Article from

The Modeling Platform

December 2016
Issue 106

Model Risk Management: An Overview

By Michele Bourdeau

Model risk management (MRM) has become an area of increased focus in recent years for banks, both from a good risk management practice perspective and because of enhanced regulatory guidelines and scrutiny. Insurance companies are slowly catching up, as their models and businesses have become gradually more complex. In addition, regulatory pressure is driving insurers to reconsider and enhance their processes around the use of models. Examples of models used for supporting the decision-making process include asset liability management (ALM), stress testing, investments pricing, planning and capital adequacy models.

This article gives an introduction to model risk and sound model risk management processes and controls. It starts with providing a definition of a model and what models are used for. It goes on to describe the various sources of model risk and why one should be concerned. The controls appropriate around the use of models—the model risk governance process—are then detailed.

WHAT IS A MODEL AND WHAT ARE MODELS USED FOR?

What models should be considered for a robust model risk management process? Let's start with a definition of a model. According to U.S. federal bank regulators,[1,2] a model is "a quantitative method, system or approach that applies statistical, economic, financial or mathematical theories, techniques and assumptions to process input data into quantitative estimates."

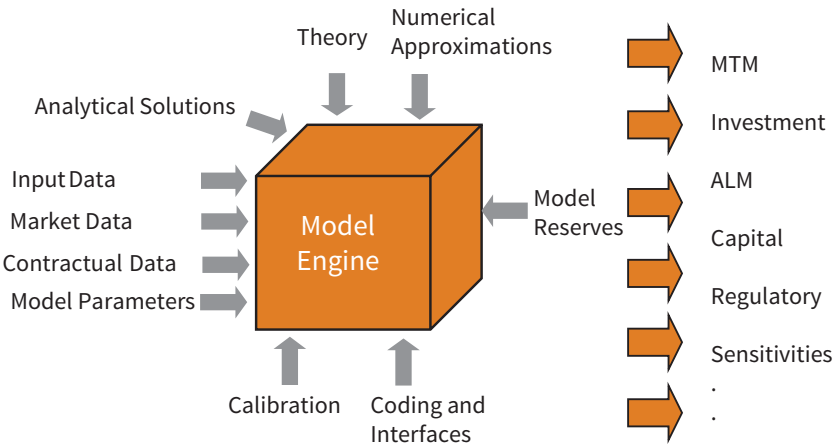
A model has three components: model inputs that include the assumptions and data that go into a model, a processing component that transforms inputs into estimates, and model outputs that transform estimates into useful business information, including any reporting component.

Model inputs include data that itself may originate from another model, and model parameters, such as volatility or interest rates. The processing component includes the model design and theoretical assumptions behind it, analytical or numerical methods and approximations used, the coding and interfaces, and the calibration of the model. Examples of model outputs can be a mark-to-market (MTM) value, a capital calculation, the price of a bond (for an investment decision), and sensitivities and stress-testing analysis results. Reports based on model outputs are used for informing decisions based on the model.

Figure 1 can help to visualize a model.

Models may be used for informing business decisions, measuring risks, valuing exposures (MTM), conducting stress testing, measuring compliance with internal limits, assessing adequacy of capital (ALM), managing client assets, meeting financial or regulatory reporting requirements and issuing public disclosures. Models are used in many areas of an organization, such as finance, securities or assets pricing, risk management, actuarial, asset or investment management, and for the management of client's assets.

Figure 1
What Is a Model?



A good model is a trade-off between replicating the business or market exactly and over modeling. Models should be developed such that they capture the most important aspects of a particular business. Models should be easy to calibrate and use. Models may need to be fast to operate if used for rapid decision-making. Model results should be easy to interpret and understandable by every user through model reports.

WHAT IS MODEL RISK, WHAT ARE ITS SOURCES AND WHY SHOULD WE BE WORRIED?

All three components of a model (input, engine and output) can be sources of model risk. Examples that lead to model risk can be errors in model methodology, errors in model implementation, models not used for their intended

purpose, model outputs being misinterpreted, model errors feeding into downstream systems, obsolete models, new complex products for which the model risks are not understood and models used in illiquid markets.

In addition, there could be a breakdown in the model control culture and processes.

Model risk is the loss resulting from misspecified, misapplied or wrongly implemented models. One could argue that all models are wrong by design because they are simplifications of reality. Model risk could arise from incorrect estimates of risks, leading to incorrect business and management decisions. Model risk could also give rise to reputational risk.

MODEL RISK GOVERNANCE

Model risk management should be approached as a multidisciplinary subject, and the responsibilities and standards for the three lines of defense need to be clearly defined and established, usually through a model risk management policy and standard operation procedures. The three lines of defense normally consist of the first line of defense or the line of business (LOB) model owners, the second line or risk management (including model risk management) and the third line or internal audit. Good communication between all relevant parties is essential. It is also essential to ensure a robust model control framework with clear audit trails evidencing all aspects of the framework. In practice, controlling model risks involves a trade-off between the level of model risk and the necessary costs of controlling the risk.

Models are subject to a model lifecycle that entails:

- All models are captured in a model inventory.
- All models are documented in detail, including their design, assumptions, limitations and the testing performed.
- Models can be tiered and the controls prioritized according to their perceived inherent risk.
- Models should be regularly subject to testing and validation (review by the LOB and/or independent validation).
- Model controls, including information technology controls, should be in place.
- Change management processes should be defined for material model changes.
- Ongoing performance monitoring of the outputs should be established.

Audit has responsibility for due diligence around these processes.

Line of Business

The first line of defense responsibilities is the line of business.

Model Development and Testing

LOBs are responsible for model development. As such, they need to define the model's purpose, develop the model's design (including the assumptions that go into the model and the model's methodology, including analytical, numerical or other tools used), write the code and/or customize a third-party vendor model. The LOBs need to implement the model, covering model inputs, coding and outputs, and make sure all components of the model work and interact smoothly and correctly with each other. The model then needs to be calibrated and tested to make sure it works as expected. This can cover sensitivity analysis, benchmarking to other models and stress testing. All aspects of the model also need to be documented and business continuity provisions put into place.

Model Documentation

Documentation of the design and operational details of the model is required to ensure business continuity and transparency of models used. Granularity of documentation takes into account the level of management or key function at which it is intended to be used. Documentation should be sufficiently detailed and complete to enable a third party to form a sound judgment on the suitability of the model for the intended purpose. The theory, assumptions, methodologies, software and empirical bases should be explained, as well as the data used in developing and implementing the model. Relevant testing and ongoing performance testing need to be documented. Key model limitations and overrides need to be pointed out so that stakeholders understand the circumstances under which the model does not work effectively. End-user documentation should be provided and key reports using the model results described. Major changes to the model need to be shared in a timely manner and documented, and IT controls should be in place, such as a record of versions, change control and access to model. Third-party vendor documentation should be subject to similar requirements, with the understanding that the methodology may not be accessible and testing is performed using sensitivity and stress-testing analysis (inputs/outputs).

Change Management

The LOB needs to establish and document processes around model releases and model change management (as an example, regression testing when a model is being changed or released). The model documentation needs to be updated to reflect major changes. In addition, clear controls around access to input data and access to code/spreadsheet or vendor where model resides need to be established.

Ongoing Performance Monitoring

LOBs need to establish a process for ongoing testing and evaluation of the model performance to make sure the model con-

tinues to work in its current operating environment. Higher risk models and those used most frequently are expected to be tested more often. Models are also expected to evolve and improve with time.

Risk Management

The second line of defense responsibilities is risk management.

Model Risk Management Policy

The second line usually establishes, with input from the first and third lines, the MRM policy and the standard operating procedures for implementing the MRM framework. Roles and responsibilities around each component of the model lifecycle need to be clearly defined and articulated.

Independent Model Validation

Model validation is typically a second line of defense activity. It can, however, be performed by the first line with oversight from the second line (peer review). In fact, among the actuarial community, there is a strong culture of model peer review. The model controls currently in place are of varying strengths and would need to be formalized and expanded to satisfy enhanced regulatory and risk management requirements. Model validation serves as an independent check on the models and controls put in place by the first line. Validation and testing activities need to take place when the model is first developed, when any significant changes to the model are made, or when the operational environment changes; for example, if the model needs to be applied to a new business or product. Validation of a particular model should be updated on a periodic basis depending on the level of changes to the model or the environment in which it operates.

Validation activities should be prioritized. Models deemed to be more risky to the organization should ideally be tested and validated more often. Model riskiness can be defined based on the complexity (quantitative or operational) of the model, the reliance on the model outputs or the financial or reputational impact of a model error. Validation activities are primarily there to assess whether the model is fit for its intended purpose and whether the first line has performed its due diligence. As such, all components of the model need to be examined, including the assumptions, inputs, data quality used, implementation and model limitations. Validation activities will depend on the nature of the model but can include sensitivity and stress-testing analysis, individual cell testing, code or spreadsheet review, reimplementation using an alternate model or benchmarking to other models, and a review of the controls around the model. Third-party vendor models are expected to be subject to the same type of scrutiny, understanding that the exact methodology and implementation are not accessible to the user and that sensitivity analysis, stress testing and benchmarking are the preferred methods for assessing the model.

The validation should be documented in detail, particularly for the higher risk models. Documentation can include a summary of the model and its assumptions, a review and assessment of the testing performed by the first line, as well as additional testing performed by the second line and evaluations on other aspects of the model such as model limitations, overrides and model reports. An overall assessment of whether the model is fit for its purpose should be included in the report.

Independent validations can results in findings. These need to be confirmed and their materiality established with input from the LOBs and other stakeholders. Material findings would need to be addressed in a relatively short time. Remediation timelines need to be set. Remediation may include redeveloping parts of the model, addressing missing documentation and adding controls around model use; for example, limiting the model use in certain conditions.

Internal Audit

The third line of defense is internal audit.

Audit's Role

Audit is responsible for the oversight over all aspects of the model control process, including the model inventory, model testing and validation, change management, and the responses and timelines of the LOBs to findings resulting from the validation of the model. As part of their review of the first and second line, audit may perform targeted reviews of model inventory, testing, validation and controls.

SUMMARY

A robust model risk management framework is good practice. Roles and responsibilities need to be clearly established around the use of models. This article presents some guidance and foundations for developing an effective model risk framework. ■

Michele Bourdeau is a managing director and head of model risk management at TIAA, where she was hired to create and implement the model risk management function. She can be reached at *mbourdeau008@gmail.com.*

ENDNOTES

1 Board of Governors of the Federal Reserve System and Office of the Comptroller of the Currency, "Guidance on Model Risk Management," SR 11-7, April 4, 2011, *https://www.federalreserve.gov/bankinforeg/srletters/sr1107.htm.*

2 Ibid., "Supervisory Guidance on Model Risk Management," SR 11-7 attachment, April 4, 2011, *https://www.federalreserve.gov/bankinforeg/srletters/sr1107a1.pdf.*