Deloitte.

Model risk management
A practical approach for
addressing common issues

Table of contents

An overview of model risk

Why model risk management is important

The insurance industry's focus on model risk management continues to gain momentum due to:
- evolving technological complexity and capability;
- heightened demands on models with regards to speed, granularity, and capacity;
- increased stakeholder expectations related to documentation, accountability, controls, and risk management.

Financial services companies have become more reliant on models in recent years for product pricing, GAAP and statutory valuation, risk and capital management, strategic planning, and other purposes. These various types of models have grown in magnitude and complexity due to innovative product designs, technological advances, regulatory requirements, and other internal and external forces. As a result, industry stakeholders appear to be at an inflection point with increased prioritization for model governance. Once companies realize the significance of their model risks, companies will be compelled to establish a new model risk management framework or improve an existing framework.

The United States financial services industry has made significant progress in model risk management since the 2008 crisis, including the introduction of regulatory changes such as SR 11-7[1] guidance, the ORSA Act[2], and the SIFI[3] designation applicable to the banking industry and some insurance companies.

However, much still needs to be done to make meaningful and mindful organizational changes that are sustainable and will provide stakeholders sufficient comfort that model risk is effectively managed within the organization. This article focuses on implementing a model risk management framework and how to overcome associated challenges.

Defining model risk

Model risk, according to SR 11-7 guidance on model risk management issued by the Federal Reserve and the Office of the Comptroller of the Currency, is defined as:
- Fundamental errors—A model produces inaccurate outputs when viewed against its design objective and intended uses.
- Incorrect use—A model's use is not aligned with its limitations and assumptions.

Such risks can arise in the following areas:
- Data—Inaccurate data leads to inaccurate model output.
- Assumptions—The model incorrectly applies assumptions, leading to spurious results.
- Methodology—An inappropriate conceptual framework leads to unrealistic results.
- Process—Processes are prone to human error, as well as calculation errors, both of which can add to model risk.
- Results/use—Inappropriate interpretation or use of results can affect decision making.

Regardless of the source, model risk can have profound financial and reputational implications and lead to costly errors or missed opportunities. Without adequate governance, models may significantly impair business decision making, as the following examples illustrate:
- Errors in hedging models may lead directly to inappropriate purchase or sell decisions, leading to unintended risk and realized losses.
- Misinterpretation of key financial metrics, which may influence management's decisions, could lead to negative impacts on policyholder benefits and sales force morale.

The primary impacts in the above examples, as well as secondary impacts, such as issues with the company's reputation and credit ratings, may more than offset the cost of implementing a sound model risk management framework.

Essential building blocks

Key building blocks for a sound model risk management framework are model governance, modeling standards, and model validation. Embedding this framework into an organization's culture is the final building block. In establishing these key building blocks, it is important to realize that not one size fits all, as each organization is different. A model risk management framework does not need to be overly complicated, and organizations should focus on core basic principles.

---

1. SR11-7 was issued by the Office of the Comptroller of the Currency (OCC) in 2011, which provides supervisory guidance on model risk management for the banking industry.

2. The Risk Management and Own Risk and Solvency Assessment (ORSA) Model Act (#505) was published by the National Association of Insurance Commissioners (NAIC) in 2014 and provides guidance to insurance companies on their internal assessments of their risk management processes.

3. Systematically Important Financial Institutions (SIFI) is a designation by the Financial Stability Oversight Council (FSOC) identifying that a bank or nonbank financial company's material financial distress (or the nature, scope, size, scale, concentration, interconnectedness, or mix of its activities) could pose a threat to U.S. financial stability.

Model governance

Establishing a model governance program provides the framework, oversight, and controls for modeling activities and managing model risk. Important features of such a program include model risk management policies and standards, modeling roles and oversight, controls, and documentation. The program should also institute processes and standards for key functions to identify and monitor model risk, including the definition of a model, a model inventory, model risk assessments, and model risk reporting.

It is essential that the model risk framework is supported by a variety of stakeholders across different functions. Roles, responsibilities, and accountability need to be clearly defined throughout a model's life cycle, including the processes for developing, implementing, maintaining, and using a model. Reporting lines and incentives need to be clear, with potential conflicts of interest identified and addressed.

Leading practices in model governance include:
- Consistently identifying models, owners, and associated use.
- Assessing model risk reflective of the complexities and dependencies within and across models.
- Implementing and maintaining a centralized model inventory, with tracking for the current validation status.

Key issue: Ignoring the end-to-end process and interaction between models

The use of individual models invariably presents model risk, the full scope of which is understood through examination of the end-to-end process—where each model fits and how it interacts with other models.

Recommendation: Process maps help to understand the scope of model risk and the interactions between models, data, and processes across the organization and represent best-practice model documentation. Models can have many uses, and understanding the organization's processes can help identify the interactions and risks between models.

Key issue: Overly complicated model definition

There are many types of models and many ways to define them, which often leads to overly complicated definitions. For example, a definition can become broad in an attempt to capture everything that might be a model, or it can be too technical by having too much focus on the calculation engine part of a model.

Recommendation: A simple definition, created through a scenario-based approach to thinking through how it applies to different situations, can lead to a more flexible framework that is effective for a variety of models. The key is to clearly explain why something is or is not a model and to apply the definition consistently across the organization.

Three lines of defense:

1. Ownership
   (model developers, users)
   – Manages day-to-day development and implementation of the company's models and is generally fulfilled by the model developers and line management.

2. Controls (risk management)
   – Coordinates and oversees the management and reporting of model risks within the first line of defense and establishes the minimum standards for managing model risk.

3. Compliance (internal audit)
   – Provides independent assessment of model risk framework and process effectiveness, as well as monitors and periodically evaluates the model risk management activities performed by the first and second lines of defense.

Modeling standards

Standards for developing, implementing, and using models help reduce model risk and allow companies to leverage industry best practices across the organization. For example, protocols for model development and change management, including appropriate testing, documentation, and communication, are key for limiting the risk associated with model development and maintenance. Model design and coding standards help maintain consistency of model structure and use across all modeling purposes and types, such as third-party and end-user systems.

Documentation of modeling activities and decisions is also essential. It should:
- Cover all aspects of the model life cycle and be sufficiently detailed so that the model can be independently validated.
- Be jointly owned by developers and model users.
- Be formally approved by all parties.

Model theory, development, implementation, use, and limitations should also be properly documented. The completeness, accuracy, and relevance of data should be assessed, as well as the appropriateness of assumptions and interdependencies used within the model. Reports should display clear interpretation of model inputs, assumptions, and outputs and explain limitations to ensure that senior management makes informed decisions.

Ongoing testing and questioning of the model should be promoted. Model tests should consider both expected and unexpected scenarios to conduct reasonability checks on the outputs of the model as well as to test the model's functionality when assumptions are changed. Model users should also participate in assessing ongoing performance and functionality of the model.

This practice provides feedback for the model development stage, thereby making model development an iterative process.

Key issue: Separation of duties and approvals

Adding greater formality to the model development process often requires more resources for proper separation of duties and approvals—a challenge for efficient and practical implementation.

Recommendation: A risk-based approach to model development and change management can provide effective governance for each model. Minimum standards, such as separate testers and model developers, can serve as a base level, with higher standards for higher risk models. Setting up a responsibility matrix or Responsible, Accountable, Consulted, Informed (RACI) chart for each model can also help resources understand and agree to their roles and required approvals.

Key issue: Formal yet practical documentation

In many companies, documentation is an unpopular task for model developers and users. Instead of addressing documentation broadly, people tend to focus on the technical aspects, and the quality of documentation tends to be measured by its length rather than the content.

Recommendation: As a foundation of effective model risk management, documentation should cover technical, operational, and control aspects of the model life cycle, as well as risk management activities. These aspects can be further broken down to include smaller elements, such as product features or methodology, which rarely change, and assumptions and controls, which must be more rigorously maintained.

In addition to understanding the types

of documentation needed for sound governance, it is also important to consider principles of effective documentation. Documentation should not be a one-time exercise that produces volumes of pages that sit unused or unreferenced until the next model validation. Instead, it should be built in layers across the modeling process, from requirements and design, to testing and implementation, with a focus on clarity and usability.

Key issue: Documentation buy-in

Because model documentation can be an extensive exercise requiring considerable time and resources, securing buy-in to the documentation process can be difficult, especially if an organization currently has minimal documentation and resource constraints.

Recommendation: The importance of and need for documentation should be clearly communicated to model developers and users, emphasizing the need for better understanding of models, knowledge sharing, and developmental evidence (i.e., documenting why modeling choices were made). This last point is crucial. It is not enough to document what has been done. There should also be a strong focus on why various decisions were made.

Creating efficiencies in the documentation process can also help with documentation buy-in. When establishing documentation needs, it is important to consider different uses of the documentation and how it can best meet the needs of various stakeholders. For example, instead of focusing technical documentation on model validation alone, a leading practice is to create documentation that can meet the needs of model developers, validation personnel, and control functions. Standard templates can also help users understand the documentation better, make the process more efficient, and create consistency across the organization.

Model validation

Model validation should provide an ongoing, effective challenge of a model, ensuring it continues to be suitable for its intended business purpose. It should include both quantitative and qualitative assessments and should be performed both prior to model implementation and periodically afterward. Model validations should be applied to both in-house and external vendor models and should span the model lifecycle. The concepts of independence, incentives, and influence should also be applied. The key elements of model validation include:

- Evaluation of conceptual soundness— This is the critical review of the model development process, including theoretical soundness, financial mathematics, consistency with industry practices, and market inputs and assumptions. Sensitivity analysis and stress testing are common methods used during this phase of validation.

- Ongoing monitoring—This is the assessment of the accuracy and completeness of data feeds and comparison of models to alternative information sources and models. It also should include analysis of overrides for potential model revisions.

- Outcomes analysis—This is the routine vcomparison of model outputs with actual outcomes, which should be carried out using a combination of quantitative and qualitative testing, parallel outcomes analysis, and back-testing. Results falling outside of predetermined thresholds indicate the potential need for model recalibration or redevelopment.

Key issue: Preparing models for validation

Once a model risk framework is set up, model validation is usually a primary focus, so it is important to prepare the models effectively. This includes having comprehensive documentation and change management processes in place, two important aspects that are often lacking.

Recommendation: Waiting for the modeling team to bring the models into compliance prior to model validation typically is not an option, because of time and resource constraints. This gap can be bridged by including the validation team in model development meetings and instituting a phased handoff approach, in which the development team hands off existing documentation to help the validation team get started, and then provides supplemental information while the validation is in progress. For example, the validation team can review model design documents as they are completed, prior to the model build, and then review the testing against the design once model building is complete. Attending the model development meetings can help shorten the validation team's learning curve so they understand the model even before receiving the documentation. Another effective practice is to conduct walkthroughs of the model functionality with the model validation team. These approaches require close coordination between the model development and validation teams. At the same time, it is important that the validation team avoids influencing the model development process, because that could impact their independence. For example, the validation team should offer opinions on the design of the model determined by the model development team rather than actually assisting the modeling team with model design.

Key issue: Ongoing validation

With the resources and time required to complete initial validations, ongoing validations often are given less attention.

Recommendation: After the initial validation, there should be a focus on model change management, with an overall schedule for revalidation of the full model. The validation team should confirm that simplifications to the model still make sense, validate changes to the model, and ensure that there is no extension of the model beyond the originally validated intended use.

Embedding a model risk culture

Given the significant potential impact that model errors can have on financial results, it is crucial for senior management to instill a strong risk culture within the company, supported by a sound model risk management framework. A leading practice approach for effectively managing key risks is a "three lines of defense" structure consisting of ownership, controls, and compliance. The three lines of defense framework provides a systematic approach to communicating model risk management and controls by clarifying essential roles and responsibilities.

While an understanding of the core components of model risk is important, the implementation of a model risk framework and changing the underlying culture are equally crucial. The goal of the three lines of defense framework should be to provide an effective structure for management and communication of modeling activities and model risk, while promoting greater understanding of model uses and their impacts. This approach can facilitate changing the governance mindset and embedding model risk management into the culture of the organization.

Key issue: Compliance vs. culture
When setting up a model risk framework, there is typically a strong focus on what rules need to be followed, with very prescriptive policies and standards. Understanding what needs to be done is important, but there is a risk of the program being so rules based that true change in the culture of the organization regarding how models are developed, implemented, and used is sacrificed.

Recommendation: A key objective should be to embed model governance culture within the organization. Rather than just focusing on compliance, the framework should provide guidance, standardization, and clear communication channels,

characteristics that can lead to long-term, improved efficiency in model development activities with enhanced governance.

For sustainability of model governance, there should be a focus on partnering with model developers and users to teach and increase awareness of model governance benefits and best practices. In this way, the goal of risk management becomes part of the process, rather than being purely an oversight function.

Key issue: Too much focus on one area
The guidance provided by SR 11-7 emphasizes the importance of expanding a company's focus beyond model validation to include model governance and standards for model development, implementation, and use. However, organizations still tend to focus too heavily on model validation.

Recommendation: A comprehensive framework should integrate and balance all aspects of model risk management, with each component working in tandem with the others.

Key issue: Working in silos
Model governance tends to be a newer part of enterprise risk management focus, so there can be a disconnect between the model risk management team, which is focused on setting up model risk management initiatives, and other enterprise risk management functions. Working in such a silo, the team can miss opportunities to leverage more established control functions and leading practices.

Recommendation: The model risk management team should interact with and leverage existing control functions, such as operational risk, to reduce redundancy, aid efficiency, and avoid overlap with existing controls standards.

Helpful hints for successful implementation– Communication, communication, communication:
Ongoing communication and easy-to-access information is critical for understanding and culture change. Some best practices include:

- Set up a central repository of information, including templates and guidelines (make it easy to find information)

- Send monthly emails to model owners with status updates, upcoming deliverables, and tips

- Hold lunch & learns and other learning/training events (ongoing training is critical for understanding and culture change)

- Hold forums for model developers and users to discuss experiences and best practices

- Adapt communication for different audiences (e.g., model developers vs. users will be interested in and need to know different information)

Key issue: Focus only on quantitative resources

Teams tasked with creating a model risk function often focus too much on quantitative skill sets and resources. This can be detrimental to effective program function by under emphasizing the governance and process aspects necessary for a balanced and effective program.

Recommendation: A mix of quantitative and qualitative skills, such as process, controls, and project management, is most effective for a model risk function, providing support beyond a pure technical focus, and also for project management and administration. Process-focused personnel should have basic understanding of models or some technical skills.

Key issue: Building around system tools

Managing model risk is a complex and interconnected process. An effective model governance program includes tools that support processes, workflows, inventory, documentation, and oversight. However, building the program to fit the tools can create operational challenges and inefficiencies.

Recommendation: It is important to first determine what requirements the organization has and what processes will best address those needs. For example, having a spreadsheet-based model inventory and risk assessment may not be ideal, but it might allow for greater initial flexibility in determining what information is needed. Over time, that information can be used to identify requirements for a more robust tool. Another important consideration is user experience. If an inventory or workflow tool is difficult to use, it can impede culture change and adoption of the new model risk framework.

One size does not fit all

A model risk framework has many components and complexities, so there is no one-size-fits-all approach to deciding which aspects are the most important for meeting near- and long-term goals. The core components of the framework are the same, but the robustness, standardization, and resources used to implement those components will vary based on each organization's needs. It is important for organizations to right-size their framework based on their unique needs.

A good starting point is to develop an understanding of leading practices for processes, controls, and documentation, and then to balance those practices against specific business needs to determine what level of maturity is desirable and achievable. The gold standard in all components of the framework is not necessarily the right answer for every organization. Organizations should evaluate their desired level of model risk management against model uses, risks, overall model risk appetite (i.e., what level and types of model risk an organization is willing to accept), and other factors such as overall business operations, growth plans, accounting bases, regulatory oversight, and rating agency expectations.

Once the organization has determined the appropriate level of model risk management, a gap analysis can help identify an appropriate path to the desired future state and prioritize efforts necessary to get there. To prioritize model risk management transformation initiatives, several complex and sometimes competing objectives will have to be balanced. Such balance can be achieved through a common vision and a transition plan.

Key issue: Trying to do too much too soon

Because effective model risk management can be a complex undertaking, starting with a complex process and attempting to implement too many best practices at once can be overwhelming.

Recommendation: Focusing on basics can help create a solid foundation, upon which more advanced capabilities can be built. For example, governance cannot just be turned on. Model risk management implementation often requires a transition plan such that governance standards and protocols can be adjusted to fit today's underlying people, processes, and technology while preparing for the actions that will move various aspects of the operating model toward the desired future-state vision.

Back to basics is an effective approach

Model governance activities have expanded over the past few years, and many organizations are in the process of developing new approaches to model risk management. There is no "quick fix" for this. Several hurdles still exist, including resource constraints, company cultural barriers, organizational structure, and modeling systems.

Programs built on the core principles of model risk management can help to position developers and users for success. At its most basic, model risk management is about continuing to question and understand models. Developers and users should know how models work and understand signs of when they do not work. They should know who is using the models and for what purpose. Instead of overly emphasizing prescriptive rules and focusing too much on compliance, developers and users will benefit from understanding the basic principles of model risk management. Holistic model governance program can accomplish that by establishing the framework and support necessary to meet today's model governance best practices while creating a sustainable method for ongoing management of model risk.

Contacts

Eric Clapprood, CERA, FSA
Principal
Deloitte Consulting LLP
+1 860 725 3473
eclapprood@deloitte.com

Corey Carriker, FSA, MAAA
Senior Manager
Deloitte Consulting LLP
+1 612 397 4376
ccarriker@deloitte.com

Maria Itteilag
Senior Manager
Deloitte Consulting LLP
+ 1 860 725 3228
mitteilag@deloitte.com

Deloitte.