MODEL RISK MANAGEMENT BEST PRACTICES, WITH A SUBSTANTIAL FOCUS ON DEFINTION, GOVERNANCE BEST PRACTICES, AND AN EMPHASIS ON MODEL VALIDATIONS

By Kaitlyn E. Gasper, CAMS, CFE, Vice President, Principal, Risk Advisory, S.R. Snodgrass, P.C.

1. INTRODUCTION

According to supervisory guidelines, models refer 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." While models with less complexity have been used for several years, as the banking industry has moved forward over the past 20 years or so, it has become increasingly complex, and models have become more prevalent for managing risk, operational efficiency, and for key financial estimates. Our goal is to address how to identify the models currently utilized by your institution, establishing a framework for managing model-related risks, and the importance of an effective validation program.

2. MODEL INVENTORY

In order to properly manage model risk, management must ensure all models currently used by the Bank are identified, assess their risk to the institution, and apply appropriate mitigation procedures, including governance, training, succession, and model validation. When identifying models utilized by the institution, all areas of the Bank must be considered, including Bank Secrecy Act/Anti-Money Laundering (BSA/AML), Asset Liability Management/Interest Rate Risk (ALM/IRR), Current Expected Credit Losses (CECL), and Automated Valuation Models (AVM), among others. As the types of models used are so diverse, it can be difficult to ensure all models are properly identified. After identifying each model, assessing them for their risk to the institution is a key measure to make sure the model owner(s) have the requisite knowledge and experience to operate the model, training is up to date, the model has been validated when applicable, and known issues or limitations are resolved. We frequently see institutions manage each model within their own silo with inconsistent application of risk mitigation procedures. As a result, the identification of the need for additional training, validation, etc. are the result of comments from regulatory examinations. Management should make sure to be proactive in this area as models become more relied upon within more aspects of the institution.

3. GOVERNANCE AND POLICY

As with all key management functions, governance is a critical aspect of model risk management as it establishes an effective environment for models to be managed. Making sure there are key lines of authority from model users/owners to senior management to the Board of Directors will allow for effective and timely reporting of problems or complications. Institutions can consider the need to identify a risk officer, or similar, position and/or risk committee to ensure models are discussed and inventoried. Adopting a model risk management policy should also be a priority for the Board and management, identifying roles and responsibilities, validation/testing expectations for each model, vendor management for any third-party

involvement, reporting procedures, and expectations for the resolution of any issues identified. It should provide guidance and acceptable procedures for management to make sure risk management procedures are consistent with the tolerance established by the Board of Directors. The Bank should also ensure internal audit's involvement in assessing whether or not those charged with the day-to-day aspects of the model risk management policy are adhering to those requirements, including retention of all supporting documentation of testing the model, accurate reporting to senior management and the Board, timely clearing of any significant validation findings, and adherence to vendor management requirements. Without an effective policy, we frequently see that management of each model is, at best, inconsistent; however, we generally see that a majority of models in use are not considered part of the overall risk management framework.

4. IMPORTANCE OF A MODEL VALIDATION

Model validations are an integral part of model risk management. Model validations should be performed when reasonable after implementation. There are certain aspects of the model that can be validated soon after implementation, which include mapping, parameters, rules, etc. On the other hand, there are aspects of the model that cannot be validated until sufficient data has been input and run through the model such as backtesting, alert generation, etc.

Institutions should focus on two types of model validations: (1) third-party model validation and (2) a validation of the institution's specific usage of the model. A third-party model validation should be obtained and reviewed when performing due diligence in model selection and then annually or as completed thereafter. The institution is not responsible for contracting this type of validation but, rather, it is the model provider's responsibility to hire a third party to validate the software. The results of this validation should be available to model users to ensure they are aware of any model capabilities not functioning properly or identification of any known limitations. Depending on the type of model, a model certificate may also be available, which certifies the model functionality to process and provide necessary outputs. This should not take the place of model validation but provides a determination on whether the technical aspect of the model is functioning properly.

The second type of model validation that should be performed validates the institution's specific use of the model. It is the responsibility of the institution to contract a third party or independent individual to complete validations on a periodic basis. The current guidance does not explicitly state the frequency of which validations are to be performed, except to say that validations should be performed periodically considering the complexity of the model and the institution's risk profile. We typically see validations performed annually for complex, higher risk institutions every three and years for less complex institutions. If significant updates or changes are made to the model, this should trigger whether a model validation is necessary on a more frequent basis. The model validation should focus on the model capabilities in use to determine whether the necessary information is input to produce the expected outputs. Typically, this validation would not include verification of mathematical accuracy, algorithms, or any other proprietary information. Both types of validations mentioned are equally important and validate

the model from the vendor and user perspective. It is imperative that management integrate model validations into their model risk management.

5. WHAT TO EXPECT DURING A MODEL VALIDATION

The primary source for formal regulatory guidance on model governance issued is the *Supervisory Guidance on Model Risk Management* in 2011 by the Office of the Comptroller of the Currency (OCC) jointly with the Board of Governors of the Federal Reserve, later adopted by the Federal Deposit Insurance Corporation in 2017. Model validations should focus on three major components: information input, processing, and model outcomes.

- The information input component: how data is delivered to the model
- The processing component: transformation of data for monitoring
- The model outcomes component: translate data into results, reports, alerts, and useful information.

The validation process varies depending on the specifics of the model and model type. The validation section of the guidance referenced above should be followed for each model type; however, the data analyzed, objectives, usage of the model results, etc. will vary for BSA/AML, ALM/IRR, and CECL models.

Assuming issues are not identified in the third-party model validation completed for the model provider or during vendor management reviews, the validation will focus on the information controlled by the institution, quality of data, controls over data, manual manipulation, assumptions, estimates made by management, parameters, etc. We frequently identify issues specific to the information input component when completing model validations. It is a best practice to understand how information is mapped from source systems to the model at implementation. Another best practice relates to default settings or parameters. Typically, model providers will activate default settings based on information they have gathered from peers or other data available. It is important that management review any defaults and either accept with an explanation to support why those fit their risk profile or adjust with an explanation to support why the change was made.

The results of the validation should be remediated timely to maximize model use in managing risk. The key takeaway from this should be that model validations are important when relying on them as a tool to manage risk.

Kaitlyn E. Gasper, CAMS, CFE, Vice President, Principal, Risk Advisory at S.R. Snodgrass, brings extensive experience working with financial institutions, including exceptional expertise with BSA (Bank Secrecy Act) Model Validations. She also works closely with both public and privately held corporations, nonprofit organizations, partnerships, limited liability corporations, and S corporations.

About S. R. Snodgrass

Founded in 1946, S.R. Snodgrass is a privately held, multi-faceted public accounting and consulting firm, known for innovative tax, assurance, technology, and financial advisory services for financial institutions, nonprofits, and businesses of all kinds. The firm has worked with more than 175 financial institutions in 16 states and employs more than 90 professionals. The firm is ranked among the country's top 300 public accounting firms according to Inside Public Accounting's 2024 list.

References:

Guidance on Model Risk Management. (2011) *Board of Governors of the Federal Reserve System.*

https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf