SUPERVISORY GUIDANCE ON MODEL RISK MANAGEMENT

CONTENTS

I. Introduction.....1
II. Purpose and Scope.....2
III. Overview of Model Risk Management.....2
IV. Model Development, Implementation, and Use.....4
V. Model Validation.....7
VI. Governance, Policies, and Controls.....14
VII. Conclusion.....18

I. INTRODUCTION

Banks rely heavily on quantitative analysis and models in most aspects of financial decision making.[1] They routinely use models for a broad range of activities, including underwriting credits; valuing exposures, instruments, and positions; measuring risk; managing and safeguarding client assets; determining capital and reserve adequacy; and many other activities. In recent years, banks have applied models to more complex products and with more ambitious scope, such as enterprise-wide risk measurement, while the markets in which they are used have also broadened and changed. Changes in regulation have spurred some of the recent developments, particularly the U.S. regulatory capital rules for market, credit, and operational risk based on the framework developed by the Basel Committee on Banking Supervision. Even apart from these regulatory considerations, however, banks have been increasing the use of data-driven, quantitative decision-making tools for a number of years.

The expanding use of models in all aspects of banking reflects the extent to which models can improve business decisions, but models also come with costs. There is the direct cost of devoting resources to develop and implement models properly. There are also the potential indirect costs of relying on models, such as the possible adverse consequences (including financial loss) of decisions based on models that are incorrect or misused. Those consequences should be addressed by active management of model risk.

This guidance describes the key aspects of effective model risk management. Section II explains the purpose and scope of the guidance, and Section III gives an overview of model risk management.

[1] Unless otherwise indicated, *banks* refers to state non-member banks, state savings associations, and all other institutions for which the Federal Deposit Insurance Corporation is the primary supervisor. It is not expected that this guidance will pertain to FDIC-supervised institutions with under $1 billion in total assets unless the institution's model use is significant, complex, or poses elevated risk to the institution.

Section IV discusses robust model development, implementation, and use. Section V describes the components of an effective validation framework. Section VI explains the salient features of sound governance, policies, and controls over model development, implementation, use, and validation. Section VII concludes.

II. PURPOSE AND SCOPE

The purpose of this document is to provide comprehensive guidance for banks on effective model risk management. Rigorous model validation plays a critical role in model risk management; however, sound development, implementation, and use of models are also vital elements. Furthermore, model risk management encompasses governance and control mechanisms such as board and senior management oversight, policies and procedures, controls and compliance, and an appropriate incentive and organizational structure.

Previous guidance and other publications issued by the FDIC on the use of models address aspects of model risk management for specific types of models or pay particular attention to model validation.[2] Based on supervisory and industry experience over the past several years, this document expands on existing guidance—most importantly by broadening the scope to include all aspects of model risk management. Many banks may already have in place a large portion of these practices, but banks should ensure that internal policies and procedures are consistent with the risk management principles and supervisory expectations contained in this guidance. Details may vary from bank to bank, as practical application of this guidance should be customized to be commensurate with a bank's risk exposures, its business activities, and the complexity and extent of its model use. For example, steps taken to apply this guidance at banks using relatively few models of only moderate complexity might be significantly less involved than those at a bank where use of models is more extensive or complex.

III. OVERVIEW OF MODEL RISK MANAGEMENT

For the purposes of this document, the term *model* refers 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. 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. Models meeting this definition might be used for analyzing business strategies, informing business decisions, identifying and measuring risks, valuing exposures, instruments or positions, conducting stress testing, assessing adequacy of capital, managing client assets, measuring compliance with internal limits, maintaining the formal control apparatus of the bank, or meeting financial or regulatory reporting requirements and issuing public

[2] For instance, the FDIC has addressed aspects of model risk management in guidance related to different activities; see Joint Agency Policy Statement on Interest Rate Risk (FIL-52-96), FFIEC Advisory on Interest Rate Risk Management (FIL-2-2010), Interagency Advisory on Interest Rate Risk Management Frequently Asked Questions (FIL-2-2012), FDIC's Credit Card Activities Manual (https://www.fdic.gov/regulations/examinations/credit_card/), and Supervisory Guidance on Implementing Dodd-Frank Act Company-Run Stress Tests for Banking Organizations With Total Consolidated Assets of More Than $10 Billion but Less Than $50 Billion (79 FR 14153). In addition, the advanced-approaches risk-based capital rules (12 CFR 325, Appendix D) contain explicit validation requirements for subject banking organizations.

disclosures. The definition of *model* also covers quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature.[3]

Models are simplified representations of real-world relationships among observed characteristics, values, and events. Simplification is inevitable, due to the inherent complexity of those relationships, but also intentional, to focus attention on particular aspects considered to be most important for a given model application. Model quality can be measured in many ways: precision, accuracy, discriminatory power, robustness, stability, and reliability, to name a few. Models are never perfect, and the appropriate metrics of quality, and the effort that should be put into improving quality, depend on the situation. For example, precision and accuracy are relevant for models that forecast future values, while discriminatory power applies to models that rank order risks. In all situations, it is important to understand a model's capabilities and limitations given its simplifications and assumptions.

The use of models invariably presents model risk, which 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 a bank's reputation. Model risk occurs primarily for two reasons:

- The model may have fundamental errors and may produce inaccurate outputs when viewed against the design objective and intended business uses. The mathematical calculation and quantification exercise underlying any model generally involves application of theory, choice of sample design and numerical routines, selection of inputs and estimation, and implementation in information systems. Errors can occur at any point from design through implementation. In addition, shortcuts, simplifications, or approximations used to manage complicated problems could compromise the integrity and reliability of outputs from those calculations. Finally, the quality of model outputs depends on the quality of input data and assumptions, and errors in inputs or incorrect assumptions will lead to inaccurate outputs.
- The model may be used incorrectly or inappropriately. Even a fundamentally sound model producing accurate outputs consistent with the design objective of the model may exhibit high model risk if it is misapplied or misused. Models by their nature are simplifications of reality, and real-world events may prove those simplifications inappropriate. This is even more of a concern if a model is used outside the environment for which it was designed. Banks may do this intentionally as they apply existing models to new products or markets, or inadvertently as market conditions or customer behavior changes. Decision makers need to understand the limitations of a model to avoid using it in ways that are not consistent with the original intent. Limitations come in part from weaknesses in the model due to its various shortcomings, approximations, and uncertainties. Limitations are also a consequence of assumptions underlying a model that may restrict the scope to a limited set of specific circumstances and situations.

Model risk should be managed like other types of risk. Banks should identify the sources of risk and assess the magnitude. Model risk increases with greater model complexity, higher uncertainty about inputs and assumptions, broader use, and larger potential impact. Banks should consider risk from individual models and in the aggregate. Aggregate model risk is affected by interaction and dependencies among models; reliance on common assumptions, data, or methodologies; and any

[3] While outside the scope of this guidance, more qualitative approaches used by banking organizations—i.e., those not defined as models according to this guidance—should also be subject to a rigorous control process.

other factors that could adversely affect several models and their outputs at the same time. With an understanding of the source and magnitude of model risk in place, the next step is to manage it properly.

A guiding principle for managing model risk is "effective challenge" of models, that is, critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate changes. Effective challenge depends on a combination of incentives, competence, and influence. Incentives to provide effective challenge to models are stronger when there is greater separation of that challenge from the model development process and when challenge is supported by well-designed compensation practices and corporate culture. Competence is a key to effectiveness since technical knowledge and modeling skills are necessary to conduct appropriate analysis and critique. Finally, challenge may fail to be effective without the influence to ensure that actions are taken to address model issues. Such influence comes from a combination of explicit authority, stature within the organization, and commitment and support from higher levels of management.

Even with skilled modeling and robust validation, model risk cannot be eliminated, so other tools should be used to manage model risk effectively. Among these are establishing limits on model use, monitoring model performance, adjusting or revising models over time, and supplementing model results with other analysis and information. Informed conservatism, in either the inputs or the design of a model or through explicit adjustments to outputs, can be an effective tool, though not an excuse to avoid improving models.

As is generally the case with other risks, materiality is an important consideration in model risk management. If at some banks the use of models is less pervasive and has less impact on their financial condition, then those banks may not need as complex an approach to model risk management in order to meet supervisory expectations. However, where models and model output have a material impact on business decisions, including decisions related to risk management and capital and liquidity planning, and where model failure would have a particularly harmful impact on a bank's financial condition, a bank's model risk management framework should be more extensive and rigorous.

Model risk management begins with robust model development, implementation, and use. Another essential element is a sound model validation process. A third element is governance, which 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. The following sections of this document cover each of these elements.

IV. MODEL DEVELOPMENT, IMPLEMENTATION, AND USE

Model risk management should include disciplined and knowledgeable development and implementation processes that are consistent with the situation and goals of the model user and with bank policy. Model development is not a straightforward or routine technical process. The experience and judgment of developers, as much as their technical knowledge, greatly influence the appropriate selection of inputs and processing components. The training and experience of developers exercising such judgment affects the extent of model risk. Moreover, the modeling exercise is often a multidisciplinary activity drawing on economics, finance, statistics, mathematics, and other fields. Models are employed in real-world markets and events and therefore should be tailored for specific

applications and informed by business uses. In addition, a considerable amount of subjective judgment is exercised at various stages of model development, implementation, use, and validation. It is important for decision makers to recognize that this subjectivity elevates the importance of sound and comprehensive model risk management processes.[4]

Model Development and Implementation

An effective development process begins with a clear statement of purpose to ensure that model development is aligned with the intended use. The design, theory, and logic underlying the model should be well documented and generally supported by published research and sound industry practice. The model methodologies and processing components that implement the theory, including the mathematical specification and the numerical techniques and approximations, should be explained in detail with particular attention to merits and limitations. Developers should ensure that the components work as intended, are appropriate for the intended business purpose, and are conceptually sound and mathematically and statistically correct. Comparison with alternative theories and approaches is a fundamental component of a sound modeling process.

The data and other information used to develop a model are of critical importance; there should be rigorous assessment of data quality and relevance, and appropriate documentation. Developers should be able to demonstrate that such data and information are suitable for the model and that they are consistent with the theory behind the approach and with the chosen methodology. If data proxies are used, they should be carefully identified, justified, and documented. If data and information are not representative of the bank's portfolio or other characteristics, or if assumptions are made to adjust the data and information, these factors should be properly tracked and analyzed so that users are aware of potential limitations. This is particularly important for external data and information (from a vendor or outside party), especially as they relate to new products, instruments, or activities.

An integral part of model development is testing, in which the various components of a model and its overall functioning are evaluated to determine whether the model is performing as intended. Model testing includes checking the model's accuracy, demonstrating that the model is robust and stable, assessing potential limitations, and evaluating the model's behavior over a range of input values. It should also assess the impact of assumptions and identify situations where the model performs poorly or becomes unreliable. Testing should be applied to actual circumstances under a variety of market conditions, including scenarios that are outside the range of ordinary expectations, and should encompass the variety of products or applications for which the model is intended. Extreme values for inputs should be evaluated to identify any boundaries of model effectiveness. The impact of model results on other models that rely on those results as inputs should also be evaluated. Included in testing activities should be the purpose, design, and execution of test plans, summary results with commentary and evaluation, and detailed analysis of informative samples. Testing activities should be appropriately documented.

The nature of testing and analysis will depend on the type of model and will be judged by different criteria depending on the context. For example, the appropriate statistical tests depend on specific distributional assumptions and the purpose of the model. Furthermore, in many cases statistical tests

[4] Less complex banks that rely on vendor models may be able to satisfy the standards in this guidance without an in-house staff of technical, quantitative model developers. However, even if a bank relies on vendors for basic model development, the bank should still choose the particular models and variables that are appropriate to its size, scale, and lines of business and ensure the models are appropriate for the intended use.

cannot unambiguously reject false hypotheses or accept true ones based on sample information. Different tests have different strengths and weaknesses under different conditions. Any single test is rarely sufficient, so banks should apply a variety of tests to develop a sound model.

Banks should ensure that the development of the more judgmental and qualitative aspects of their models is also sound. In some cases, banks may take statistical output from a model and modify it with judgmental or qualitative adjustments as part of model development. While such practices may be appropriate, banks should ensure that any such adjustments made as part of the development process are conducted in an appropriate and systematic manner, and are well documented.
Models typically are embedded in larger information systems that manage the flow of data from various sources into the model and handle the aggregation and reporting of model outcomes. Model calculations should be properly coordinated with the capabilities and requirements of information systems. Sound model risk management depends on substantial investment in supporting systems to ensure data and reporting integrity, together with controls and testing to ensure proper implementation of models, effective systems integration, and appropriate use.

Model Use

Model use provides additional opportunity to test whether a model is functioning effectively and to assess its performance over time as conditions and model applications change. It can serve as a source of productive feedback and insights from a knowledgeable internal constituency with strong interest in having models that function well and reflect economic and business realities. Model users can provide valuable business insight during the development process. In addition, business managers affected by model outcomes may question the methods or assumptions underlying the models, particularly if the managers are significantly affected by and do not agree with the outcome. Such questioning can be healthy if it is constructive and causes model developers to explain and justify the assumptions and design of the models.

However, challenge from model users may be weak if the model does not materially affect their results, if the resulting changes in models are perceived to have adverse effects on the business line, or if change in general is regarded as expensive or difficult. User challenges also tend not to be comprehensive because they focus on aspects of models that have the most direct impact on the user's measured business performance or compensation, and thus may ignore other elements and applications of the models. Finally, such challenges tend to be asymmetric, because users are less likely to challenge an outcome that results in an advantage for them. Indeed, users may incorrectly believe that model risk is low simply because outcomes from model-based decisions appear favorable to the institution. Thus, the nature and motivation behind model users' input should be evaluated carefully, and banks should also solicit constructive suggestions and criticism from sources independent of the line of business using the model.

Reports used for business decision making play a critical role in model risk management. Such reports should be clear and comprehensible and take into account the fact that decision makers and modelers often come from quite different backgrounds and may interpret the contents in different ways. Reports that provide a range of estimates for different input-value scenarios and assumption values can give decision makers important indications of the model's accuracy, robustness, and stability as well as information on model limitations.

An understanding of model uncertainty and inaccuracy and a demonstration that the bank is accounting for them appropriately are important outcomes of effective model development, implementation, and use. Because they are by definition imperfect representations of reality, all

models have some degree of uncertainty and inaccuracy. These can sometimes be quantified, for example, by an assessment of the potential impact of factors that are unobservable or not fully incorporated in the model, or by the confidence interval around a statistical model's point estimate. Indeed, using a range of outputs, rather than a simple point estimate, can be a useful way to signal model uncertainty and avoid spurious precision. At other times, only a qualitative assessment of model uncertainty and inaccuracy is possible. In either case, it can be prudent for banks to account for model uncertainty by explicitly adjusting model inputs or calculations to produce more severe or adverse model output in the interest of conservatism. Accounting for model uncertainty can also include judgmental conservative adjustments to model output, placing less emphasis on that model's output, or ensuring that the model is only used when supplemented by other models or approaches.[5]

While conservative use of models is prudent in general, banks should be careful in applying conservatism broadly or claiming to make conservative adjustments or add-ons to address model risk, because the impact of such conservatism in complex models may not be obvious or intuitive. Model aspects that appear conservative in one model may not be truly conservative compared with alternative methods. For example, simply picking an extreme point on a given modeled distribution may not be conservative if the distribution was misestimated or misspecified in the first place. Furthermore, initially conservative assumptions may not remain conservative over time. Therefore, banks should justify and substantiate claims that model outputs are conservative with a definition and measurement of that conservatism that is communicated to model users. In some cases, sensitivity analysis or other types of stress testing can be used to demonstrate that a model is indeed conservative. Another way in which banks may choose to be conservative is to hold an additional cushion of capital to protect against potential losses associated with model risk. However, conservatism can become an impediment to proper model development and application if it is seen as a solution that dissuades the bank from making the effort to improve the model; in addition, excessive conservatism can lead model users to discount the model outputs.

As this section has explained, robust model development, implementation, and use is important to model risk management. But it is not enough for model developers and users to understand and accept the model. Because model risk is ultimately borne by the bank as a whole, the bank should objectively assess model risk and the associated costs and benefits using a sound model-validation process.

V. MODEL VALIDATION

Model validation is the set of processes and activities intended to verify that models are performing as expected, in line with their design objectives and business uses. Effective validation helps ensure that models are sound. It also identifies potential limitations and assumptions, and assesses their possible impact. As with other aspects of effective challenge, model validation should be performed by staff with appropriate incentives, competence, and influence.

All model components, including input, processing, and reporting, should be subject to validation; this applies equally to models developed in-house and to those purchased from or developed by vendors or consultants. The rigor and sophistication of validation should be commensurate with the bank's overall use of models, the complexity and materiality of its models, and the size and complexity of the bank's operations.

[5] To the extent that models are used to generate amounts included in public financial statements, any adjustments for model uncertainty are required by existing law to comply with generally accepted accounting principles.

Validation involves a degree of independence from model development and use. Generally, validation should be done by people who are not responsible for development or use and do not have a stake in whether a model is determined to be valid. Independence is not an end in itself but rather helps ensure that incentives are aligned with the goals of model validation. While independence may be supported by separation of reporting lines, it should be judged by actions and outcomes, since there may be additional ways to ensure objectivity and prevent bias. As a practical matter, some validation work may be most effectively done by model developers and users; it is essential, however, that such validation work be subject to critical review by an independent party, who should conduct additional activities to ensure proper validation. Overall, the quality of the process is judged by the manner in which models are subject to critical review. This could be determined by evaluating the extent and clarity of documentation, the issues identified by objective parties, and the actions taken by management to address model issues.

In addition to independence, banks can support appropriate incentives in validation through compensation practices and performance evaluation standards that are tied directly to the quality of model validations and the degree of critical, unbiased review. In addition, corporate culture plays a role if it establishes support for objective thinking and encourages questioning and challenging of decisions.

Staff doing validation should have the requisite knowledge, skills, and expertise. A high level of technical expertise may be needed because of the complexity of many models, both in structure and in application. These staff also should have a significant degree of familiarity with the line of business using the model and the model's intended use. A model's developer is an important source of information but cannot be relied on as an objective or sole source on which to base an assessment of model quality.

Staff conducting validation work should have explicit authority to challenge developers and users and to elevate their findings, including issues and deficiencies. The individual or unit to whom those staff report should have sufficient influence or stature within the bank to ensure that any issues and deficiencies are appropriately addressed in a timely and substantive manner. Such influence can be reflected in reporting lines, title, rank, or designated responsibilities. Influence may be demonstrated by a pattern of actual instances in which models, or the use of models, have been appropriately changed as a result of validation.

The range and rigor of validation activities conducted prior to first use of a model should be in line with the potential risk presented by use of the model. If significant deficiencies are noted as a result of the validation process, use of the model should not be allowed or should be permitted only under very tight constraints until those issues are resolved. If the deficiencies are too severe to be addressed within the model's framework, the model should be rejected. If it is not feasible to conduct necessary validation activities prior to model use because of data paucity or other limitations, that fact should be documented and communicated in reports to users, senior management, and other relevant parties. In such cases, the uncertainty about the results that the model produces should be mitigated by other compensating controls. This is particularly applicable to new models and to the use of existing models in new applications.

Validation activities should continue on an ongoing basis after a model goes into use, to track known model limitations and to identify any new ones. Validation is an important check on model use during periods of benign economic and financial conditions, when estimates of risk and potential loss can become overly optimistic, and when the data at hand may not fully reflect more stressed conditions. Ongoing validation activities help to ensure that changes in markets, products, exposures,

activities, clients, or business practices do not create new model limitations. For example, if credit risk models do not incorporate underwriting changes in a timely manner, flawed and costly business decisions could be made before deterioration in model performance becomes apparent.

Banks should conduct a periodic review—at least annually but more frequently if warranted—of each model to determine whether it is working as intended and if the existing validation activities are sufficient. Such a determination could simply affirm previous validation work, suggest updates to previous validation activities, or call for additional validation activities. Material changes to models should also be subject to validation. It is generally good practice for banks to ensure that all models undergo the full validation process, as described in the following section, at some fixed interval, including updated documentation of all activities.

Effective model validation helps reduce model risk by identifying model errors, corrective actions, and appropriate use. It also provides an assessment of the reliability of a given model, based on its underlying assumptions, theory, and methods. In this way, it provides information about the source and extent of model risk. Validation also can reveal deterioration in model performance over time and can set thresholds for acceptable levels of error, through analysis of the distribution of outcomes around expected or predicted values. If outcomes fall consistently outside this acceptable range, then the models should be redeveloped.

Key Elements of Comprehensive Validation

An effective validation framework should include three core elements:

- Evaluation of conceptual soundness, including developmental evidence
- Ongoing monitoring, including process verification and benchmarking
- Outcomes analysis, including back-testing

1. Evaluation of Conceptual Soundness

This element involves assessing the quality of the model design and construction. It entails review of documentation and empirical evidence supporting the methods used and variables selected for the model. Documentation and testing should convey an understanding of model limitations and assumptions. Validation should ensure that judgment exercised in model design and construction is well informed, carefully considered, and consistent with published research and with sound industry practice. Developmental evidence should be reviewed before a model goes into use and also as part of the ongoing validation process, in particular whenever there is a material change in the model.

A sound development process will produce documented evidence in support of all model choices, including the overall theoretical construction, key assumptions, data, and specific mathematical calculations, as mentioned in Section IV. As part of model validation, those model aspects should be subjected to critical analysis by both evaluating the quality and extent of developmental evidence and conducting additional analysis and testing as necessary. Comparison to alternative theories and approaches should be included. Key assumptions and the choice of variables should be assessed, with analysis of their impact on model outputs and particular focus on any potential limitations. The relevance of the data used to build the model should be evaluated to ensure that it is reasonably representative of the bank's portfolio or market conditions, depending on the type of model. This is an especially important exercise when a bank uses external data or the model is used for new products or activities.

Where appropriate to the particular model, banks should employ sensitivity analysis in model development and validation to check the impact of small changes in inputs and parameter values on model outputs to make sure they fall within an expected range. Unexpectedly large changes in outputs in response to small changes in inputs can indicate an unstable model. Varying several inputs simultaneously as part of sensitivity analysis can provide evidence of unexpected interactions, particularly if the interactions are complex and not intuitively clear. Banks benefit from conducting model stress testing to check performance over a wide range of inputs and parameter values, including extreme values, to verify that the model is robust. Such testing helps establish the boundaries of model performance by identifying the acceptable range of inputs as well as conditions under which the model may become unstable or inaccurate.

Management should have a clear plan for using the results of sensitivity analysis and other quantitative testing. If testing indicates that the model may be inaccurate or unstable in some circumstances, management should consider modifying certain model properties, putting less reliance on its outputs, placing limits on model use, or developing a new approach.

Qualitative information and judgment used in model development should be evaluated, including the logic, judgment, and types of information used, to establish the conceptual soundness of the model and set appropriate conditions for its use. The validation process should ensure that qualitative, judgmental assessments are conducted in an appropriate and systematic manner, are well supported, and are documented.

2. Ongoing Monitoring

The second core element of the validation process is ongoing monitoring. Such monitoring confirms that the model is appropriately implemented and is being used and is performing as intended.

Ongoing monitoring is essential to evaluate whether changes in products, exposures, activities, clients, or market conditions necessitate adjustment, redevelopment, or replacement of the model and to verify that any extension of the model beyond its original scope is valid. Any model limitations identified in the development stage should be regularly assessed over time, as part of ongoing monitoring. Monitoring begins when a model is first implemented in production systems for actual business use. This monitoring should continue periodically over time, with a frequency appropriate to the nature of the model, the availability of new data or modeling approaches, and the magnitude of the risk involved. Banks should design a program of ongoing testing and evaluation of model performance along with procedures for responding to any problems that appear. This program should include process verification and benchmarking.

Process verification checks that all model components are functioning as designed. It includes verifying that internal and external data inputs continue to be accurate, complete, consistent with model purpose and design, and of the highest quality available. Computer code implementing the model should be subject to rigorous quality and change control procedures to ensure that the code is correct, that it cannot be altered except by approved parties, and that all changes are logged and can be audited. System integration can be a challenge and deserves special attention because the model processing component often draws from various sources of data, processes large amounts of data, and then feeds into multiple data repositories and reporting systems. User-developed applications, such as spreadsheets or ad hoc database applications used to generate quantitative estimates, are particularly prone to model risk. As the content or composition of information changes over time, systems may need to be updated to reflect any changes in the data or its use. Reports derived from

model outputs should be reviewed as part of validation to verify that they are accurate, complete, and informative, and that they contain appropriate indicators of model performance and limitations.

Many of the tests employed as part of model development should be included in ongoing monitoring and be conducted on a regular basis to incorporate additional information as it becomes available. New empirical evidence or theoretical research may suggest the need to modify or even replace original methods. Analysis of the integrity and applicability of internal and external information sources, including information provided by third-party vendors, should be performed regularly.

Sensitivity analysis and other checks for robustness and stability should likewise be repeated periodically. They can be as useful during ongoing monitoring as they are during model development. If models only work well for certain ranges of input values, market conditions, or other factors, they should be monitored to identify situations where these constraints are approached or exceeded.

Ongoing monitoring should include the analysis of overrides with appropriate documentation. In the use of virtually any model, there will be cases where model output is ignored, altered, or reversed based on the expert judgment of model users. Such overrides are an indication that, in some respect, the model is not performing as intended or has limitations. Banks should evaluate the reasons for overrides and track and analyze override performance. If the rate of overrides is high, or if the override process consistently improves model performance, it is often a sign that the underlying model needs revision or redevelopment.

Benchmarking is the comparison of a given model's inputs and outputs to estimates from alternative internal or external data or models. It can be incorporated in model development as well as in ongoing monitoring. For credit risk models, examples of benchmarks include models from vendor firms or industry consortia and data from retail credit bureaus. Pricing models for securities and derivatives often can be compared with alternative models that are more accurate or comprehensive but also too time consuming to run on a daily basis. Whatever the source, benchmark models should be rigorous and benchmark data should be accurate and complete to ensure a reasonable comparison.

Discrepancies between the model output and benchmarks should trigger investigation into the sources and degree of the differences, and examination of whether they are within an expected or appropriate range given the nature of the comparison. The results of that analysis may suggest revisions to the model. However, differences do not necessarily indicate that the model is in error. The benchmark itself is an alternative prediction, and the differences may be due to the different data or methods used. If the model and the benchmark match well, that is evidence in favor of the model, but it should be interpreted with caution so the bank does not get a false degree of comfort.

3. Outcomes Analysis

The third core element of the validation process is outcomes analysis, a comparison of model outputs to corresponding actual outcomes. The precise nature of the comparison depends on the objectives of a model, and might include an assessment of the accuracy of estimates or forecasts, an evaluation of rank-ordering ability, or other appropriate tests. In all cases, such comparisons help to evaluate model performance, by establishing expected ranges for those actual outcomes in relation to the intended objectives and assessing the reasons for observed variation between the two. If outcomes analysis produces evidence of poor performance, the bank should take action to address those issues. Outcomes analysis typically relies on statistical tests or other quantitative measures. It can also include expert judgment to check the intuition behind the outcomes and confirm that the results make

sense. When a model itself relies on expert judgment, quantitative outcomes analysis helps to evaluate the quality of that judgment. Outcomes analysis should be conducted on an ongoing basis to test whether the model continues to perform in line with design objectives and business uses.

A variety of quantitative and qualitative testing and analytical techniques can be used in outcomes analysis. The choice of technique should be based on the model's methodology, its complexity, data availability, and the magnitude of potential model risk to the bank. Outcomes analysis should involve a range of tests because any individual test will have weaknesses. For example, some tests are better at checking a model's ability to rank-order or segment observations on a relative basis, whereas others are better at checking absolute forecast accuracy. Tests should be designed for each situation, as not all will be effective or feasible in every circumstance, and attention should be paid to choosing the appropriate type of outcomes analysis for a particular model.

Models are regularly adjusted to take into account new data or techniques, or because of deterioration in performance. Parallel outcomes analysis, under which both the original and adjusted models' forecasts are tested against realized outcomes, provides an important test of such model adjustments. If the adjusted model does not outperform the original model, developers, users, and reviewers should realize that additional changes—or even a wholesale redesign—are likely necessary before the adjusted model replaces the original one.

Back-testing is one form of outcomes analysis; specifically, it involves the comparison of actual outcomes with model forecasts during a sample time period not used in model development and at an observation frequency that matches the forecast horizon or performance window of the model. The comparison is generally done using expected ranges or statistical confidence intervals around the model forecasts. When outcomes fall outside those intervals, the bank should analyze the discrepancies and investigate the causes that are significant in terms of magnitude or frequency. The objective of the analysis is to determine whether differences stem from the omission of material factors from the model, whether they arise from errors with regard to other aspects of model specification such as interaction terms or assumptions of linearity, or whether they are purely random and thus consistent with acceptable model performance. Analysis of in-sample fit and of model performance in holdout samples (data set aside and not used to estimate the original model) are important parts of model development but are not substitutes for back-testing.

A well-known example of back-testing is the evaluation of value-at-risk (VaR), in which actual profit and loss is compared with a model forecast loss distribution. Significant deviation in expected versus actual performance and unexplained volatility in the profits and losses of trading activities may indicate that hedging and pricing relationships are not adequately measured by a given approach. Along with measuring the frequency of losses in excess of a single VaR percentile estimator, banks should use other tests, such as assessing any clustering of exceptions and checking the distribution of losses against other estimated percentiles.

Analysis of the results of even high-quality and well-designed back-testing can pose challenges, since it is not a straightforward, mechanical process that always produces unambiguous results. The purpose is to test the model, not individual forecast values. Back-testing may entail analysis of a large number of forecasts over different conditions at a point in time or over multiple time periods. Statistical testing is essential in such cases, yet such testing can pose challenges in both the choice of appropriate tests and the interpretation of results; banks should support and document both the choice of tests and the interpretation of results.

Models with long forecast horizons should be back-tested, but given the amount of time it would take to accumulate the necessary data, that testing should be supplemented by evaluation over shorter periods. Banks should employ outcomes analysis consisting of "early warning" metrics designed to measure performance beginning very shortly after model introduction and trend analysis of performance over time. These outcomes analysis tools are not substitutes for back-testing, which should still be performed over the longer time period, but rather very important complements.

Outcomes analysis and the other elements of the validation process may reveal significant errors or inaccuracies in model development or outcomes that consistently fall outside the bank's predetermined thresholds of acceptability. In such cases, model adjustment, recalibration, or redevelopment is warranted. Adjustments and recalibration should be governed by the principle of conservatism and should undergo independent review.

Material changes in model structure or technique, and all model redevelopment, should be subject to validation activities of appropriate range and rigor before implementation. At times banks may have a limited ability to use key model validation tools like back-testing or sensitivity analysis for various reasons, such as lack of data or of price observability. In those cases, even more attention should be paid to the model's limitations when considering the appropriateness of model usage, and senior management should be fully informed of those limitations when using the models for decision making. Such scrutiny should be applied to individual models and models in the aggregate.

Validation of Vendor and Other Third-Party Products

The widespread use of vendor and other third-party products—including data, parameter values, and complete models—poses unique challenges for validation and other model risk management activities because the modeling expertise is external to the user and because some components are considered proprietary. Vendor products should nevertheless be incorporated into a bank's broader model risk management framework following the same principles as applied to in-house models, although the process may be somewhat modified.

As a first step, banks should ensure that there are appropriate processes in place for selecting vendor models. Banks should require the vendor to provide developmental evidence explaining the product components, design, and intended use, to determine whether the model is appropriate for the bank's products, exposures, and risks. Vendors should provide appropriate testing results that show their product works as expected. They should also clearly indicate the model's limitations and assumptions and where the product's use may be problematic. Banks should expect vendors to conduct ongoing performance monitoring and outcomes analysis, with disclosure to their clients, and to make appropriate modifications and updates over time.

Banks are expected to validate their own use of vendor products. External models may not allow full access to computer coding and implementation details, so the bank may have to rely more on sensitivity analysis and benchmarking. Vendor models are often designed to provide a range of capabilities and so may need to be customized by a bank for its particular circumstances. A bank's customization choices should be documented and justified as part of validation. If vendors provide input data or assumptions, or use them to build models, their relevance for the bank's situation should be investigated. Banks should obtain information regarding the data used to develop the model and assess the extent to which that data is representative of the bank's situation. The bank also should conduct ongoing monitoring and outcomes analysis of vendor model performance using the bank's own outcomes.

Systematic procedures for validation help the bank to understand the vendor product and its capabilities, applicability, and limitations. Such detailed knowledge is necessary for basic controls of bank operations. It is also very important for the bank to have as much knowledge in-house as possible, in case the vendor or the bank terminates the contract for any reason, or if the vendor is no longer in business. Banks should have contingency plans for instances when the vendor model is no longer available or cannot be supported by the vendor.

VI. GOVERNANCE, POLICIES, AND CONTROLS

Developing and maintaining strong governance, policies, and controls over the model risk management framework is fundamentally important to its effectiveness. Even if model development, implementation, use, and validation are satisfactory, a weak governance function will reduce the effectiveness of overall model risk management. A strong governance framework provides explicit support and structure to risk management functions through policies defining relevant risk management activities, procedures that implement those policies, allocation of resources, and mechanisms for evaluating whether policies and procedures are being carried out as specified. Notably, the extent and sophistication of a bank's governance function is expected to align with the extent and sophistication of model usage.

Board of Directors and Senior Management

Model risk governance is provided at the highest level by the board of directors and senior management when they establish a bank-wide approach to model risk management. As part of their overall responsibilities, a bank's board and senior management should establish a strong model risk management framework that fits into the broader risk management of the organization. That framework should be grounded in an understanding of model risk—not just for individual models but also in the aggregate. The framework should include standards for model development, implementation, use, and validation.

While the board is ultimately responsible, it generally delegates to senior management the responsibility for executing and maintaining an effective model risk management framework. Duties of senior management include establishing adequate policies and procedures and ensuring compliance, assigning competent staff, overseeing model development and implementation, evaluating model results, ensuring effective challenge, reviewing validation and internal audit findings, and taking prompt remedial action when necessary. In the same manner as for other major areas of risk, senior management, directly and through relevant committees, is responsible for regularly reporting to the board on significant model risk, from individual models and in the aggregate, and on compliance with policy. Board members should ensure that the level of model risk is within their tolerance and direct changes where appropriate. These actions will set the tone for the whole organization about the importance of model risk and the need for active model risk management.

Policies and Procedures

Consistent with good business practices and existing supervisory expectations, banks should formalize model risk management activities with policies and the procedures to implement them. Model risk management policies should be consistent with this guidance and also be commensurate with the bank's relative complexity, business activities, corporate culture, and overall organizational structure. The board or its delegates should approve model risk management policies and review them annually to ensure consistent and rigorous practices across the organization. Those policies

should be updated as necessary to ensure that model risk management practices remain appropriate and keep current with changes in market conditions, bank products and strategies, bank exposures and activities, and practices in the industry. All aspects of model risk management should be covered by suitable policies, including model and model risk definitions; 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 should emphasize testing and analysis, and promote the development of targets for model accuracy, standards for acceptable levels of discrepancies, and procedures for review of and response to unacceptable discrepancies. They should include a description of the processes used to select and retain vendor models, including the people who should be involved in such decisions.

The prioritization, scope, and frequency of validation activities should be addressed in these policies. They should establish standards for the extent of validation that should be performed before models are put into production and the scope of ongoing validation. The policies should also detail the requirements for validation of vendor models and third-party products. Finally, they should require maintenance of detailed documentation of all aspects of the model risk management framework, including an inventory of models in use, results of the modeling and validation processes, and model issues and their resolution.

Policies should identify the roles and assign responsibilities within the model risk management framework with clear detail on staff expertise, authority, reporting lines, and continuity. They should also outline controls on the use of external resources for validation and compliance and specify how that work will be integrated into the model risk management framework.

Roles and Responsibilities

Conceptually, the roles in model risk management can be divided among ownership, controls, and compliance. While there are several ways in which banks can assign the responsibilities associated with these roles, it is important that reporting lines and incentives be clear, with potential conflicts of interest identified and addressed.

Business units are generally responsible for the model risk associated with their business strategies. The role of model owner involves ultimate accountability for model use and performance within the framework set by bank policies and procedures. Model owners should be responsible for ensuring that models are properly developed, implemented, and used. The model owner should also ensure that models in use have undergone appropriate validation and approval processes, promptly identify new or changed models, and provide all necessary information for validation activities.

Model risk taken by business units should be controlled. The responsibilities for risk controls may be assigned to individuals, committees, or a combination of the two, and include risk measurement, limits, and monitoring. Other responsibilities include managing the independent validation and review process to ensure that effective challenge takes place. Appropriate resources should be assigned for model validation and for guiding the scope and prioritization of work. Issues and problems identified through validation and other forms of oversight should be communicated by risk-control staff to relevant individuals and business users throughout the organization, including senior management, with a plan for corrective action. Control staff should have the authority to restrict the use of models and monitor any limits on model usage. While they may grant exceptions to typical procedures of model validation on a temporary basis, that authority should be subject to other control mechanisms, such as timelines for completing validation work and limits on model use.

Compliance with policies is an obligation of model owners and risk-control staff, and there should be specific processes in place to ensure that these roles are being carried out effectively and in line with policy. Documentation and tracking of activities surrounding model development, implementation, use, and validation are needed to provide a record that makes compliance with policy transparent.

Internal Audit

A bank's internal audit function should assess the overall effectiveness of the model risk management framework, including the framework's ability to address both types of model risk described in Section III, for individual models and in the aggregate. Findings from internal audit related to models should be documented and reported to the board or its appropriately delegated agent. Banks should ensure that internal audit operates with the proper incentives, has appropriate skills, and has adequate stature in the organization to assist in model risk management. Internal audit's role is not to duplicate model risk management activities. Instead, its role is to evaluate whether model risk management is comprehensive, rigorous, and effective. To accomplish this evaluation, internal audit staff should possess sufficient expertise in relevant modeling concepts as well as their use in particular business lines. If some internal audit staff perform certain validation activities, then they should not be involved in the assessment of the overall model risk management framework.

Internal audit should verify that acceptable policies are in place and that model owners and control groups comply with those policies. Internal audit should also verify records of model use and validation to test whether validations are performed in a timely manner and whether models are subject to controls that appropriately account for any weaknesses in validation activities. Accuracy and completeness of the model inventory should be assessed. In addition, processes for establishing and monitoring limits on model usage should be evaluated. Internal audit should determine whether procedures for updating models are clearly documented, and test whether those procedures are being carried out as specified. Internal audit should check that model owners and control groups are meeting documentation standards, including risk reporting. Additionally, internal audit should perform assessments of supporting operational systems and evaluate the reliability of data used by models.

Internal audit also has an important role in ensuring that validation work is conducted properly and that appropriate effective challenge is being carried out. It should evaluate the objectivity, competence, and organizational standing of the key validation participants, with the ultimate goal of ascertaining whether those participants have the right incentives to discover and report deficiencies. Internal audit should review validation activities conducted by internal and external parties with the same rigor to see if those activities are being conducted in accordance with this guidance.

External Resources

Although model risk management is an internal process, a bank may decide to engage external resources to help execute certain activities related to the model risk management framework. These activities could include model validation and review, compliance functions, or other activities in support of internal audit. These resources may provide added knowledge and another level of critical and effective challenge, which may improve the internal model development and risk management processes. However, this potential benefit should be weighed against the added costs for such resources and the added time that external parties require to understand internal data, systems, and other relevant bank-specific circumstances.

Whenever external resources are used, the bank should specify the activities to be conducted in a clearly written and agreed-upon scope of work. A designated internal party from the bank should be able to understand and evaluate the results of validation and risk-control activities conducted by external resources. The internal party is responsible for: verifying that the agreed upon scope of work has been completed; evaluating and tracking identified issues and ensuring they are addressed; and making sure that completed work is incorporated into the bank's overall model risk management framework. If the external resources are only utilized to do a portion of validation or compliance work, the bank should coordinate internal resources to complete the full range of work needed. The bank should have a contingency plan in case an external resource is no longer available or is unsatisfactory.

Model Inventory

Banks should maintain a comprehensive set of information for models implemented for use, under development for implementation, or recently retired. While each line of business may maintain its own inventory, a specific party should also be charged with maintaining a firm-wide inventory of all models, which should assist a bank in evaluating its model risk in the aggregate. Any variation of a model that warrants a separate validation should be included as a separate model and cross-referenced with other variations.

While the inventory may contain varying levels of information, given different model complexity and the bank's overall level of model usage, the following are some general guidelines. The inventory should describe the purpose and products for which the model is designed, actual or expected usage, and any restrictions on use. It is useful for the inventory to list the type and source of inputs used by a given model and underlying components (which may include other models), as well as model outputs and their intended use. It should also indicate whether models are functioning properly, provide a description of when they were last updated, and list any exceptions to policy. Other items include the names of individuals responsible for various aspects of the model development and validation; the dates of completed and planned validation activities; and the time frame during which the model is expected to remain valid.

Documentation

Without adequate documentation, model risk assessment and management will be ineffective. Documentation of model development and validation should be sufficiently detailed so that parties unfamiliar with a model can understand how the model operates, its limitations, and its key assumptions. Documentation provides for continuity of operations, makes compliance with policy transparent, and helps track recommendations, responses, and exceptions. Developers, users, control and compliance units, and supervisors are all served by effective documentation. Banks can benefit from advances in information and knowledge management systems and electronic documentation to improve the organization, timeliness, and accessibility of the various records and reports produced in the model risk management process.

Documentation takes time and effort, and model developers and users who know the models well may not appreciate its value. Banks should therefore provide incentives to produce effective and complete model documentation. Model developers should have responsibility during model development for thorough documentation, which should be kept up-to-date as the model and application environment changes. In addition, the bank should ensure that other participants in model risk management activities document their work, including ongoing monitoring, process verification, benchmarking, and outcomes analysis. Also, line of business or other decision makers should

document information leading to selection of a given model and its subsequent validation. For cases in which a bank uses models from a vendor or other third party, it should ensure that appropriate documentation of the third-party approach is available so that the model can be appropriately validated.

Validation reports should articulate model aspects that were reviewed, highlighting potential deficiencies over a range of financial and economic conditions, and determining whether adjustments or other compensating controls are warranted. Effective validation reports include clear executive summaries, with a statement of model purpose and an accessible synopsis of model and validation results, including major limitations and key assumptions.

VII. CONCLUSION

This document has provided comprehensive guidance on effective model risk management. Many of the activities described in this document are common industry practice. But all banks should confirm that their practices conform to the principles in this guidance for model development, implementation, and use, as well as model validation. Banks should also ensure that they maintain strong governance and controls to help manage model risk, including internal policies and procedures that appropriately reflect the risk management principles described in this guidance. Details of model risk management practices may vary from bank to bank, as practical application of this guidance should be commensurate with a bank's risk exposures, its business activities, and the extent and complexity of its model use.