

A PUBLIC POLICY PRACTICE NOTE

Model Risk Management

May 2019

Developed by the Model Risk Management Work Group of the
ERM/ORSA Committee of the American Academy of Actuaries



AMERICAN ACADEMY *of* ACTUARIES

Objective. Independent. Effective.™

A PUBLIC POLICY PRACTICE NOTE

Model Risk Management

May 2019

Developed by
the Model Risk Management Work Group
of the ERM/ORSA Committee
of the American Academy of Actuaries



AMERICAN ACADEMY *of* ACTUARIES

Objective. Independent. Effective.™

The American Academy of Actuaries is a 19,500-member professional association whose mission is to serve the public and the U.S. actuarial profession. For more than 50 years, the Academy has assisted public policymakers on all levels by providing leadership, objective expertise, and actuarial advice on risk and financial security issues. The Academy also sets qualification, practice, and professionalism standards for actuaries in the United States.

A PUBLIC POLICY PRACTICE NOTE
2018-19 Model Risk Management Work Group

Seong-min Eom, MAAA, FSA, PRM
Chairperson

Lesley Bosniack, MAAA, CERA, FCAS
Charles Ford, MAAA, FSA, CFA
Daniel Hui, MAAA, FSA, CERA, CFA
Malgorzata Jankowiak-Roslanowska, MAAA, ASA

Shiraz Jetha, MAAA, CERA, FSA
Joshua Liu, MAAA, FRM, FSA
Patricia Matson, MAAA, FSA
Gina O'Connell, MAAA, FSA
Jon Zeu Wu, MAAA, FSA, CERA

Special thanks to those who helped finalize the practice note: Maryellen J. Coggins, MAAA, FCAS, CERA and David E. Heppen, MAAA, FCAS.



AMERICAN ACADEMY *of* ACTUARIES

Objective. Independent. Effective.™

1850 M Street NW, Suite 300
Washington, DC 20036-5805

A PUBLIC POLICY PRACTICE NOTE

This practice note is not a promulgation of the Actuarial Standards Board, is not an actuarial standard of practice, is not binding on any actuary and is not a definitive statement as to what constitutes generally accepted practice in the area under discussion.

Events occurring subsequent to this publication of the practice note could make the practices described in this practice note irrelevant or obsolete.

This practice note was prepared by the Model Risk Management Work Group of the ERM/ORSA Committee of the American Academy of Actuaries. The practice note represents a description of some of the practices believed by the current subgroup to be employed by actuaries in the United States in 2018-19. It should be recognized that the information contained in the practice note discusses current and emerging practice, but is not a definitive statement as to what constitutes generally accepted practice in this area.

Comments and questions are welcome. Please send comments to:
RMFRCPolicyAnalyst@actuary.org.

A PUBLIC POLICY PRACTICE NOTE

Table of Contents

I. Executive Summary	6
II. Model Risk.....	7
1. Definition of Model	7
2. Definition of Model Risk	8
3. Practical aspects of model definition	8
4. Model Validation	9
III. Model Risk Management Practice	10
1. Model Risk Policy and Governance.....	10
2. Model Inventory.....	12
3. Model Documentation.....	14
4. Process and Control	14
5. Model Risk Scoring/Measurement.....	16
1) Scoring Model Risk - Model Risk Scorecard.....	17
2) Model Risk Quantification.....	17
6. Model Development and Implementation.....	18
7. Model Review/Validation	20
1) Model Owner’s Role.....	20
2) Model Validation	20
8. Performance Monitoring	22
9. Practical Aspects of Modeling	22
IV. Relevant Regulation.....	25
United States	25
Canada.....	25
United Kingdom.....	25
APPENDIX 1 Sample Model Validation Plan	26
Model Validation Plan Assumptions	26
Detailed Model Validation Plan.....	26

A PUBLIC POLICY PRACTICE NOTE

I. Executive Summary

This practice note discusses current model risk management practices within the insurance industry. Modeling and the associated governance and controls are becoming more and more important as the use of models for financial reporting and key strategic decision-making in companies increases rapidly.

Actuaries often use models to analyze uncertain outcomes. Even with prudent development and careful use of a model, uncertainty and variability could still exist. Actual experience can differ, sometimes significantly, from the estimates derived from the modeled results. A model is an approximation of reality, not the reality itself, therefore differences between the modeled results and actual experience may not indicate a flawed model or noncompliance with standards.

An important aspect of an actuary's work in modeling is an understanding of not only the technical aspects of building, updating, and using models, but also how they are governed, and what controls are necessary to mitigate the risk of errors in the models or the results.

Below is a summary of industry practices related to the management and mitigation of model risk.

A PUBLIC POLICY PRACTICE NOTE

II. Model Risk

1. Definition of Model

There are various definitions of a model depending on the purpose/use of the model within an organization or industry. Definitions can evolve within an organization or industry based on the development of the model or expansion of the model's use.

The current exposure draft of the proposed actuarial standard of practice for modeling¹ defines a model as:

“A simplified representation of relationships among real world variables, entities, or events using statistical, financial, economic, mathematical, or scientific concepts and equations. A model consists of three components: an information input component, which delivers assumptions, data, and sometimes parameters to the model; a processing component, which transforms input into output; and a results component, which translates the output into useful business information. Models are used to help explain a system, to study the effects of different parts of a system, to predict the behavior of a system, or to derive estimates and guide decisions.”

The U.S. Federal Reserve and Office of the Comptroller of the Currency (OCC)'s Supervisory Guidance on Model Risk Management (SR 11-7)², which primarily deals with banking organizations, defines a model as:

“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* consists of three components: an information input component, which delivers assumptions and data to the model; a processing component, which transforms inputs into estimates; and a reporting component, which translates the estimates into useful business information.”

¹ <http://www.actuarialstandardsboard.org/asops/modeling-fourth-exposure-draft/>.

² <https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm>.

A PUBLIC POLICY PRACTICE NOTE

2. Definition of Model Risk

Model risk can be understood as the loss (economic, reputational, etc.) arising from decisions based on flawed or misused models. Four basic sources of model risk are: (1) data limitations in terms of either or both availability and quality; (2) estimation uncertainty or methodological flaws in model design (volatility of estimators, simplifications, approximations, inappropriate assumptions, improper design, etc.); (3) calculation or coding error; and (4) inappropriate use of a model (use outside its intended purpose, lack of resources with knowledge to use properly, failure to update and recalibrate, etc.).

The risks of models can fit into Enterprise Risk Management (ERM) risk categories such as:

- (i) Specific risk categories (e.g., credit risk, insurance risk) due to inaccuracies in the estimation of metrics important to an organization such as capital, value of assets or liabilities, or income levels.
- (ii) Operational risk resulting from the development, implementation or improper use of models in decision-making (e.g., product pricing, evaluation of financial instruments, monitoring of risk limits, etc.)

3. Practical aspects of model definition

A model can be stand-alone or a part of a chain of models that receive or deliver inputs or outputs. When operating in conjunction with other models, it can be challenging to delineate where a model starts or stops within a process. For example, a model may have several statistical components used in the calibration of assumptions. Further calculations could use these assumptions to produce metrics which guide decision-making. Each statistical component could be defined as its own model with the aggregation step being yet another model. Alternatively, the entire sequence can be defined as a single model.

There are no hard and fast rules, and either model definition can be suitable for use. The model boundary is typically defined so that a model is specific enough to be coherent yet comprehensive enough to cover as much as is necessary. With a suitable definition of a model determined, an organization can establish appropriate model risk management policies and procedures.

In situations where there is no discretion in terms of the assumptions and methodologies employed, such as when a set of calculations is very simple and straightforward, these calculations may not fulfill the definition of a model. As a result, the computation may

A PUBLIC POLICY PRACTICE NOTE

be subject to review and validation outside of the scope where model governance dictates. In general, tools that do not fit the definition of a model can have validation checkpoints, but these would be outside of model governance.

4. Model Validation

For purposes of this paper, the term “validation” means all the various processes, reviews, and testing that need to be done to ultimately determine that a model is ready for use. For additional information, please see [Section III-7](#).

III. Model Risk Management Practice

Common elements of model risk management include:

- Model Risk Policy and Governance
- Model Inventory
- Model Documentation
- Model Process and Control
- Model Risk Scoring/Measurement
- Model Development and Implementation
- Model Review/Validation
- Performance Monitoring

1. Model Risk Policy and Governance

Consistent with their own perceptions of best practices, organizations formalize model risk management activities with policies and the procedures to implement them. Model risk management policies are generally commensurate with the organization's relative complexity, business activities, corporate culture, and overall organizational structure. The board of directors or its delegates typically approve model risk management policies and review them periodically to ensure consistent and appropriate practices across the organization. These policies are then updated as necessary to ensure that model risk management practices remain appropriate and keep current with changes in market conditions, products and strategies, exposures and activities, and practices in the industry. All aspects of model risk management are generally covered by such policies, usually including model and model risk definitions; roles and responsibilities of key stakeholders; assessment of model risk; acceptable practices for model development, implementation and use; appropriate model validation activities; and governance and controls over the model risk management process.

Policies often emphasize testing for robustness and promote targets for model accuracy, measures for acceptable levels of discrepancies, and procedures for reviewing and responding to unacceptable discrepancies. Policies typically include a description of the processes used to select and retain vendor models, including the people who are to be involved in such decisions.

The prioritization, scope, and frequency of validation activities are usually addressed in these model risk governance policies. Some organizations include a model classification or tiered system which is used to determine the level of thoroughness that will be used in the monitoring, validation, and documentation of models. The policies may establish standards for the extent of validation that needs to be performed before models are put

A PUBLIC POLICY PRACTICE NOTE

into production and the scope of ongoing validation. The policies may also document the requirements for validation of vendor models and third-party products. Finally, policies typically contain requirements for the maintenance of the model risk management framework, including:

- Inventory of models in use
- Detailed documentation on each model including its timely update
- Model controls and validation processes
- Uses of model results
- Model issues and their resolution

Detailed model documentation will allow the model to be replicated by a third party for the testing purpose or to be transferred to a new modeler without loss of knowledge.

Policies typically identify the roles and assign responsibilities within the model risk management framework with clear detail on staff expertise, authority, reporting lines, and continuity. Ownership is clearly delineated based on an organization’s risk management governance structure. The governance structure may follow the “three lines of defense” concept: model owners, model risk management, and internal audit. Controls outline the use of external resources for validation and compliance, and specify how that work will be integrated into the model risk management framework.

A summary of the potential responsibilities of the three lines of defense framework related to model risk management is as follows:

Role	Responsibility
First Line: Business Modelers	<ul style="list-style-type: none"> • Determination of model “fitness” • Development of model • Implementation of model • Assessment of model validity • Assessment of model risk • Maintenance of model controls • Monitoring model performance • Building/maintaining model documentation
Second Line: ERM, Risk Committee, Compliance	<ul style="list-style-type: none"> • Development/approval of policies and procedures for model risk management • Oversight of model governance • Maintenance of the model inventory • Affirmation of model risk assessment* • Affirmation of model validity/Independent model validation* • Affirmation of sufficiency of model documentation*

A PUBLIC POLICY PRACTICE NOTE

Third Line: Internal Audit	<ul style="list-style-type: none">• Test the effectiveness of first-line control: ensure model information contained in the model inventory is accurate and complete, perform testing to evidence model effectiveness, and maintain effective documentation.• Test the effectiveness of second-line control: effective implementation of model risk policy and procedure, maintain a well-functioning model inventory, provide effective challenges on models, and provide timely reporting to senior management on model risk.
----------------------------	--

** For models owned by ERM, an independent area may take responsibility*

2. Model Inventory

Model inventory is a summary of the organization's model information and model risk exposures, and it supports the assessment and mitigation of an organization's overall model risk. It is a comprehensive list not limited to the actuarial or financial departments, but encompasses all functions (marketing, operations, customer service, etc.). Building and maintaining the model inventory regularly can contribute to the effective management of model risk.

Depending on the organization's model risk management policies and procedures, the content of the model inventory can vary. Common content of inventories would typically include:

- Model name
- Description including the software or system in which the model is operated
- Version and latest update date
- Model owner and role within the organization
- Purpose of model
- Model use(s)
- Model limitations
- Status of model (e.g., in development, in production, etc.)
- Model complexity (typically a ranking based on defined criteria)
- Model materiality
- Model assessment date

A PUBLIC POLICY PRACTICE NOTE

Model inventories can also capture model validation date, validation status, validation person/department, model documentation status and document name, and interaction with other models or tools.

A component of developing a model inventory is to determine the information to be contained in an organization's model inventory along with the procedure for the collection of this information. Typically, model information is provided by the model owner because they have the best overall knowledge of a model. In practice, a model inventory team may supply a model information questionnaire or template to model owners for gathering the inventory data and necessary model details. This effort could involve coordinations across business units. An expansive effort across an organization can present challenges in applying the definition of a model in practice. Aggregating and reviewing model owner inventory input is typical to help ensure accuracy and consistency in the application of the model definition and representation of inventory details. The model inventory team is the likely candidate to ensure a centralized, comprehensive and consistent model inventory that is regularly refreshed.

Information typically included in the model inventory is the model's complexity and materiality. Model complexity and materiality can aid in measuring the significance of the model to the organization and the degree of potential model risk. Model complexity can be determined based on the data, assumption, and computational complexity. Assessment of materiality may take into consideration the purpose, use, and impact of the modeled results, and the materiality level could be determined based on the organization's risk threshold and limits. Complexity and materiality could be expressed in tiers (e.g., tier 1, 2, and 3 or low, medium and high).

A model inventory is a centralized listing (database) of significant models under an organization's management. To maintain independence between model owners and the model inventory owner, it is common for the model inventory to be maintained by a centralized function such as ERM department or any other relevant corporate function. For small companies, the model inventory may be maintained by the model owners collectively. In order to retain appropriate independence, review of the processes and controls for creation and maintenance of the model inventory can involve a review by the third line of defense (internal audit). For example, if ERM department is responsible for the model inventory, internal audit may periodically review the inventory and the associated processes and controls.

Depending on the organization's model risk management framework and governance structure, a model steward may be responsible for maintaining the model inventory. There may even be multiple model stewards for various types of models. A model steward could provide expert knowledge and recommend methodologies and approaches to managing model risks. Other roles of a model steward may include:

A PUBLIC POLICY PRACTICE NOTE

- Maintaining model risk management policies and procedures
- Maintaining and updating the status of each model (e.g., under development, implemented, retired)
- Tracking the version of each model
- Developing model test methodologies and managing the model testing and validation status and schedule
- Aligning model document quality and any templates
- Reviewing and updating the inventory

3. Model Documentation

Thorough documentation is a critical part of governing models and, more broadly, business processes. Documentation is essential for developing a complex model, using the model in a production environment, auditing the model and related processes, and handing off the model to successive owners. While a detailed study of model documentation is outside the scope of this paper, common practices include coverage of:

- Model owner as of a date
- Intended purpose and uses
- Version/last change date
- Summary of last validation and result
- Assumptions made in model construction
- Developer notes associated with any codes or calculation engine underlying the model
- Data sources and formats
- Parameter assumptions
- Dependencies on other models and processes
- Key outputs
- Applicable regulations and guidelines
- Limitations and future research areas
- Detailed step-by-step user instructions

4. Process and Control

Model process refers to the end-to-end steps performed related to the model, including model data and other inputs, model calculations, and model output. Model control refers

A PUBLIC POLICY PRACTICE NOTE

to the mechanism of maintaining integrity of the model as it is built and as users are changing or refining input data, making changes to calculations, and creating output through the production process.

Model input data, which either passes through or remains in its original state during the model process, is used to generate the end results based on the specifications for reporting or analysis. Controls on the input data typically include controls on the completeness and accuracy of data.

Change control for system upgrades and coding additions may also be required as part of the model process due to newer versions released from a third-party vendor or new product implementation or other features occurring in the business being modeled. Change control is a formal documentation and sign-off process that describes the nature of the change and quantifies its business impact. In addition, if the model is substantially changed a partial validation or full validation may be necessary.

Controls on the model production process are helpful to reduce variability and ensure reliability. Process control is a key component of model risk management. It can lower variability and ensure consistently high-quality results. Process controls are maintained at a target level to maximize efficiency as well as to ensure reliable results.

Model process controls can be grouped into data integrity, model validation, and projection dynamics. Data integrity plays a vital role in model risk management. It could involve input validation and data reconciliation, and provides a sense of comfort to a modeler when reconciling actual data to model data at the beginning of the modeling process.

Model validation requires a validator to have the sophisticated skills and technical background necessary to operate a model. Model validation can involve review of model inputs and intended use, checking of model mechanics, parallel or back-testing, ongoing performance monitoring, and confirmation that the model is appropriate for its intended use. Checking of model mechanics could be performed by independently replicating all or part of a model from scratch or reviewing the model coding and calculations for accuracy relative to the documented intent. Once validated, a model can typically be used from the prior production cycle for the current production cycle until a change is required (assuming it is in an appropriately controlled environment). Parallel testing and back-testing can help to ensure that the same model has been used for production from period to period. The purpose of the model is documented so that testers can verify that the model is used as intended.

It is becoming more common for more critical and complex models—for example, those used for financial reporting and other key business decisions within the organization—to be set up in a production environment. In some cases, ownership of the production

A PUBLIC POLICY PRACTICE NOTE

version of the model is with the information technology (“IT”) department rather than the actuarial (or other business unit or corporate) department. The production version of the model is used to run periodic analysis, and users of the model have limited to no ability to make any changes to the production environment without working through a formal change control process. Separate from the production environment, a “sandbox” version of the model allows model users to make and test changes that will not affect the model runs that are used for production. When a production change is needed the change is tested in the sandbox, and when final specifications for the change are ready they are provided to the modeling team for implementation. The modeling team is often comprised of IT coders or a combination of IT and actuarial coders to make the requested model changes as well as users to perform acceptance testing. Once approved the change can be brought into the production environment. This process helps mitigate risk of model errors but could require more advanced planning with all stakeholders for future model changes.

For models that are not part of a production environment it is still important to have controls to maintain the integrity of the model. Once a model has been verified as described above, user access and change controls may be used to maintain the model’s integrity until a change (and an associated re-validation) is needed. Such controls can involve maintaining a model in a restricted location to eliminate unintended access, requiring passwords for model use, restricting users’ ability to change the model, and detecting controls that identify if changes have been made and alert model owners or users to those changes.

Projection analytics involve evaluation of model results to assess whether they are aligned with model inputs and documented model mechanics. For example, if a model is designed to project future asset growth based on starting assets, a reinvestment strategy, and assumed returns by asset class, projection analytics could be used to verify that the proper starting assets, reinvestment strategy, and assumed returns are being used by the model. Analytical tests might involve looking at trends in asset values by class and returns on assets by asset class in the model output for reasonableness.

5. Model Risk Scoring/Measurement

To manage model risk effectively, model risk measurement may be a part of an organization’s model risk management activities. The measuring approach is ideally consistent across an organization to monitor and manage model risk comprehensively. It may be qualitative or quantitative. It is common for organizations to assess model risk within their model inventory in order to determine how to apply the model governance framework. In other words, greater governance requirements are applied for higher-risk models. This would typically be done using some kind of model risk scoring. Examples

A PUBLIC POLICY PRACTICE NOTE

of criteria that might influence scoring include how the model results are used (strategic decisions, financial reporting, etc.), the materiality of the model outputs, the nature of the model (spreadsheet, homegrown, vendor-based), frequency of use and updates, and whether it is used in a production environment. Organizations may also measure model risk for purposes of enterprise operational risk analysis, which could then lead to operational risk indicators or operational risk capital calculations.

1) Scoring Model Risk - Model Risk Scorecard

Scoring can be a qualitative approach. One way of scoring is through a model risk scorecard listing risk attributes (e.g., uncertainty surrounding inputs and assumptions, complexity of the model, type of model, significance of the model results, interactions with other models or tools, use of the model).

Because scoring of model risk is subjective, it can be a challenge for companies to maintain a consistent approach. A clear communication with all stakeholders may help to address this challenge.

2) Model Risk Quantification

Generally, model risk is classified as a part of operational risk and could be quantified with the same approach as evaluating other operational risks—that is, develop estimates for the frequency and severity of model risk events, and use those to quantify losses at a defined level of likelihood. While this is not common practice, some companies include a quantified view of model risk in their risk metrics. This can be done by collecting historical information on losses associated with model risk (such as model errors or model failures) and using the data to construct a distribution of the risk occurrence (or, if there is insufficient data to fit to a distribution, using the data to define a tail or adverse event). From this data, a company could estimate the loss associated with model risk at a defined level of severity, such as 1 in 10 or 1 in 100. However, such analysis is only as good as the input assumptions regarding the expected loss and distribution of the risk. Therefore, some companies use more qualitative approach.

Alternatively, models may be tested to understand their limits and to assess their stability under various conditions through stress testing.

Due to the current limitations in stochastic modeling of the frequency and severity of model risk events, frequency and severity of the model risk may be simply classified - such as low, medium, high. The final results might not be very different from the model risk scoring approach.

A PUBLIC POLICY PRACTICE NOTE

Organizations can assess the materiality of their model risk based on the potential financial impact.

6. Model Development and Implementation

There is currently a wide range of practice regarding model development and implementation. Some of the considerations for model development and implementation include the following:

- Model ownership
- Model purpose and intended use
- Model specifications
- Segregation of duties
- Test versus production environments
- Governance process for new model implementation
- Periodic confirmations for implemented models
- Approach for version updates

It is becoming increasingly common for organizations to have a centralized modeling team by area of expertise or product line (e.g., market risk, annuities, catastrophe, pandemic, etc.). However, not every organization has sufficient resources to allow the creation of dedicated modeling teams. As an alternative, the functions that use models as part of their day-to-day activities may have modeling experts that serve a similar role for the models applicable to their area. In these instances, it is helpful to have a centralized and common model policies and procedures to ensure consistency across multiple sets of model users. Such policies and procedures can be developed by a centralized function such as corporate actuarial, compliance, or ERM.

A critical consideration related to the development and implementation of a model is whether the model is fit for its intended purpose. Evaluating fitness of purpose as part of model development is still evolving in the insurance industry. Practices involve documenting the intended purpose of the model including considerations such as:

- Key technical requirements (i.e., what does the model need to calculate?)
- Frequency of use
- Ease of use
- Extent of training required
- Ability to modify calculations

A PUBLIC POLICY PRACTICE NOTE

- Frequency of updates
- Documentation
- Control features
- Reporting

With these considerations, alternative models can be compared to assess goodness of fit. For example, a model that works very well for reserving purposes may not be a good fit for pricing purposes. Even for producing the exact same modeling result, the frequency of use, ease of use, and ability to modify calculations can be insufficient. Further, a pricing model that targets an expected profit margin, in most situations, may not be suitable for the assessment of tail risk. Some organizations have specific guidelines for evaluating the fitness of a model for its intended use, including documentation and review required. Others use a more informal approach in which key model developers and users are responsible for assessing goodness of fit and then the selection of the model.

Implementation of a model involves selecting and building the hardware and software environment for the model, developing the data feeds, building the calculation engine, developing output feeds and reports, and developing and implementing controls for each portion of the model run process. Considerations include where software will reside (a shared drive, cloud-based, etc.), user access controls, change controls, access to computing power (such as internally housed processing “grids” or use of external processing resources), links to data warehouses, links to reporting engines, and the nature of controls (automated, manual, preventive vs. detective). Implementation typically also involves user acceptance testing and an approval process prior to actual use of the model for its intended purpose.

Practice typically includes two types of model documentation: model development and model implementation. A model development document describes, in generally understood terms, what the model will do, model methodology and calculations, data requirements and model inputs, model outputs, and various model tests such as back-testing, sensitivity testing, and benchmark testing that ensure that the model is performing adequately. A model implementation document describes how the model is implemented, the hardware and software environment, how the model is operated, testing that ensures the model is implemented correctly, system maintenance, model change control, and access control.

Just as the operation of the model typically calls for appropriate segregation of duties, so does model development and implementation. A “three lines of defense” approach may be applied, in which the model owners have responsibility for model development and implementation, with appropriate review and oversight from an independent party such as ERM, and final review and testing by internal audit. The “first line” model developers

A PUBLIC POLICY PRACTICE NOTE

can involve multiple stakeholders. For example, a combined team of business units and modelers from a centralized modeling team could define the desired characteristics of the model based on its intended use, select an appropriate model, develop business and technical specifications for the model, build and test the model, and ultimately deploy the model into production. The ERM function might define policies and procedures for model development and implementation, performs a secondary review of the development and implementation for adherence to those policies, and provides feedback and input.

Most vendor models develop periodic updates to the underlying capabilities, often through a new software version. These too would usually be subject to some or all of the requirements for a new model. For example, the update might be tested in a sandbox environment first for users to become comfortable with model results. Then, the updated version would be scheduled for implementation in the production environment through the IT change process and would require user acceptance testing. Lastly, for version updates (or other model changes), the organization may evaluate differences in results of current and prior models by parallel testing.

7. Model Review/Validation

1) Model Owner's Role

The model owner typically reviews the model on a regular basis to mitigate the risks identified in the assessment or a previous validation. Typical responsibilities of the model owner are listed below:

- Maintaining the day-to-day viability of the model for its intended use;
- Implementing appropriate controls to mitigate model risk;
- Documenting the model, including updating the model inventory and informing those responsible for model risk management of any changes;
- Engaging those responsible for model validation to evaluate or re-evaluate the risk of each model regularly and prioritize models to be validated, including new models; and
- Working with those responsible for model validation.

2) Model Validation

Many organizations have requirements related to model validation (which, depending on the organization, could be called model certification, affirmation, or validation). This practice note refers to it as validation. Regardless of terminology, there are a set of requirements and procedures that typically occur before a model is deemed ready for use. The model risk management policy will indicate requirements for validation,

A PUBLIC POLICY PRACTICE NOTE

which usually relate to the riskiness of the model, whether it is new, and whether it has previously been validated (and how recently).

Model validation can involve review of model inputs, checking model mechanics, parallel or back-testing of a model, review of model results, and confirmation that the model is appropriate for its intended use. Checking of model mechanics could be performed by independently replicating all or part of a model from scratch or reviewing the model coding and calculations for accuracy relative to its documented intent.

Models can be categorized within the model inventory. For example, “Model validated and fit for use,” “Validation in progress,” or “Models can’t be validated or not fit for use.”

When changes in an existing model occur, the model owner consults with the model validation team if the changes will trigger models for validation. Model owners typically work with the assigned model validation team to set a model validation schedule and resolve issues or suggested improvements within a specified period of time.

An example of a model validation plan can be found in [Appendix I](#).

To begin model validations, model risk management team typically engages with model owners to validate their models according to a pre-set schedule or updated schedule for new models or material changes to existing models, and provide model related uses, ownership, control environment, data input, documentation, and output. Other times the model validation schedule and plans are owned by others responsible for model governance, and they communicate plans to the model owners.

Model owners typically monitor model risk on a regular basis, including reviewing industry practices with respect to current model methodology and remediating any model deficiencies to protect the integrity of the models.

Primary responsibilities of the model validation team usually are:

- Evaluating whether any changes in existing models will trigger model validation events;
- Understanding the model, its governance and ownership, its intended use, any internal or external requirements for the model, and who the key users of the model are;
- Performing independent review and challenging the conceptual soundness, input, output, and analysis of the models based on their intended uses;

A PUBLIC POLICY PRACTICE NOTE

- Performing independent testing necessary to support assessment of model fitness; and
- Producing a model validation report including requirements for remediation and other recommendations.

Remediation of model deficiencies and reduction of model risk are often responsibilities of the model owner. In order to fulfill these responsibilities, the model owner may develop a regular schedule of activities, coordinating with model risk management team members, internal audit, or other model risk monitoring team members. Remediation progress may be tracked and reported through a process set up by the organization. Typically, in addition to the model owner and the model validation team, risk management, internal audit, IT, the modeling team, or any relevant business units linked to the model input and use can be involved in the model risk remediation processes.

8. Performance Monitoring

A model risk management policy defines the requirements and frequency for performance monitoring for the early detection of deviations from target performance, as well as performance monitoring responsibilities. After a model is put into production, it can be important to track emerging actual experience and successive estimates from the model using the latest available data to evaluate deviations from expected results. The policy should ideally define the reporting requirements of the monitoring results (e.g., regular tracking of actual-to-expected outcomes) and the related actions taken.

Performance monitoring typically involves a periodic review of model results, and whether there are unexpected results or uses of the model results. Monitoring of results could point to gaps between actual and modeled results, increased unattributed changes in results, increased questions from users, or issues relative to competitors or benchmarks.

9. Practical Aspects of Modeling

When an organization is establishing its definition of a model, it might look to external sources. The Federal Reserve and the Actuarial Standards Board definitions cited in [Section II-1](#) of this practice note are two of the many available external sources. Due to the increased emphasis on sound model risk management, it is important to develop a definition of a model and model governance design that meet internal needs as well as the needs of external stakeholders including regulatory bodies, rating agencies, policyholders, and shareholders.

There can be gray areas in determining whether a tool meets the definition of a model, and judgment may need to be exercised. Participants independent of model ownership

A PUBLIC POLICY PRACTICE NOTE

could provide unbiased judgment in identifying models. Such participants could be other internal employees or external parties such as auditors or regulators. Their input is valuable in situations where tools are in the gray areas of meeting the definition of a model. It is generally better to have a very low bar for defining a tool as a model. The more tools that are included, the more tools will be subject to the rigor of an organization's model governance. An organization might choose to subject a tool to model governance that does not fit within the definition of a model if its use is critical to making key business decisions.

An organization may lack sufficient skilled resources to allow for robust segregation of duties with respect to model review or validation needs. A practical solution is to borrow resources from other parts of the organization such as another business unit. This not only provides independent resources but allows for the sharing of alternative model development and maintenance practices. Typically, such sharing of resources across an organization does not change the ultimate model owner.

Consistent processes around building and maintaining models are a sound goal. Inconsistent approaches across an organization, whether it be related to the model design, building, testing, updating, etc., are likely when beginning the process of formalizing model governance. A review of the processes in place can assist in the identification of best practices to be shared and ultimately required as a part of an organization's model governance. For example, an IT department experienced in building and testing systems might be able to recommend methodical and comprehensive approaches to complex or new models. In addition, clarity of roles and responsibilities in making decisions related to models can build consistency, such as:

- Who ultimately decides whether a particular tool is a model.
- How an organization decides that it is time to build a new model or retire a legacy model.
- Who decides whether model validation feedback will be incorporated into a model.

Lastly, developing a model inventory, ranking models based on their importance to the overall financial projections, and identifying the manner in which the results of different models depend on one another can be a time-consuming undertaking. Although these steps are very important to the risk management of models, the key models are often known to an organization without pursuing a comprehensive modeling inventory. To ensure that a key model is not overlooked and that models can be prioritized, the ranking of models according to financial significance, whether quantitatively or qualitatively, can assist in identification of all key models. Early on in the implementation of model risk governance, applying governance requirements to the key models may be a more immediate need relative to compiling a complete and fully ranked inventory of models.

A PUBLIC POLICY PRACTICE NOTE

Further, it may be more important to address key items related to each governance requirement, whether it be validation of the most influential aspects or implementation of the proper security features in specific areas of key models, as opposed to ensuring completeness of each requirement. Immediate relief from the most critical modeling risks can provide greater value than pursuing comprehensive model governance if a choice has to be made. It is a typical practice to expand the model governance process over time, including as many models as is feasible for the organization.

A PUBLIC POLICY PRACTICE NOTE

IV. Relevant Regulation

United States

- Valuation Manual, VM-G (Appendix G) - Corporate Governance Guidance for Principle-Based Reserves, Section 3
https://store.naic.org/documents/cmte_a_latf_related_val_2019_edition.pdf?37
- US Actuarial Standards of Practice: ASOP No. 23, *Data Quality*
<http://www.actuarialstandardsboard.org/asops/data-quality/>
- Model Governance Practice Note: Some Considerations for Practicing Life Actuaries
https://www.actuary.org/sites/default/files/files/publications/Model_Governance_PN_042017.pdf
- Model Governance Checklist: Some Considerations for Practicing Life Actuaries, August 2016
http://actuary.org/files/publications/PBRChecklist_Final.pdf

Canada

- Guideline E-23—Enterprise-Wide Model Risk Management Guideline
<http://www.osfi-bsif.gc.ca/Eng/fin-if/rg-ro/gdn-ort/gl-ld/Pages/e23.aspx>

United Kingdom

- Solvency II: internal models – assessment, model change and the role of non-executive directors – SS17/16, Nov. 25, 2016
<http://www.bankofengland.co.uk/pr/Pages/publications/ss/2016/ss1716.aspx>
- Solvency II: regulatory reporting, internal model outputs – SS25/15 Update, Feb. 16, 2017
<http://www.bankofengland.co.uk/pr/Pages/publications/ss/2017/ss2515update.aspx>

A PUBLIC POLICY PRACTICE NOTE

APPENDIX 1 Sample Model Validation Plan

Model Validation Plan Assumptions³

1. Assumes that the focus is on substantively validating the model, without reliance on user controls (in some cases, model review might start with review of controls, and if they are strong, no “hands on” validation would be performed).
2. Model is of moderate complexity and there are no significant resource constraints. Simple models may be completed more quickly while complex models may take longer. Constraints on model owner or model validation resources would extend timeline.
3. Assumes that there is reasonable model documentation in place.
4. Information is readily available (if more time is needed to gather information, the elapsed time for the review will be longer).
5. Assumption validation is a separate exercise and is only covered at a high level here with respect to confirmation of appropriateness for the specific model being validated. An exhaustive assumption validation/review would take additional steps and time.

Detailed Model Validation Plan⁴

- I. Planning
 - a. Establish goals and objectives
 - b. Perform resource planning
 - c. Kickoff meeting with stakeholders
 - d. Establish key contact person
 - e. Develop project plan including tasks, timing, responsibilities, and deliverables
 - f. Create initial data request
 - g. Develop initial sampling approach (methodology, time periods, etc.)
- II. Review of model inputs
 - a. Review documentation of model inputs and sources
 - i. Review model documentation
 - ii. Conduct interviews/send follow-up requests as needed
 - b. Obtain and review actual model inputs
 - i. Inventory-type data (assets, policies, etc.)

³ Source: Risk & Regulatory Consulting. Not to be duplicated without prior written consent

⁴ Source: Risk & Regulatory Consulting. Not to be duplicated without prior written consent

A PUBLIC POLICY PRACTICE NOTE

- ii. Assumptions
 - iii. Market data
 - iv. Product specifications
 - v. Other
 - c. Compare inputs to documentation, identify gaps
 - d. Verify model inputs back to source (may be done on a sample basis)
 - i. Inventory-type: compare model inputs to source systems
 - ii. Assumptions: compare to supporting experience studies (internal or external), evaluate credibility considerations, fitness for purpose, approach for margins
 - iii. Market data: compare to publicly available data where available, other supporting documentation (price quotes, Bloomberg data, etc.)
 - iv. Product specifications: compare model inputs to policy forms
 - e. Document findings and conclusions
- III. Review of calculation engine/model checking
- a. Review documentation of calculations and intended use
 - i. Review the testing performed internally by model owners and developers
 - b. Determine approach(es) for calculation validation
 - i. Review of code
 - ii. Full replication of model
 - iii. Replication on a sample basis
 - iv. Aggregate reasonability tests such as dynamic validations, analytical tests, sensitivity testing
 - c. If needed, perform sampling of test population
 - i. Subsets of code
 - ii. Sample of policies, products, assets, scenarios, etc.
 - d. Perform testing on model calculations based on validation approach(es) chosen
 - e. Compare calculations to documentation, identify gaps
 - f. Evaluate calculations relative to other applicable standards, if any
 - i. Internal standards (for example, assumption setting)
 - ii. Regulations (for example, VM-20)
 - iii. Actuarial standards of practice (for example, ASOP No. 7, ASOP No. 13)
 - g. Document findings and conclusions
- IV. Review of model outputs

A PUBLIC POLICY PRACTICE NOTE

- a. Review model outputs, including any end-user computing applications and end-user reports
- b. Evaluate overall fitness of model for purpose
- c. Compare ultimate results/reports to direct model outputs, identify gaps
- d. Review the reports from the model output and compare the objectives of the reports with contents
- e. Document findings and conclusions

V. Reporting

- a. Draft findings and recommendations
- b. Business/owner review
- c. Finalize reporting

VI. Ongoing Communications and Project Management