Understanding Requirements for Model Validations
By James Jarrett, Director, Baker Tilly Virchow Krause, LLP

With the use of models becoming more frequent among financial institutions, federal examiners are pressuring institutions to perform validations on all of the models being utilized. The common models being used include Bank Secrecy Act/Anti-Money Laundering, Interest Rate Risk/Asset Liability Management and Allowance for Loan and Lease Loss (ALLL).

Management and individuals involved in modelling at financial institutions need to understand the applicable regulatory requirements per current bulletins, key elements to review for each type of model validation – including frequency of completion – and best practices for reporting the results.

REGULATORY REQUIREMENTS
The Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC) and the Federal Reserve Bank (FRB) have all issued specific guidance on the use of business models. The items below provide some history for regulatory guidance on model validations:

- **December 2005**
  - The FDIC provided “unofficial” supervisory insights on model governance.
- **January 2010**
  - The National Credit Union Association (NCUA) issued an advisory on Interest Rate Risk Management to include generic model validation guidance.
- **June 2017**
  - The OCC (2001-12) and the FRB (SR 11-7) issued joint guidance describing the key elements of model risk management. The FDIC and NCUA were not part of the joint issuance of the guidance in April 2011.
  - The FDIC issued FIL 22-2017 officially adopting the guidance issued by the OCC and FRB in 2011 with technical conforming changes.

Model Risk Management
The use of a model does not reduce risk to zero. Model risk is 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 an institution’s reputation. Model risk should be managed like all other risks and be part of the annual risk assessment process.

Regulatory guidance outlines a principle for managing model risk called “effective challenge,” which is defined as critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate changes.

In its basic form, a model consists of three components:

1. **Information input component** – delivers assumptions and data to the model
2. **Processing component** – transforms inputs into estimates
3. **Reporting component** – translates the estimates into useful business information

Each of these three components should be included as part of the model validation process to help ensure there are no areas of weakness that would increase the overall model risk.

Model Risk Management Framework
An effective model risk management framework should include:

- Disciplined and knowledgeable development that is well documented and conceptually sound
- Controls to ensure proper implementation
- Processes to ensure correct and appropriate use
- Effective validation processes
- Strong governance, policies and controls
- Use of vendor and other third-party models should be incorporated into the model risk management framework
These points outline that the use of a model begins prior to implementation, a documentation roadmap is essential and the process does not end with implementation. Additionally, the last bullet point states that even third-party models are subject to the other bullet points.

There are three key elements to model risk management:

**Model development, implementation and use**  
The development and implementation should be completed by knowledgeable, experienced people within the institution or third-party vendors. The "use" should confirm that the model is being used as intended.

**Model validation process**  
See next section

**Governance**  
This sets an effective framework with defined roles and responsibilities for clear communication of model limitations and assumptions, as well as the authority to restrict model usage.

**MODEL VALIDATION**  
Model validation is specifically detailed in the regulatory guidance – it is the set of processes and activities intended to verify models are performing as expected. Additionally, model validations identify potential limitations and assumptions and require the need to determine the impact. Model validations should be completed by staff with the appropriate knowledge and experience of the model subject matter.

The three components (input, process and reporting) should be subject to validation. This applies to in-house developed models, as well as those purchased from a vendor. The amount of testing required will depend on how the model is used and the amount of control the institution has within the model. In some models (e.g., Interest Rate Risk), the institution may supply the third-party vendor the input information and assumptions to be input into the model. In these cases, the institution does not have direct access to the model calculations and scenarios. In comparison, a BSA/AML model and an ALLL model are usually purchased software that is implemented on the institution’s information technology domain. The institution will have direct access to the software, including the ability to edit assumptions and alerts and to tailor the model to its products, services and operations.

Model validations should be completed by staff independent of those responsible for implementation, development and use. While staff completing the validation should have the knowledge, skills and expertise needed for that subject area, the concept of knowledge does not mean from an information technology standpoint. The person completing the validation should have knowledge of the purpose of the model. For example, when validating a BSA/AML model, the person completing the validation should have sufficient knowledge of the requirements of BSA/AML to be able to review transaction detail, alerts and suspicious activity.

It is always best to complete the model validation in a test environment. This would eliminate the potential negative impact on “actual” customer information in the event there are issues. Additionally, model validation is not a “one and done” process. The regulatory guidance states “Banks should conduct a periodic review – at least annually, but more frequently if warranted.” As these model validations are normally done by a third party, this is an additional annual cost institutions must consider.

**Components of a Model Validation**

- **Conceptual design**  
Evaluate the logic and design of the model.

  The model was designed in a way to achieve a certain objective; now the question is: Is the model designed in a way to do exactly that? Is there anything missing? Are all risks that the institution is exposed to taken into consideration? Does it include all products and services? Documentation is key in this component and ensuring the proper group is involved.

- **System validation**  
Validate the system to ensure that it is properly designed to perform.

  After ensuring that the conceptual design is adequate in mitigating risks, the system itself should be tested to ensure that it reflects the same. For example, testing the output and effectiveness of the generated alerts to drive further tuning of the thresholds and scenarios. In many cases, institutions should run the model parallel to the existing process for several months to validate the results. During the validation process, this parallel testing should be reviewed.

  During system validation, it is essential to ensure systems, products, services and transactions are considered and flow to the model. For example, the implementation of the BSA/AML model would need to ensure all products, services, systems are considered. Not all products (e.g., Trust) are contained on the core processing system. The model validation should verify that all systems are properly mapped to the model software.
Data validation

Validate that accurate and complete information is captured by a system to execute the model.

A system can be designed and implemented to achieve its objective, but end up failing badly due to data integrity issues. If the input data is not reliable, the output would not be in a position to give any value. This part will require identifying source systems and transaction codes, ensuring accurate data feeds. This piece of the validation is critical as the results of the data drive the results of the model and the reporting. During this phase of the validation, information is traced from the originating system to the model to verify all of the key data is captured. This would include any assumptions within the model. The basic concept here is “garbage in, garbage out.”

Process validation

This phase includes an evaluation of controls, the reconciliation of source data systems with model inputs, and the usefulness and accuracy of model outputs and reporting.

During this phase, it is verified that everything from the core system (source data) was captured by the model. For an IRR model, this involves a review of the data sent to a third party and the output reports compiled by the third party to ensure the information is part of the model.

Model Risk and Deficiencies

Several factors can influence the outcome of the validation and whether it performs as it should. The most common issues affecting the effectiveness and accuracy of the models include:

- Exclusion of customers, products and services
- System data is inaccurate, incomplete or irrelevant to the model purpose or design
- Data mapping errors/irregularities, file load errors
- Design of rules and/or configurations inconsistent with regulatory expectations and the institution’s risk exposures
- Logic errors which produce inaccurate output
- Lack of change management and/or adaptation to changes in organization activities that affect model performance
- Lack of resources and expertise to effectively manage model risk management activities
- Unclear lines of authority or accountability

REPORTING THE RESULTS

While a model validation is not technically an audit, a formal report should be written or issued if a third party has been contracted to complete a model validation. The reports should be issued to management responsible for the model. Additionally, consider presenting the report to the audit committee or board of directors of the institution. The information can help inform them on various components of the institution’s operations and strategies.

The following items should be included in the report:

- The scope of the model validation
- The date the validation was completed
- Which regulatory compliance requirements the validation was conducted under (e.g., OCC, FRB or FDIC)
- Detailed procedures completed during the validations
- Detailed recommendations for improvements and corrective action to be taken by management
- An overall rating (e.g., satisfactory, needs improvement, unsatisfactory) as to the effectiveness of the model

During the next regulatory review, the report and workpaper documentation should be provided to the examiners.

For those institutions that are subject to validation requirements, following the rules and timing requirements are a must, but all financial institutions using models within their organization would be wise to validate. As organizations understand the validation process more thoroughly, there are organizational and strategic opportunities to be gained.

Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of the Financial Managers Society.

About the Author

James Jarrett is a director in the corporate governance and risk management group of Baker Tilly Virchow Krause, LLP and has more than 25 years of audit, accounting, and regulatory compliance experience in the financial services industry.