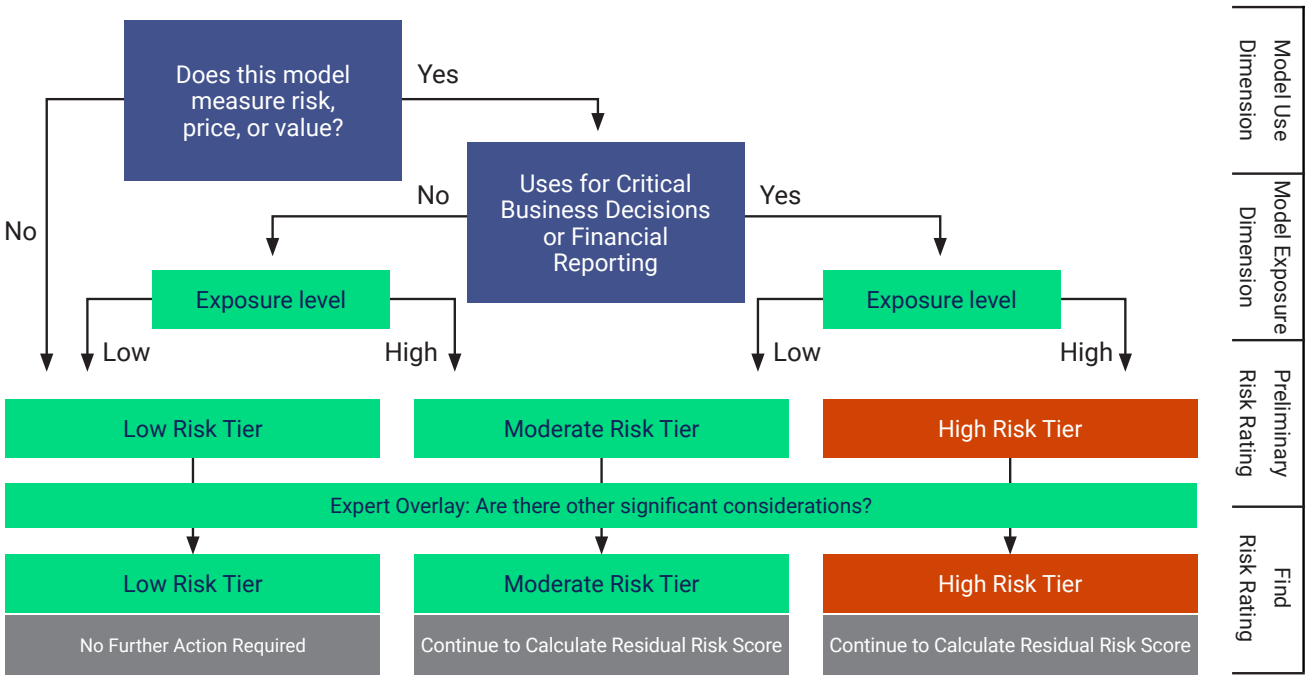

Figure 2 By Sanjeev Mankotia & Aruna Joshi

Model Risk Tiering Methodology		
Inherent Risk Assessment	**Score**	**Application of Controls**
Measure Price, Risk, Value, Balance Sheet Impact	0,5	
Critical Decision Making	0,5	
Financial Exposure	0,5	
Non-Financial Exposure	0,5	
Intrinsic Risk Assessment		
Data Quality	0,5	
Outcomes Analysis	0,5	
Implementation	0,5	
Performance Monitoring	0,5	
Maturity	0,5	
Complexity	0,5	
Risk Adjustments	-5,0,5	
Residual Risk		

Table 1

The degree to which each of these components has documented, verifiable frameworks in place to control the risk presented can provide reduction in the Intrinsic risk of the model. This can be used to produce a total risk score or risk tier. Some of these elements can only be introduced after the model is in production (e.g., performance monitoring) and provide no risk relief when a model is initially validated and risk rated.

A schematic of the proposed risk tiering outlined above is depicted in Figure 2.

Table 1 outlines a good framework for a risk tiering process where a score of 0 indicates low risk in a particular category and 5 indicates high risk. There is an additional risk adjustment category that is subjective and discretionary. The mapping of the total score to risk tiering needs to be calibrated to the firm's risk appetite.

Model Inventory

Once the models are identified and risk rated, they will need to be inventoried. You may ask, why does my bank need an inventory, and does the system need to be complex?

The first answer is every bank needs a model inventory. This is because the models in use at the firm, their performance, limitations, users, and even owners change over time. Also, there are required model updates and changes that need to be tracked to ensure timely resolution of issues and to identify model rollbacks when new model changes do not go as expected.

A model should be included in the inventory when it is first proposed, whether it will be built in house or it is going to be purchased from a vendor. This will enable the timely tracking of model development/acquisition milestones like documentation, model validation, and model monitoring.

As for the second question, the complexity and the technology behind the inventory should be commensurate with the extent and risk of model usage at the bank. Most banks can start with an Excel spreadsheet to prototype and manage the model inventory before building or buying more advanced tools. Remember: If you know the risks you want to manage and how to manage them, you are in a better position to evaluate third-party tools. This will prevent the wasteful out-of-system modifications when the tool does not work in line with the bank's needs.

The model inventory at a small institution can be very basic, with the number in the inventory small in comparison to a national or multinational. Institutions around the $10 billion asset mark typically have an inventory ranging from 20 to 40 depending on the business model. However, more important than the count of models is the process for ensuring you have identified models and the inventory tracks the appropriate information over time. The model inventory is a dynamic risk management tool which evolves with the model risk cycle, the risk environment, and changes in the model and its usage.

Though the fields of the inventory should fit the idiosyncratic needs of the bank, the following field groups have become known as best practice:

- General model information.
- Model development information.
- Model validation information including performance monitoring.
- Implementation information.
- Approved uses.
- Attestation from model owners and users as to appropriate use and policy compliance.

We illustrate some of the common fields in use within these groups in Table 2 on page 19.

Group	Field Name	Comments
Information	Model ID	Unique Identifier
	Model Version	Track Changes/Version Control
	Model Name	
	Model Status	Development/In Use/Retired, etc.
Model Development Information	Date added to Inventory	
	Application Environment	Excel, Matlab, SAS, etc.
	Development Internal/External	Internally Built or Vendor Model
	Model Type	Statistical, Arbitrage Free
	Model Purpose/Products	CCAR, Stress Testing
	Model Owner Name	
	Model Owner Group	Business or Functional Area
	Model Developer Name	
	Model Developer Group	
	Model Development Completion Date	
	Model Inputs	Quarter ending balances, Charge-offs
	Source of Model Inputs	SNL. Bloomberg
Model Validation	Model Outputs	PD, LGD, etc.
	Model Risk Rating	
	Model Validator	
	Validation Internal/External	
	Date of Last Validation	
	Date of Next Expected Validation	
	Date of Last Annual Review	
	Date of Next Expected Annual Review	
	Model Performance at Last Review	
	Validation Status	
	Approval Conditions	
	Model Use Limitations	
	Data Limitations	
	Policy Exceptions	
Implementation	Implementation Date	
	Last Implementation Review	Implementations should be viewed at least during the (re) validations
	Next Implementation Review	
Use	First Use Date	
	Model User(s)	
	User Groups(s)	
	Approved Users	CCAR, Retail Underwriting
Retired	Retirement Date	
	Retirement Reasons	
Attestation	Model Owner	
	Management	
	Attestation date	

Table 2

Model Development

At many institutions, the risk management of models is considered after a model is developed or acquired from a vendor. This mindset poses real risks to the bank and should be remedied by incorporating model development into the model risk management process. Bluntly speaking, treating risk management as an afterthought is an error. It is important for every bank, regardless of its size, to understand the risks it is accepting when it proposes the development or purchase of a model. Therefore, the model development process must be a well-designed process and include, at minimum, model risk management, the model owner, and ultimate model users.

The Process Itself

Existing models can be absorbed into the development process. But here we focus on new models and changes to models. The first step should be identifying the business need for that particular model. The business leader should initially reach out to the model development team, which should then reach out to the risk management committee so that all components of model development, or discussions around existing model modifications, are properly and safely addressed. If a new model or vendor model is purchased, this will create a model inventory entry.

Risk management plays a critical role in the model development and model review processes. The risk management team is the body that will identify the needs of the organization as they apply to the model. Risk management will also outline the documentation necessary to ensure the model meets not just regulatory requirements but internal standards as well. If a third party (vendor model) is under consideration, third-party risk management will need to be engaged as another crucial player who will conduct some of the critical up-front negotiations with the vendor(s).

An effective model development process has at minimum the following components:

- **Purpose and Objective Assessment:** This involves the potential model owner or business leader, MRM, and the model developer assessing why the model is needed and the objectives of the model. Note that this should happen before the developer begins working on the potential model or the vendor demonstrates their model. This can simply be a meeting where model risk management learns about the proposed model, begins to formulate a risk assessment of the proposed model, and can formulate a validation strategy inclusive of resources. This also kicks off the model inventory process, with a model ID assigned and model purpose/use field populated.
- **Requirements or Expectations:** Outlining the model requirements in sufficient detail to benchmark subsequent development or vendor capabilities is essential to ensuring the developed or purchased product is ultimately fit for purpose. Portfolio or business coverage and access or control requirements should be included. To the extent possible, performance standards should be considered. This will also help develop the validation strategy.
- **Documentation Standards:** Developed by MRM and potentially tailored to individual model types, consistent and strong documentation ensures business continuity as developers change firms or roles or as new users utilize internally built or vendor models.
- **Development Guidelines:** In addition to the above, it is good practice to have development standards. Integral to this will be testing. As SR 11-7 notes: “An integral part of model development is testing, in which the various components of a model and its overall functioning are evaluated to determine whether the model is performing as intended.” Testing is where Requirements or Expectations (#2) are assessed and why it’s important to outline them initially. Testing should check the model’s accuracy, its robustness and stability, and include the impacts of assumptions. Stress testing the model to understand its limitations is also a critical aspect of development testing. These development guidelines can be included in MRM’s documentation standards or published separately.

Importance of Business Continuity

An organization could spend years building out models, but if the internal teams produce them with little or no documentation, business continuity is in jeopardy. The bank could use those models successfully for several years. But at some point, the individual or group that built the models moves on, and the firm has no idea how to address problems should they arise because there is no documentation. Imagine a scenario where no bank employees know the codes that implement the models, so the bank must hire an individual or company that can reverse engineer the model, costing thousands of dollars and countless hours.

That error in judgment also exposes the bank to a barrage of regulatory and financial risks. The point is that well-developed documentation is critical from both a business continuity and risk management perspective.

Using an Outside Vendor for Model Development

Before reaching out to outside vendors for model development or for a third-party model, the bank should first ask itself if it has the skill set internally to build the model. If the answer is yes, does that staff have the time to produce a model? If the bank does not have the staff currently, it can still develop it in-house, but it will need to hire the personnel with this expertise and bring them on board. All of this may be worth the cost because that model is going to need to be supported and maintained for years.

If the answer is 'no' and adding staff to build, say, an anti-money laundering model is cost prohibitive, the conclusion may be to use an outside vendor. But the question remains: What is the cost/benefit analysis of developing a model internally versus outsourcing the process?

Securing the services of an outside vendor, although cost effective, may introduce issues with sustainability and quality. How will the vendor meet all your standards? Increasingly, banks often overlook whether portions of a vendor's model or the model itself may be proprietary. If that is the case, it is absolutely essential that the bank understand that using a model with proprietary data or information does not relieve the bank of its responsibilities. If the model fails and catastrophic errors occur, you can sue the vendor, but your clients and the regulators will come after the bank, not the vendor. It is crucial that you still diligently risk manage that relationship. That means ensuring the bank understands even the proprietary components of the model well enough so the documentation works. Banks own the risk of the models they bring in-house. Period. The vendors do not own that risk.

The importance of model development documentation cannot be stressed enough. The standards for the documentation should be the same as for a model developed internally. Everyone internally should know what risk they are owning with the model.

This is certainly not to suggest that using a vendor's services is dangerous. What we are emphasizing is that when selecting a vendor it needs to be clear from the start that the vendor will be required to provide documentation that is in line with the bank's internal requirements and needs, and that the vendor will be working with the bank's risk management team. Also ensure the vendor can make required changes to the model going forward and, conversely, if a a vendor makes changes to the model's codes or other components, the bank is given notice and provided reasons why those changes are being made. Ask if those changes make sense for the bank and its needs.

Model Validation

Ensuring all models are validated and fit for use is of increasing concern to bank clients, investors, and regulators (and appropriately so). Furthermore, the standards around what is considered strong validation are increasing as the use of models grows and the risks involved become increasingly clear. This is also leading to a more consistent approach to model validation and benchmarks for a sound model validation.

One concern confronting small institutions trying to manage their risks appropriately is the question of how often to validate. In this regard, there is no short answer or predetermined time, but high-risk models should be validated and revalidated much more frequently, maybe annually in best practice. Regulators have made it clear that the scope, depth, and rigor of a validation should be commensurate with the scale and complexity of that model in the context of the individual firm. This applies as well to the frequency of revalidation.

As a simple example of how this frequency could differ by firm, we consider the same model alternately employed at a $250 billion asset institution for credit decisioning the entire portfolio and at a $10 billion asset institution where it complements expert judgment to risk manage 50% of a portfolio. The rigor of that validation should be different, downsized, and rescoped for that smaller institution given the risk profile of the portfolio and the use of the model. In particular, the range of tests and the severity of issues would be different for the larger institution.

The challenge for smaller institutions as the model inventory grows is attracting and retaining the resources to effectively validate models of various types. The expertise requirements vary greatly depending on the model use. As an example, the skills to appropriately validate a retail credit model differ vastly from those required to validate a BSA/AML model and to validate a derivative pricing model. As a result, many smaller institutions need to engage third parties to properly validate some or many of their models.

To handle this third-party arrangement effectively, the bank must ensure the third party has the requisite skill set to effectively validate the model. The bank should also baseline expectations in a statement of work (SOW) and expect regular check-ins as the validation progresses.

It is very important to observe that model validation is critical to sound risk management whether the model is developed internally or from a vendor. The bank should not and cannot rely on the vendor to perform an independent validation and should ensure that any vendor is willing to comply with the bank's model validation requirements, including sound documentation, performance monitoring, and independent review.

As noted, ongoing monitoring is a key aspect of model validation. Because of its importance, we also devote a few more comments to it in the following.

An effective validation framework should include three core elements:

1. Evaluation of conceptual soundness, including developmental evidence.
2. Ongoing monitoring, including process verification and benchmarking.
3. Outcomes analysis, including back-testing.

Some of the process elements that have become “best practice” in the industry to build upon these core elements are the following:

Pre-model development (revalidation) meeting

- ✓ Used to understand intended model purpose and requirements.
- ✓ Assess findings and observations from prior validations and their status.
- ✓ Discuss model changes, if any, since last validation.

Documentation review with developers and business leads

- ✓ Answer documentation questions.
- ✓ Make owners aware of any deficiencies that may slow the validation process.

Evaluation of conceptual soundness, including developmental evidence

Ongoing monitoring, including process verification and benchmarking

Ongoing monitoring plan review and critique

Implementation review

Regular check-ins with developer and business

Findings, issues, and recommendations

Validation report

Ongoing monitoring

Model Monitoring

All models should be continually monitored for performance. A monitoring plan outlining expectations should be reviewed as part of model validation and approved by the independent model validation team or model risk manager. The metrics and reporting should initially be based on back-tests performed by the model developer and potentially repeated by the validator and updated over time. Importantly, the degree of monitoring in terms of frequency, resource allocation, etc., should be commensurate with the risk of the model and therefore driven by the risk rating.

The topic of model monitoring may conjure images of fancy systems and armies of teams watching flashing buttons on rows of monitors, but that is not necessary. Good model monitoring occurs over the life of each model, and it can be as simple as ascertaining the model's performance in regular meetings with senior executives and model owners.

Effective model monitoring includes outlining performance expectations in terms of quantitative limits – for example, using a system of red, amber, and green is common. These should be reviewed on a regular basis (e.g., quarterly or semiannually), depending on the risk level of the model. Best practice is to establish escalation protocols to senior level committees and ultimately the Board. However, Board level escalations should be reserved for the highest risk models and degradation of performance to severe levels.

Setting up a monitoring framework for a model need not be complex to start. For example, take a credit decision model developed internally or by a vendor where back-testing has demonstrated 90% accuracy in differentiating good from bad credits (along with precision and other metrics). If the model returned 75-80% accuracy, it could be considered in the red or amber level, depending on the bank's acceptable risk level. The bank would then review the actual credits developed over the past six months or a year; determine the accuracy of the model; and assess whether the model performance is red, amber, or green.

It is key that when the bank establishes model monitoring, there are appropriate actions associated with each level of performance. Those steps should be in writing and well documented in the model policy and procedure. However, as with any policy, there could be exceptions. Figure 3 describes the components of a strong model monitoring program.

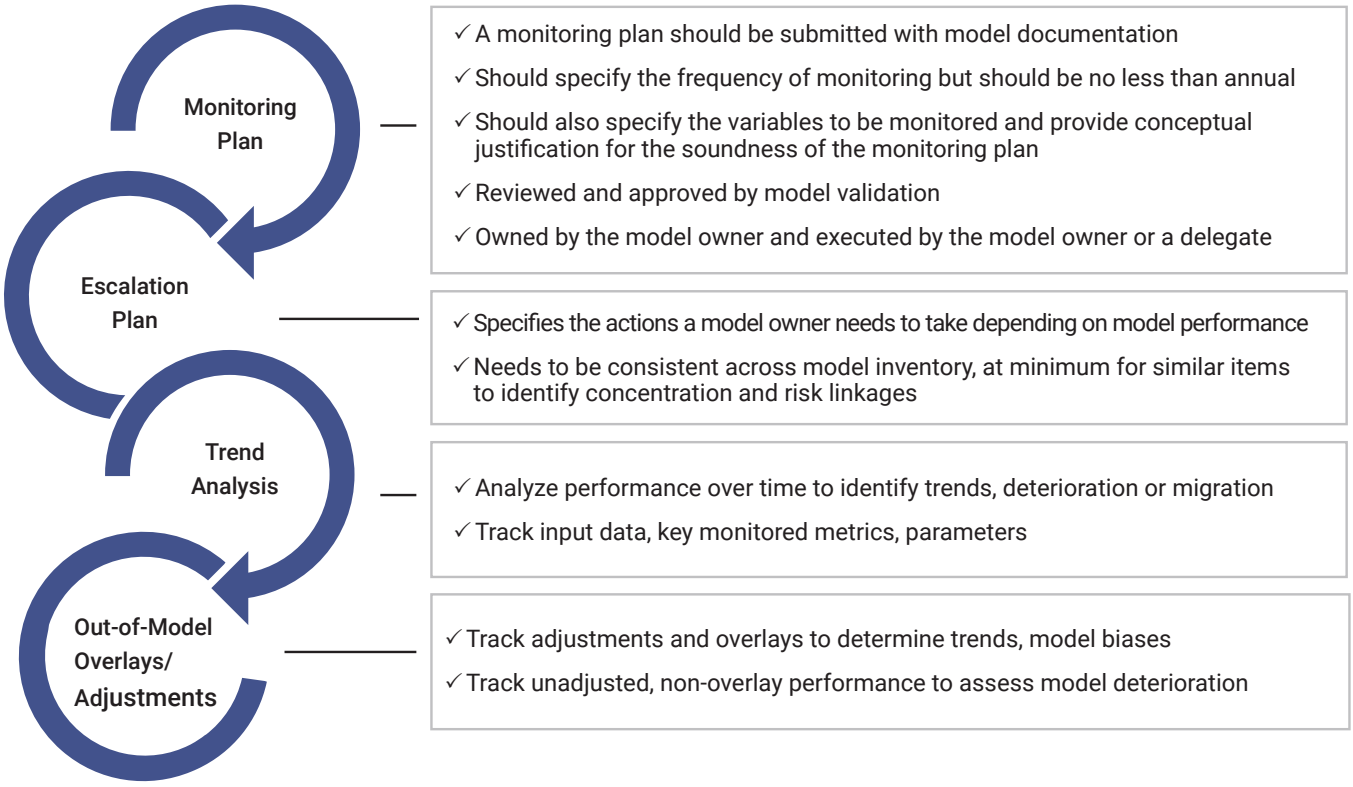

Figure 3

Model Risk Reporting (and Risk Appetite Revisited)

Reporting requirements continue to grow as senior management, clients, investors, regulators, and Boards seek to manage their interests related to the bank. Reporting requirements around model risk management are not immune to this trend. It is important to focus on the objectives outlined in this Model Risk Management Framework, how those impact the board, and let that drive initial reporting requirements. This will naturally lead to individual business/functional line reports as these leaders will need to understand their impact on Boardlevel reporting.

So, we start with asking and in turn answering the question: What does the Board need to know? Though the answer does depend on the bank, some of the core requirements are on the following page.

Each of these elements are critical in achieving the bank's model risk framework objectives and achieving sustainability. The challenge is efficiently organizing the risk into (at least) the "buckets" identified above to reduce complexity and increase clarity so Board members understand the risk. Starting from this perspective also better aligns business and risk reporting with the information the Board receives.

To efficiently digest and utilize this information most banks now have a risk committee of the Board. This is an oversight committee that guides the risk management practice and objectives of the bank. However, at many smaller institutions MRM is new to the Board and has not been fully integrated into the Board risk committee functions. We next discuss best practice in this regard.

Risk Committees

Management Risk Committee: The risk committee is a management level committee that has a crucial role in any bank, providing critical oversight and guidance to management to execute business within the risk appetite of the firm. Most banks, large and small, have developed risk committees. However, including model risk management as a responsibility of the risk committee will be new for many smaller institutions. To accomplish this, the risk committee needs to have a member(s) familiar with model risk and its various components as well as the best and current practices in managing that risk. This is a challenge for most small banks that can be minimized, but not alleviated, with ongoing training and the hiring of a model risk expert (presumably the model risk manager) and her inclusion on the committee. To be effective, the committee members should be representative of both the risk management side and the business side of the bank. There should also be policies and procedures for escalation to the risk committee, which should have ultimate decision-making authority.

Risk Committee of the Board: Usually information on model risk at larger institutions is provided to the Board through the management risk committee to the risk committee of the Board. Though it is not required to be a standalone committee, it is common practice for the largest banks and regional banks, and is increasingly best practice for banks approaching the $10 billion asset level, at which point the OCC and FDIC expect an even higher standard related to model risk management. At its core, a risk committee of the Board will help the Board fulfill one of its core obligations: To understand the bank's risk profile.[5]

Within the category of Board/management, the largest percentage of Matters Requiring Board Attention (MRBA) in a recent review by the FDIC on its reports of examination (ROEs) relates to corporate governance issues focusing on ineffective or incomplete policies and procedures.[6] Another area frequently cited in a recent analysis was Interest Rate Risk (IRR), where most of the MRBAs related to ineffectively monitoring, measuring, and controlling IRR, including establishing risk tolerance parameters for IRR model results. Most of these issues are best handled and even prevented by having a strong risk committee of the Board which has a dedicated stream for model risk management to address the increasing use and risk of models at community banks.

Examples of model risk issues that could be escalated to the committee are:

- Is the bank using overlays too often for a particular model?
- Is it time to recalibrate or rebuild?
- Does the bank have the appropriate number of resources?

5 https://www.fdic.gov/regulations/examinations/supervisory/insights/sise16/sise16-article1.pdf
6 https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum16/sisummer16-article2.pdf

What the Board Needs to Know:

- **What are the most important models for the firm?**
  - Importance should be stratified by risk type.
  - The risk ranking or Total Risk Score approach can be utilized to determine importance.
- **Under what conditions are the most important models expected to work well and not work well? In what circumstances are they likely to break down?**
  - Collectively, are model outputs credible?
  - What "moves the dial" in terms of key assumptions or judgments?
  - Are those assumptions and judgments reasonable?
- **Key dependencies and assumptions: What are the key dependencies or linkages in risk?**
  - Are all key models dependent on a limited number of factors, or …
  - Are models essentially independent of inputs and assumptions?
- **Governance:**
  - Is the governance framework working?
  - Are we adequately monitoring and describing/reporting on the state of model risk?
  - Are we quickly identifying gaps?
    - ✓Gaps in governance.
    - ✓Gaps in risk assessment.
  - Are we working with business, risk, and audit to provide adequate oversight?
  - Are controls maintaining model risk within acceptable bounds (i.e. risk appetite)?

Conclusion

The use and complexity of models will continue to grow at all banks, but the pace of expansion at community banks will likely outpace their larger peers for the foreseeable future. In part, this is due to the difference in initial baseline use of models for critical decision making at these institutions, but it is also closely tied to the relative benefits models will provide to community banks. However, these benefits do not come without risks that need to be managed to make the gains sustainable. Developing a sound, cost-efficient model risk management framework that is appropriately scaled for the institution is a key element of making the gains from increased model use sustainable. The framework outlined here can help in that endeavor.

ProSight™

ProSightFA.org