Effective Model Risk Management for Financial Institutions: The Six Critical Components

A White Paper by Brookton N. Behm, John A. Epperson, and Arjun Kalra
As a greater number of banks and other financial institutions adapt their risk management practices to meet more stringent regulatory guidelines, a new industry standard for model risk management is developing. Outlined here are the critical components of an effective model risk management program that complies with the tougher requirements.
As the financial institutions industry has evolved, banks increasingly rely on complex models to support their economic, financial, and compliance decision-making processes. These models are developed to represent real-world relationships. Because they are simplified representations of reality, however, the models present inherent risk to an institution. The complexity of a financial institution’s structure—which could include multiple legal entities and business units and a growing breadth of products and services—creates additional risk and increases the need to manage risk at an enterprise-wide level.

The Office of the Comptroller of the Currency (OCC) and the Federal Reserve Board issued “Supervisory Guidance on Model Risk Management,” important regulatory guidance, on April 4, 2011. According to the guidance, the term “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.”

As banks attempt to dissect the guidance and comply with regulatory expectations, a number of questions arise: What is a model? How often must a model be validated? How does a bank with models that are already in production meet the newly defined expectations of model development and implementation? How does an institution begin to develop an effective model risk management program?

To address these questions, financial institutions that rely on bank-specific models should use what regulators refer to as a “model risk management framework” for developing, implementing, and using the models. This framework enables banks to predict and identify risk more accurately and, therefore, make better top-level and line-of-business decisions based on model results. (See sidebar, “Risks in Banking Models.”)

To truly reduce risks inherent in bank models, a comprehensive and sustainable model risk management program should take into account a number of critical components, including the following:

1. Model inventory and assessment;
2. Model development, implementation, and use;
3. Model validation;
4. Model tuning and optimization;
5. Model governance; and

Each of these six components is discussed in this white paper.
Meeting Business Needs and Regulatory Expectations

Spurred by the industry’s need to meet regulatory expectations and business objectives, a greater variety of models is being developed and implemented. As models have proliferated, managing model risk has become more challenging for financial institutions. In some cases, banks have diluted the effectiveness of their model risk management programs by taking a piecemeal approach to managing model risk. This limited approach is often evidenced by highly fragmented operations and technology platforms, inconsistent top-down leadership, and a lack of enterprisewide accountability.

The guidance provides banks with a basic framework for deploying an enterprisewide model risk management program, and examiners now expect banks to use the framework when designing, implementing, and improving all models. Examiners are looking for a formalized, prescriptive methodology dictating the three basic components of the model risk management framework that the guidance identifies and requires:

1. Model development, implementation, and use;
2. Model validation; and
3. Model governance.

These expectations obligate banks to modify their model risk management approach in order to comply with the new industry standard.

In addition, regulators expect organizations that use models to provide evidence that the model risk management framework in place effectively identifies and manages the risk arising from the bank’s reliance on models. Evidence might include, for example, documentation that the bank has identified where its data resides and who is responsible for the quality of that data meeting model governance requirements.

Financial institutions are struggling with how to adapt a consistent and enterprisewide program to manage model risk in a way that is consistent with the supervisory guidance. Many organizations already have in place enterprisewide policies and procedures for financial models but might not have extended a similar approach to other operating or compliance models deployed by the organization.

Some banks are finding that reworking or enhancing existing model risk management processes to comply with supervisory guidance can be costly and complicated. Finally, in many cases, banks are realizing they have in place few of the model risk management components necessary for an effective model risk management program.
Defining a Model Risk Management Framework

Banks should build their models using the three requirements in the guidance but also with three additional critical components of effective model risk management (exhibit 1): model inventory, model tuning and optimization, and a model foundation. The model foundation components – business and regulatory alignment, supporting documentation, enabling technology, and project management – reflect overall supporting elements that further the effectiveness of models.

The determination that these particular components are critical to model risk management is based on a Crowe Horwath LLP analysis of regulatory guidance, examination findings, dialogues with regulators, and client insights. Financial institutions that implement and optimize the six components explained here can more effectively build a comprehensive model risk management program that meets business and regulatory needs.

Exhibit 1: Critical and Supporting Components of Model Risk Management
1. Model Inventory and Assessment

A model inventory takes stock of the implementing components – primarily the people, processes, and technology – that support bank models (exhibit 2). The inventory of existing models at any single financial institution may be large and can include both manual and automated processes and technology. Once a model inventory is completed, the organization should assess the enterprise risk of each item in the inventory in order to manage operational risks commensurate with the perceived risks in the model.

Exhibit 2: The Implementation Components for Models

Completing a model inventory requires taking the following three steps:

1. **Enterprise identification.** The organization’s risk management team defines the purpose, functionality, and intended use of models enterprisewide that support a bank’s economic, financial, and compliance decision-making processes.

2. **Model risk assessment.** The organization assesses the enterprise risk of the model. For example, the use of people, processes, and technology might represent an elevated risk that dictates the level and scope of the model risk management activities the organization applies to a particular model. Financial institutions should consider
2. Model Development, Implementation, and Use

A model must be well documented and tailored to the unique risk profile of the organization (exhibit 3). Due to the varying risk profiles and business requirements of different financial institutions, each model must be customized to meet the specific needs of the institution. When banks design models, relevant stakeholders – including executives, IT personnel, and affected line-of-business leaders – should assess for efficacy and regulatory compliance the design structure, the approach to implementation, and the use of the model’s output.

Exhibit 3: Designing and Using Models
Model Development and Implementation

■ **Model definition and requirements.** According to the joint guidance, “An effective development process begins with a clear statement of purpose to ensure that model development is aligned with the intended use.” Banks must document model definitions and requirements for meeting business and regulatory needs. This development process involves the bank’s identification of the various sources of its functional data. The process also includes defining and documenting performance, technical requirements, and assumptions, and the result serves as the baseline justification for the model.

■ **Model design.** A model must be designed based on the documented objectives of the model and various functional and technical requirements. Any limitations or merits of the model must be documented and appropriately considered as the model is developed. Model limitations – which could be tied to model inputs, uncertain assumptions, the processing component of the model, or the way the model output is created – will be an important consideration when model risk is assessed. Examples of model limitations are a lack of key data elements needed to identify risk or support business decisions; limited functionality of a system to produce model results; or an absence of reporting metrics needed to analyze the effectiveness of a model.

■ **Data management.** Models typically rely heavily on data quality, and data is never perfect. Efforts must be made to assess the completeness, accuracy, and relevance of assumptions and input data for the model.

To verify that the model is being used in a manner consistent with business and regulatory needs, financial institutions should implement a feedback mechanism to learn from and improve the process during the development, implementation, and post-implementation of the model.

Model Use

■ **Analysis of results.** According to the guidance, “An understanding of model uncertainty and inaccuracy and a demonstration that the bank is accounting for them appropriately are important outcomes of effective model development, implementation, and use.” Executives must analyze model results relative to limitations and design assumptions in order to assess the potential performance of a model before other stakeholders use the results.

■ **Continuous feedback and improvement.** To verify that the model is being used in a manner consistent with business and regulatory needs, institutions should implement a feedback mechanism to learn from and improve the process during the development, implementation, and post-implementation of the model. For a process of continuous improvement, management must empower users of models to provide input and feedback to the model designers and managers.
3. Model Validation

Ongoing evaluation of models is required to confirm that results are accurate and controls are adequate. The guidance defines model validation as “the set of processes and activities intended to verify that models are performing as expected, in line with their design objectives and business uses. It also identifies potential limitations and assumptions, and assesses their possible impact.”

While the concept of validation is not new, the guidance expands the expectations for an effective validation review. The guidance states, “All 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.”

Exhibit 4: Testing Models
Model validation confirms that an institution’s model is aligned with business and regulatory expectations and is properly executing tasks that take into account the underlying risks and lead to accomplishing the bank’s business objectives. The approach to validation focuses on the following four components related to the conceptual design, system, data, and process for models (exhibit 4):

1. **Conceptual design validation.** Do the conceptual design and capabilities of the model meet the identified business and regulatory needs? In assessing the conceptual soundness of a model, executives should consider key metrics and evidence supporting the ability of the model to accurately predict risks and execute the business objectives of the model. This process may include performing back-testing or outcome analytics to compare model outputs to corresponding actual outcomes or results.

2. **System validation.** All technology and automated systems implemented to support a model have inherent limitations. System validation independently confirms that the development, implementation, and ongoing use of technology are properly designed and integrated enterprisewide to support the model.

3. **Data validation.** Is the model capturing accurate and complete information? Data errors or irregularities impair results and might lead to the organization’s failure to identify and respond to elevated risks.

4. **Process validation.** It’s important to verify that the design and ongoing sustainability of the model’s processes are resulting in output that is accurate, managed effectively, and subject to appropriate controls.

Model validation is often complex and resource-intensive. Testing is generally done by individuals who have not previously provided input on either the design or implementation of the model.

### 4. Model Tuning and Optimization

Tuning and optimization is the ongoing process of testing and enhancing the model. Model tuning is an important aspect of the development and implementation of a model as well as its ongoing management and sustainability. Following are the three primary elements of a comprehensive model-tuning program (exhibit 5):

1. **Gap analysis.** Gap analysis helps to ensure that all of the risks the bank faces are being monitored at an appropriate level. For example, gap testing might identify new products or services that are not accounted for within a model, or the testing might identify model assumptions that do not reflect current practices or market factors. To confirm that an organization’s risks and model objectives are being covered appropriately, the organization or third-party vendor must remediate any gaps or limitations identified during this analysis. Furthermore, the organization should put into place a process for periodically assessing gaps.
2. **Prescriptive methodology.** Optimizing models requires a consistent methodology founded in quantitative analysis. Prescriptive methodology is a formal documentation of the comprehensive approach the bank is using to optimize the model. The methodology must also define change-control procedures and the initiating events that require subsequent tuning. Examiners now call not only for the periodic assessment of model parameters but also for the definition of specific events – such as a change to an organization’s risk profile due to an acquisition – that warrant tuning.

3. **Documentary evidence.** Examiner and auditor expectations call for an audit trail of changes in the model’s parameters during the tuning process. Documentary evidence is used to demonstrate to regulators and auditors that the model is aligned to the prescriptive methodology for managing business activities and risks. Without supporting documentation, the prescriptive methodology might not stand up to a regulatory examination. The bank must maintain the documentary evidence for the life of the model.

**Exhibit 5: Refining and Optimizing Models**
5. Model Governance

All financial institutions that rely on models should implement an appropriate governance program. According to the guidance, “Even if model development, implementation, use, and validation are satisfactory, a weak governance function will reduce the effectiveness of overall model risk management.”

Exhibit 6: Governance Controls and Oversight for a Comprehensive Model Risk Management Program

Source: Crowe analysis
An organization’s governance policies, procedures, and processes should support controls and oversight to manage an effective and sustainable program. Models should be implemented from end to end, starting with the board of directors and senior management, who design and oversee operating models; and including the line-of-business managers, who are responsible for implementation; third-party vendors or IT specialists, who implement technology components; and compliance risk managers, who must manage the risk that is inherent in the model. Effective model governance requires the following elements:

- **Senior management and board involvement.** Senior management and the boards of directors must set the direction and oversee the policies of a model risk management framework. Models that are managed at the leadership level are more likely to be supported by well-thought-out policy and procedures as well as comprehensive methodologies that are executed consistently throughout the enterprise and managed through continuous improvements.

- **Policies and procedures.** At a minimum, the cornerstones of the guidance – development, implementation, and use; validation; and governance – must be addressed in formalized and enterprisewide policies. Implementing procedures should dictate the organization’s prescriptive methodology for managing the risks of models the institution relies on.

- **Roles and responsibilities.** Clear lines of reporting identify who owns model risk management processes and affirm the control structure that supports compliant procedures. When the bank lacks the knowledge to manage these functions, an individual should be responsible for augmenting the organization’s expertise in order to meet the bank’s model risk management standards.

- **Enterprise risk management and reporting.** Organizations with an enterprise risk management function should define the principal risks, events, or changes in the organization that could affect business processes. An effective model risk management framework promptly identifies such risks and assesses their potential impact on bank models. Clear lines of authority and reporting are required to oversee how a model's performance might change as a result of changes in the organization.

- **Independent audit and testing.** Auditing and self-testing effectively should challenge the model’s conceptual design, data reliability, and risk management controls. The role of auditing and self-testing is not to duplicate model risk management activities but rather to assess how effectively a model risk management framework meets business and regulatory needs.
6. Model Foundation

The model foundation is the final component critical to an effective model risk management program (see exhibit 1). A strong foundation provides structure, consistency, and efficiency to support program compliance. Following are the four elements of a robust model foundation:

1. **Business and regulatory alignment.** Regulators might deem a model risk management program ineffective if business needs are not aligned to regulatory standards. Misalignment could result in a bank’s failure to appropriately manage the risks inherent in models and thus lead to poor decision-making and even regulatory fines and penalties.

2. **Supporting documentation.** Detailed document management and retention are necessary for all areas of model risk management, including but not limited to policies and procedures, periodic model validation results, detailed tuning and optimization analysis, and model inventory and risk assessment.

3. **Enabling technology.** Technology helps executives to manage the breadth of requirements for an effective model risk management program. Financial institutions must define their approaches to using technology based on their size, regulatory standards, and the model risks they face. From simple spreadsheet maintenance systems to the purchase of an enterprisewide model risk management software solution from a third-party vendor, the way technology is used varies from institution to institution.

4. **Project management.** Various internal and external stakeholders and third-party vendors often come together to develop and implement models. Experienced project management personnel are critical to managing resources effectively and implementing models successfully.
Conclusion

Minimizing model risk in an era of mandated model risk management standards requires a financial institution to design, implement, test, and improve its models on an ongoing basis. The model risk management framework outlined here is designed to lead banks through the critical components of building an effective and compliant model risk management program.

Institutions that do not adopt a documented, consistent model risk management framework risk incurring regulatory actions, fines, and other penalties. All aspects of model risk management require banks to provide robust supporting documentation that demonstrates to regulators and auditors that their models are effective and aligned to business and regulatory needs. Using a project management structure overseen by senior management contributes to consistency in the organization and the integrity of its models.

Additional tools and strategies are available to help institutions with the daunting requirements of the guidance. Given the complexities of model risk management, many banks are turning to technologies available in the marketplace that can help them deploy a systematic and consistent approach to model risk management. Using technology also helps with the documentation, quantitative analysis, and tuning procedures that federal examiners have come to expect.
Contact Information

Brookton Behm is a principal with Crowe Horwath LLP in the Grand Rapids, Mich., office. He can be reached at 616.233.5566 or brookton.behm@crowehorwath.com.

John Epperson is with Crowe in the Oak Brook, Ill., office. He can be reached at 630.575.4220 or john.epperson@crowehorwath.com.

Arjun Kalra is with Crowe in the San Francisco office. He can be reached at 415.946.7449 or arjun.kalra@crowehorwath.com.

---