FEDERAL HOUSING FINANCE AGENCY

ADVISORY BULLETIN

AB 2013-07

Model Risk Management Guidance

Purpose

This advisory bulletin replaces Federal Housing Finance Agency Advisory Bulletin 2009-AB-03 (*Validation and Documentation of Models and Related Controls on Internal Processes*). The earlier advisory bulletin provided guidance on model risk management for the Federal Home Loan Bank (FHLBank) System. This guidance's scope includes Fannie Mae and Freddie Mac in addition to the FHLBanks and the Office of Finance (collectively, the Regulated Entities).[1] A Regulated Entity's model risk management framework should reflect the entity's size, complexity and extent of model use and level of risk exposure. Large, complex entities that develop their own models should have an appropriately rigorous framework in place. Both Fannie Mae and Freddie Mac are considered to be large, complex enterprises for purposes of this bulletin. As less complex entities, based on the current extent and scale of their model development, the FHLBanks should have a framework that is commensurate with their model use and risk exposure.

This advisory bulletin sets the minimum thresholds, based on the extent and scale of each Regulated Entity's model development, for the Federal Housing Finance Agency's supervisory expectations for model risk management by outlining the framework of baseline control and governance requirements. This bulletin is intended to be applied using a risk-based approach to models, model-based applications, modeling processes and significant end-user computing tools that are used to help make key business and financial decisions. Regulated Entities should apply the same principles outlined in this advisory bulletin to internally-developed and vendor-provided models, whether used and managed in-house or externally by a vendor.

This advisory bulletin draws on FHFA's supervisory experience at the Regulated Entities and is consistent with related guidance issued by other federal financial regulatory agencies.[2]

[1] Although the Office of Finance is not a "regulated entity" as the term is defined in the Federal Housing Enterprises Financial Safety and Soundness Act of 1992, as amended, for purposes of convenience, this advisory bulletin includes the Office of Finance when referring to the Regulated Entities collectively, unless otherwise noted.

[2] Board of Governors of the Federal Reserve System and Office of the Comptroller of the Currency. *Supervisory Guidance on Model Risk Management.* OCC 2011-12 (April 4, 2011).

Background and Key Points

The Regulated Entities use models in a variety of areas including but not limited to financial instrument valuation, compliance, capital reserves measurement, loss allowance, financial reporting, and market and credit risk measurement and control. Although models are often essential, reliance on inaccurate or inappropriate models may lead to poor or costly decisions.

Effective risk-based model risk management entails a comprehensive approach in identifying risk throughout the model lifecycle. A Regulated Entity should embed a risk management framework in its policies, procedures, roles and responsibilities of model stakeholders, and a well-coordinated committee structure. This framework promotes periodic monitoring and reporting of model risk horizontally and vertically across a Regulated Entity. It envisions the placement of stronger process control where risk arises; an appropriate organizational structure to promote transparency of risk; an independent model risk management group; and clear direction from a Regulated Entity's compliance units, senior management, and its board of directors (the board). The board's risk committee sets the model risk appetite at the corporate level. Model stakeholders including model users, developers, owners, and oversight groups should have clear accountabilities to promote compliance with model risk limits and management guidelines.

This framework incorporates recent trends in model risk management. Specifically, it adopts the practice of managing inherent model risk at the source – the assignment of model risk management responsibilities to model developers, owners and users. Also, the framework expands the risk management group's role from one solely performing validation activities to one that is more proactive in risk identification and measurement. Additionally, the framework recommends that the board and senior management exercise oversight through working groups and committees. Working groups and management committees provide model stakeholders forums in which to discuss model issues and approve mitigating actions. The framework likewise expands the assurance function of internal audit in large, complex enterprises to include continuous monitoring of model controls and an enhanced ability to review the effectiveness of the validation function. For less complex entities, internal audit's role could be more limited and focus on compliance with relevant policies and procedures.

Critical to the success of managing model risk is full ownership by model developers, owners and users of the responsibilities of managing risk consistent with the view that model risk is a risk management responsibility rather than a compliance obligation. Model risk is best managed at its source through a structured and disciplined approach in model development, testing, implementation, validation, and use. This is executed through a formalized control framework with a highly specific set of control procedures and standards present through the model lifecycle. Model owners and developers manage risk through proper development and implementation of models in accordance with these guidelines. Similarly, the model user takes guidance from specific control procedures to ensure that the model is used appropriately and all manner of model use is

reported and inventoried. Examples of control guidelines include model documentation standards, model performance standards, model change and control procedures, and technical model development standards to guide model implementation.

An independent model risk management group provides a secondary layer of control by identifying and measuring residual model risk via its model validation, periodic review, and ongoing monitoring activities.

Senior management and the board perform vital governance and oversight functions through their review and approval of proposed remediation or mitigation approaches. Management committees provide the appropriate forums where corporate model strategies are discussed and management approves short-term model risk mitigation actions and longer-term model risk remediation approaches. At large, complex enterprises, internal audit assesses the design and effectiveness of the overall model risk management framework through its model and business process audits and its assessment of the validation function's effectiveness.

In establishing this framework, senior management should ensure that roles and responsibilities are clear and that model risk issues are identified and reported horizontally and vertically across a Regulated Entity. Clear accountability is needed to ensure that model stakeholders have the proper incentives to manage their respective risk areas.

Senior management should create an appropriate organizational structure to promote effective organizational challenge of models. Key elements of having effective organizational challenge to models include findings management, performance tracking, reporting, and an escalation process. The independent validation group should be adequately staffed and have the requisite skills and experience to assess the conceptual design of the modeling approach. Model risk should be transparent and reported to the board and senior management. Remedial actions should be timely and escalation procedures clear. All stakeholders, including modelers, model users and independent validators, should participate actively to influence model development planning and prioritization. The support of senior management and the board is vital in promoting a culture of collaborative model risk awareness across a Regulated Entity.

Regulated Entities should customize their model risk management framework based on the extent and complexity of model use and their level of risk exposure. Large, complex enterprises that develop their own models should have a more rigorous and extensive framework in place. Less complex and smaller entities should design their framework to ensure minimum supervisory requirements are met in a cost-effective manner.

Federal Housing Finance Agency Model Risk Management Guidance
Table of Contents

Definition of Model and Model Risk

Model Universe

Models, model-based applications, modeling processes, and significant end-user computing tools (EUCs) are included in the model universe for the purposes of this advisory bulletin, which will refer to them collectively as "models" in the remaining narrative, unless stated otherwise.

The term modeling refers to an activity in which a model is used to calculate an output based on a set of assumptions, theories or system of postulates and data that are not axiomatically correct. Current regulatory guidance defines a model as a quantitative methodology or approach using statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates.[3] Financial and economic models are approximations of real-world phenomena or future events using mathematical techniques and statistical methods. Models derive quantitative estimates of causal relationships or correlations between input data and the measured output. The same estimation or calculation techniques using qualitative assumptions are also models for purposes of this guidance. Model use is defined as using a model's output as a key basis for informing business decision-making, managing risk or developing financial reports.

A model-based application is software that integrates various component models and their input data to produce quantitative estimates. A modeling process is a composite set of models, modeling activities, EUCs, management judgment or qualitative adjustments of model outputs by business units to produce quantitative estimates for business decision-making, financial reporting or risk measurement (e.g., loss allowances or capital reserves). In determining whether a modeling process must be included under the institution's framework for managing model risk, senior management should take into account the significance and the consequence of its use from a financial, legal, and reputational risk perspective, or whether it impacts a significant balance sheet item for financial reporting purposes.

The Regulated Entities should consider significant or important EUCs as models for purposes of this advisory bulletin. Examples of these EUCs include applications that directly tie to model performance, financial reporting, corporate loss forecasts, securitizations, home price appreciation, interest rate projections, and economic capital.

Models can also be defined by their state of existence, such as active, active-superseded, and limited-use excepted models. An active model refers to the current version of a model in use. Active-superseded models are previous versions of component models that remain temporarily in use in other modeling applications due to operational constraints until a newer version can be put into production. This usually occurs in large, complex enterprises, and additional controls and

[3] OCC 2011-12.

closer monitoring of the model output should be used for this temporary solution. Limited-use excepted models are put into production for a specifically approved application pending completion of a full independent model validation, and should have a detailed analysis and proper approval prior to implementation.

The board or its delegated representative retains the final decision-making authority in determining the model universe as outlined above. Corporate policies should provide clear guidance on the scope of the model universe with specific examples as necessary.

Model Risk

This advisory bulletin defines model risk as the risk of loss resulting from model errors or the incorrect use or application of model output. Economic models are fundamentally uncertain or imprecise because they are imperfect representations of real-world phenomena. How well a model captures real life events is an indication of model risk. Uncertainty in financial models, for example, sometimes results from attempts to quantify human emotion or expectations in decision making. Model risk can be diminished but not entirely eliminated.

Model errors come from various sources. Errors in theoretical formulation and conceptual design originate from flawed logic or assumptions, model misspecification or omission of variables. Data quality issues, inadequate sample sizes and stale data contribute to model performance issues such as instability, inaccuracy or bias in model forecasts. Model risk also arises from inadequate controls over model use. Examples include unreported models resulting in unmeasured model risk, unapproved model use, improperly used models, and inadequate understanding of model uncertainty or limits. Faulty development and implementation in software systems, incorrect application, and unapproved on-top adjustments and overrides can lead to model control issues and errors. Flawed test procedures or failure to perform thorough and extensive user acceptance tests can lead to significant model risk. Underperforming models, and those with long outstanding findings, create model risk as well. It is important to recognize that even appropriately applied and correctly used models can produce model errors and that perfectly accurate model results can be misapplied or misused. The potential for errors coming from various sources necessitates an all-encompassing model risk management framework requiring prudent management and oversight.

Model error may lead to financial, legal, regulatory and reputational risk. Consequences can include incorrect business decisions, ineffective management of risk, suboptimal levels of capital and loss reserves, and inadequate or inaccurate financial reporting.

Model Risk Management Framework

A comprehensive framework for managing model risk across a Regulated Entity relies on good governance and oversight by the board and senior management; a formalized control framework to

ensure disciplined model development, implementation, and use; and effective model risk identification and measurement for short-term mitigation and longer-term remediation. This framework is implemented through corporate policies and procedures and by assigning clear roles and responsibilities for managing model risk. It is vital for a Regulated Entity to understand how well models are being applied strategically and how they are performing in practice. Such a framework is designed to ensure that every model is developed and used to maximize the operational impact to make better business decisions.

Most of the Regulated Entities have established an enterprise risk management group, including an independent model risk oversight function reporting to the chief risk officer (CRO). Regardless of the organizational structure, the board should provide overall guidance for managing model risk, ensure that a Regulated Entity operates within approved tolerance levels, and direct changes when appropriate. The board and senior management provide direct oversight over models in various business applications or indirectly via committees. An effective reporting structure ensures that model risk information flows vertically and horizontally across the organization and committee structure.

Formal, written policies codify management's approach towards managing model risk. Model policies should specify the roles and responsibilities of stakeholders, reporting lines, delegations of authority, and accountability. A documented and approved model control framework (as described below) provides specific control procedures for model development, implementation, and use. Model owners and users manage risk at its source, and the model risk management group independently measures and validates the effectiveness of model risk mitigation and remediation strategies. A Regulated Entity's corporate culture, reporting structure, findings management, and escalation processes should allow for an effective organizational challenge of models. Model interactions and dependencies, reliance on common data or methodologies, and other factors that can adversely affect models and their outputs all impact aggregate model risk. All models should be properly identified along with their business use and risk to the organization for effective model inventory management.

The following sections in this advisory bulletin elaborate on regulatory expectations regarding implementation of the above framework. Further sections discuss corporate policies and procedures, roles and responsibilities of key stakeholders, governance and key controls, effective model validation, and minimum requirements for model development and documentation.

Policies & Procedures

Each Regulated Entity should have a board-level model policy (self-standing or part of a broader document) that describes its model risk framework and sets its model risk appetite commensurate with the organization's complexity, business activities, and overall organizational structure. The model policy should define what qualifies as a model, model-based application, modeling process

or significant EUC. The policy should define how to classify a model based on purpose, use and related importance to a Regulated Entity's financial statements, financial disclosures, risk management, or decision making. Furthermore, the model policy should identify individual roles within the model risk governance framework and assign responsibilities to the business units and risk oversight for the development and maintenance of each model. The designation of responsibilities should clearly indicate the parties responsible for reviewing and approving models as well as significant changes to models. In addition, parties should be identified as responsible for evaluating the model's output (e.g., risk metrics), inputs (e.g., data inputs and assumptions), and any manipulation of the output that goes into final reports.

Senior management should supplement board-level policies with more granular policies and procedures depending on the degree and complexity of model use. The board and/or its delegates should review and approve model risk management policies on an annual basis. Policies should cover all aspects of model risk management including the definition and classification of models; assessment of model risk; acceptable practices for model development, testing, implementation, use, and effective challenge; appropriate model validation activities; and oversight and controls over the model risk management process.

Policies and procedures should provide clear guidelines for developing model classifications or risk rankings. A model's complexity, business impact and the extensiveness of use generally determine its risk ranking or classification. In large, complex enterprises, the model risk management group and internal audit should harmonize their model risk rankings to achieve consistency.

Entities should have sufficient policies, procedures and documentation encompassing the entirety of model lifecycle to facilitate effective model development, validation, implementation, use, and retirement. The level of prioritization, scope, frequency, and documentation of validation activities should be commensurate with the relative importance of a model to a Regulated Entity's decision making or risk management processes. Policies should ensure that all new models have a development plan, including a process for selecting and retaining vendor models, and implementation procedures with appropriate threshold and testing requirements.

Policies should establish a model validation program (as described below) to promote validation and monitoring activities. If a Regulated Entity uses external resources for validation and compliance functions, it should have policies that outline controls around external resources and detail how it will integrate the contracted work into its model risk management oversight.

Management should fully document, test, validate, and approve a model before it enters production. Policies should provide guidance on mitigating limited but allowable exceptions to full validation prior to implementation, required pre-production approvals, and any additional control procedures. The policies should also detail the validation requirements for vendor models and third-party products. In cases where a vendor model is used, prior to relying on a vendor's model

results, the vendor should provide its independent model validation results if available, and the Regulated Entity should test its own internal processes surrounding the use of the model. Policies should also ensure regular confirmation that vendors are updating their models at an appropriate frequency to reflect relevant changes in market conditions and material developments in the financial engineering field.

Policies should establish change control procedures for implementing significant changes and updates to models. Significant model changes may require a model validation. Policies and procedures should emphasize testing, ongoing monitoring and analysis, and promote the establishment of model accuracy standards and thresholds for acceptable levels of discrepancies. Procedures should entail the review of and response to unacceptable discrepancies. Policies should ensure that model results, whether produced by vendors or internally, are regularly benchmarked against results from alternative sources as possible. Policies and procedures should also address the decommissioning or replacement of models.

Policies should also address the retention and safekeeping of model inputs, model documentation, model results, and validation reports. Policies should clearly lay out the responsibilities of business units and those individuals responsible for ensuring adherence to procedures and processes governing documentation, change control, and validation.

A Regulated Entity should update policies and procedures as necessary to ensure that model risk management practices remain relevant and applicable to changing business practices, products, strategies, and risk exposures, and changing market conditions and industry practices.

Roles & Responsibilities

The following describes roles and responsibilities for key model stakeholders in managing model risk. A general overview of model stakeholders follows, but may differ slightly across the Regulated Entities. A Regulated Entity should establish a model risk management framework to meet minimum model supervisory requirements and provide maximum benefit within cost conscientious parameters.

Board of Directors

The board and its designated committee(s) provide the tone from the top related to oversight and governance of risk at a Regulated Entity. Board policies set risk appetite, reporting requirements, and clear delegations of authority. The board should regularly receive reports on the aggregate level, direction, and management of salient and emerging model risk issues.

Chief Risk Officer

The CRO generally owns and approves all model risk policies, standards and procedures, and chairs the primary model risk oversight committee tasked with overseeing enterprise-wide model risk issues. The CRO should provide regular reports on model risk issues and performance metrics to the board. The CRO is responsible for providing the board an aggregate view of the level and direction of model risk. For less complex entities, the CRO could delegate some of their model risk management responsibilities to other qualified personnel from within the institution.

Model Owner

Each model should have a designated owner who is primarily accountable for its development and implementation throughout its lifecycle.[4] The owner plays a key role both in managing model risk at its source and in the ongoing monitoring and mitigation of that risk. The owner's key responsibility is to ensure that the model is appropriately developed and used for its intended business purpose. The owner's primary duties include maintaining adequate documentation, testing, and developing model performance benchmarks and thresholds to ensure continued robust performance as market conditions change.

On an ongoing basis, the owner is primarily responsible for monitoring model performance in its specific business application and making on-top adjustments to mitigate persistent model underperformance in the short term. Annually, the owner should assess and attest to the performance of the model. The model owner should initiate prompt remediation to model findings and breaches in model performance thresholds. Owners should produce regular reports to inform management and the oversight group of any model performance issues.

Model User

The model user plays a key role both in managing model use risk and in the ongoing monitoring and mitigation of model risk. The user is primarily responsible for appropriate testing and use of the model or its output within business processes or in decision-making. The user takes responsibility for using correct input data and should fully understand how the data was developed and its proper application in the model. The model user should employ a model for its intended purpose and obtain the necessary approval when considering a specific use for another business application. The model user should also participate in user acceptance tests of new model implementations.

On an ongoing basis, the model user should raise model performance issues and initiate change requests when needed. Model users perform vital stewardship functions by ensuring the model

[4] The model owner could be either the developer or primary model user at some of the Regulated Entities.

remains current and outstanding validation and audit findings are addressed in a timely manner. Model users should vet on-top model adjustments with business unit management and oversight committees.

Model Risk Management Group

The model risk management group functions as the second layer of control in managing model risk through its independent validation of models, periodic reviews, assessments, and continuous monitoring of model risk. Depending on a Regulated Entity's organizational structure, staff from several groups, such as model validation, operations risk, enterprise risk management, and business unit risk officers, may handle the responsibilities of model risk management. Traditionally, the central role of the risk management group has been the independent validation of models. The group's role should also include risk identification and measurement and the provision of an independent review and approval of model performance metrics. Annually, the model risk management group should review and assess the risk classifications and outstanding findings of all models in the institution's inventory. The model risk management group may initiate additional targeted validation work or may enhance or modify risk mitigants in place based on the results of this assessment.[5]

The model risk management group should actively participate in various working groups and management committees to capture model information from a variety of sources. In less complex entities, the model risk management group should participate in working group and management committee meetings relevant to addressing model risk issues. Any identified risk may trigger a targeted validation, review, mitigation or remediation. The model risk management group should ensure proper maintenance of model and model use inventories and validation of models according to approved schedules. In large, complex enterprises, this includes the development of an annual validation plan which helps to facilitate resource management, workforce planning and scheduling. The plan enables the CRO to assess the validation group's performance against measurable targets in its annual performance review.

An effective model risk management group should be staffed with the appropriate skill sets. The validation group should have appropriate technical modeling skill sets to independently validate conceptual and theoretical model designs. It should also have the right complement of business analytics, project management and planning abilities for effective reporting, continuous monitoring of model risk issues, and findings management. In large, complex enterprises, risk officers may be embedded in business units to enhance understanding of model use in a specific business context.

[5] Some examples of actions include on-top adjustments, more frequent performance monitoring or reporting, limited model use, or lower risk limits.

Internal Audit

Internal audit functions as another control layer in the model risk management framework. In large, complex entities, internal audit evaluates the overall effectiveness of the model risk management framework. In less complex entities, internal audit would primarily focus on evaluating compliance by model owners and users with policies and procedures that specify control activities for model development, implementation, and use. In large complex entities, internal audit should also have the ability to validate model performance and risk management effectiveness.

A Regulated Entity that develops models internally and uses them extensively usually maintains a specialized model audit group. Less complex entities that generally do not develop their own models may choose not to have such a group within internal audit. This group should have adequate experience and skills to independently conduct individual model audits as well as assess the adequacy of technical model validations. This specialized model review group within internal audit should submit an annual audit plan to the audit committee. The plan should include both its targeted audits of high impact models and support activities on integrated business process audits with model or modeling process components. Targeted model audits evaluate and test the design and operating effectiveness of model validation and controls for model development and implementation. Business process audits evaluate the design adequacy and effectiveness of model process controls. Audits of other business processes may identify model-related risk, such as deficiencies in information technology (IT) system controls around certain models. The model audit group should collaborate with the model validation group to develop a common set of model risk rankings or categories.

A Regulated Entity may utilize external audit resources to provide additional capacity for reviews. Such resources should be able to provide reviews independent from a Regulated Entity's model development and implementation.

Committees

Management committees and working groups provide the model stakeholders a forum to discuss model risk issues and remediation actions. A management-level model risk committee provides a forum for the reporting and aggregation of all model risk issues. This in turn facilitates analysis by and direction from senior management. Committee agenda items include corporate model strategy and model development, planning, and prioritization. This committee is also the final escalation point for outstanding model risk issues before formal elevation to the board.

Specialized committees such as valuation, asset-liability management, financial reporting, market risk, credit risk, and loss allowance and reserve committees discuss and approve short-term mitigants and longer-term remediation plans for model use risk. For example, a model user's proposed on-top adjustments to address model performance issues in the interim are reviewed and

approved by senior management pending a longer-term solution that may entail re-specifying a model. In the model risk management framework discussed above, committees and business unit working groups provide the crucial information linkages that allow for vertical and horizontal reporting of model risk issues across a Regulated Entity on an ongoing basis. Each committee's charter should outline its responsibilities with respect to the models under its authority.

Working groups may be formed on a permanent or ad-hoc basis. Regardless of specific form, senior management should create minimum standards and expectations on working group processes, reports and results. Although a degree of variability is expected in terms of the scope and agenda items of various working groups, a minimum level of standardization should be established to promote effective working groups.

Information Technology (IT)

The IT department of a Regulated Entity should establish a model-related IT infrastructure and control process. This IT process should ensure an environment in which models function properly and take full advantage of their capabilities. The control process should include at minimum data integrity, hardware, security, and version control. Automation and technological innovation helps improve model performance and a Regulated Entity's ability to efficiently govern modeling. Model platforms employed should provide an optimal number of servers and central processing units as well as an appropriate setup for distributing processing to maximize performance. Models can exist in many areas and be embedded in larger information systems. Data can flow from various sources. Coordinating the input, output, and aggregation of data flows is essential to ensuring data and reporting integrity. IT should also ensure that it creates adequate, completely segregated environments for model testing and production in order to prevent inadvertent changes to critical data used in decision making processes. A Regulated Entity should ensure coordination between business units and IT departments to ensure proper implementation and ongoing use of models and effective systems integration.

Model Control Framework

Model owners, developers, and users should provide the primary control for model risk. To facilitate this, a Regulated Entity needs a formalized model development and implementation control framework. Model documentation standards, security, change, and version controls, performance tracking, data integrity, and technical model development standards are all essential to achieving a structured, disciplined approach to model development, implementation, and use. Senior management, the model risk management group and committees generally provide a second layer of controls. Model inventory management, periodic assessments, model validations, risk measurement, limits and on-going model risk monitoring are all necessary to actively manage model risk in the organization. These controls aid in the model risk identification and measurement process and allow a Regulated Entity to address individual and aggregate model risk.

Model risk controls should be embedded in policies, procedures, and the roles and responsibilities of all stakeholders. Described below are some key controls in greater detail.

Model Inventory Management

A Regulated Entity should maintain a comprehensive inventory listing models implemented for use, under development, or recently retired, and update the inventory at least on a quarterly basis. A Regulated Entity should classify or risk rank each listed model based on its inherent risk as driven by its factors such as its purpose, extent of use, and relative impact to financial statements, financial disclosures, risk management, or decision making. The FHLBanks may differentiate between mission critical, significant, and other models.

The inventory should include all models that affect risk management, business decisions, and financial statements and disclosures. Model inventory management includes internally developed models, vendor models, and models shared with another Regulated Entity(ies). The model inventory captures the key attributes of a model including its use, purpose, classification, owner, governance committee, last update, and validation schedule. The inventory should also include the source of inputs (including other models) as well as model outputs. For vendor models, the model inventory should identify the version number of the model in use as well as the latest version of the model available in the marketplace.

For large, complex enterprises, the model inventory should include major assumptions, key sensitivities, performance thresholds, and significant adjustments for each model. In addition, large, complex enterprises should maintain a model use inventory which lists all upstream and downstream applications of core or component models. A model use inventory necessitates an up-to-date model interdependencies diagram or chart.

Change & Version Control Management

Each Regulated Entity should have robust model change controls in place with policies and procedures that clearly define the roles and responsibilities of all interested parties. Only approved parties should alter a model's code. Each model should have a change control log that states when the model was changed, the nature of the change, who was responsible for the change, and who approved the change, as applicable. The change control log is a document that allows others to clearly understand a model's function its and settings, and aid in its auditing. A Regulated Entity should validate and approve all significant model changes according to its policies and procedures prior to deployment into production. The model's governance authority should define and establish applicable threshold levels which determine what constitutes a significant model change.

Model Performance Tracking

Each Regulated Entity should, at least on a quarterly basis, monitor the performance of its mission-critical or high-risk models. Performance monitoring should use thresholds approved at least on an annual basis by the model risk management group. The model risk management group should report results of model performance tracking to the relevant model oversight committee(s) and the board on a regular basis.

Model performance tracking consists of routine model backtesting, benchmarking, stress testing, and review of model output reports. If tracking errors exceed thresholds, a Regulated Entity needs to consider whether the implications of those errors present a significant risk to their financial position. If it so determines, the model owners need to decide whether making reasonable adjustments to the model will control or mitigate the problem. If model owners are continually making adjustments to the model based on results, the model may be outdated and require remedies other than adjustments to control or mitigate the problem.

Model backtesting consists of comparing projected model results with actual results. Benchmarking consists of comparing a model's performance metrics to actual information available in the marketplace, where applicable. Stress testing provides a better understanding of how a model reacts to non-typical events. The review of performance results, whether of backtesting, benchmarking or stress testing, is judgmental. Such reviews depend on many factors including the current and legacy conditions a Regulated Entity, the historical time horizon under review, and the variables used in the performance review. Proper analysis of model performance when tracked and measured over time should help provide early warning of potential model issues.

Model Assumptions and Adjustments

Each Regulated Entity should maintain a consolidated list of the major assumptions and adjustments applied to highly risk ranked or classified models. Adjustments include on-top adjustments and model re-calibrations. A Regulated Entity should update this list on a quarterly basis, and the list should be a part of senior management's (and possibly the board's) evaluation of model risk.

A Regulated Entity should have a formalized process for all models to document, validate, and update assumptions, historical inputs, or business scenarios used as model inputs. The process should enable approval, monitoring, and periodic update of model inputs. A Regulated Entity should evaluate assumptions for their appropriateness and reasonableness in light of current business and market conditions as well as other material factors. Assumptions should be supportable and result in accurate estimates of risk. The evaluation of the reasonableness and appropriateness of assumptions should consider prevailing industry practices with regard to the selection of assumptions for similar purposes. The documentation should describe the assumption

or historical input, source used to derive the assumption, owner's responsible for deriving and updating the assumption, frequency of update, and justification (in the case of a subjective assumption). Model owners should provide a clear rationale for their assumptions and should identify, explain, and justify departures from industry practice. Senior management should review assumptions on a regular basis. Vendors who provide modeling services to a Regulated Entity and manage those services off-site (e.g., vendors who model the credit worthiness of advance collateral) should provide enough documentation or descriptions of their modeling assumptions and data sources for the Regulated Entity to compare these to industry standards.

Data Management

Data management refers to both internal and external data sources. Data are critical to a model and should be subject to rigorous analysis. A Regulated Entity should track and assess how it uses similar data from the same or different sources to feed various models. Model development, validation, and ongoing monitoring should include a review of the data and assumptions used as inputs to a model. External data should also be subject to periodic review and where possible checked against alternative sources, such as market, credit, and instrument pricing data.

A Regulated Entity should maintain data management policy, standards, or procedures to establish proper controls and oversight over the extraction, transformation, and output of model data. The policy should establish governance requirements to facilitate independent audit and review of technical documentation, data quality, sampling methodology, programming code quality, and data output. The modeler's technical data document should be of sufficient detail to allow for an independent replication of sampling data used to estimate a model.

Model Validation Program

A Regulated Entity should establish a validation program to identify and measure model risk as well as permit the proper mitigation and remediation of the risk. A Regulated Entity should subject its models to independent validation, monitoring, and periodic reviews and assessments. A model validation program should apply the same principles to internally developed models and vendor-provided models whether used and managed "in-house" by a Regulated Entity or externally by the vendor.

Validation is the process of determining that a model's results accurately meet the requirements of its intended use and that the model is reasonable for use. Model validation typically includes an independent review of the model's logical and conceptual soundness, confirmation of its proper operation, a comparison against competing models, and a comparison of model predictions against subsequent real-world events. Validation should also help model users understand potential weaknesses and limitations of a model.

Independent Model Validation

All models are subject to independent model validation according to the schedule set forth in the model inventory based on model classification or annual validation planning. The frequency and scope of validation should be commensurate with the relative importance of a model to a Regulated Entity's decision-making or risk management processes. The financial costs and consequences associated with the model producing highly inaccurate or unexplainable results should factor into the robustness of the validation. Overall, a model's usage in the business process, its business impact, and its criticality (e.g., high, medium, or low) should drive the vigor of its validation process.

A Regulated Entity should independently validate newly developed models and models that undergo significant changes, as defined or established by model thresholds, prior to deploying the models into production. Exceptions to performing a full model validation prior to implementation may occur under extenuating circumstances provided that the model owner properly documents the reason and the model's governance authority and the CRO approves of the exception. Furthermore, the model owner should provide a detailed analysis for review and approval by the business unit and model risk management group prior to implementation. If an exception occurs, the Regulated Entity should complete an independent model validation within a reasonable time period after implementation. Additional controls and monitoring requirements are needed until the validation is completed. An example is a limited-use excepted model that a large, complex enterprise puts into production for a specifically approved application, pending completion of a full independent model validation. A limited-use excepted model may be put into production before a full validation is completed for reasons such as model errors requiring immediate correction or urgent adoption of regulatory changes in accounting rules.

A Regulated Entity may perform a limited-scope model validation in cases where changes to a model may be isolated. In such cases, they should document the evidence warranting a limited validation. The Regulated Entity should determine what types of changes may trigger a limited scope validation. Some instances that may warrant a limited validation include changes in data flow into and out of a model, changes in model parameters and assumptions, significant changes in the market environment, and modeling of new instruments or products. Furthermore, if a model and its components have not changed, a Regulated Entity may perform a limited validation to meet its scheduled full validation requirement provided that the model still undergoes an annual review or assessment.

Only qualified personnel who demonstrate the necessary knowledge, skills, and experience should carry out model validation. These personnel may be internal staff, external consultants, or a combination of the two. The standards of knowledge, skills, and experience necessary to conduct such reviews tie directly to the model being validated. More complex models may warrant the engagement of third-party experts to supplement internal validations. If a Regulated Entity

employs external consultants in the validation process, management should consider changing consultants or their personnel periodically, such as every three to four years, to ensure client-consultant impartiality. A model validation can be split between more than one validator (e.g., internal staff and external resources) when model validation tasks can be efficiently divided and qualified parties have the expertise and industry experience to perform the validation. When relying on a portion of a model or its results not addressed through joint validation, a Regulated Entity would be responsible for validating any uncovered portions or results.

Model validation reports should include an assessment of the materiality of the findings or recommendations in the reports. Although an overall model validation rating (e.g., satisfactory) can be included in the validation report, it may not indicate whether the model owner can effectively mitigate the identified model's risks and their potential impacts to an acceptable level consistent with the Regulated Entity's model risk tolerance level. Therefore, a Regulated Entity should use caution and not rely solely on model validation report ratings to assess the model risk facing the organization.

For externally managed models, a Regulated Entity should request vendors to provide technical documentation and any available results from their own internal testing. A Regulated Entity should have documentation from a vendor that outlines how a model works as part of its purchasing process. If any information regarding a model comes from discussions with the vendor, then the Regulated Entity should document those discussions. The Regulated Entity should also request regular confirmation from vendors, including third-party pricing services, that they are updating their models at an appropriate frequency to reflect relevant changes in market conditions and/or material developments in the financial engineering field. Vendor documentation should describe its quality assurance and benchmarking practices. Vendor provided information can complete the validation of an externally managed model when paired with a Regulated Entity's internal validation and periodic benchmarking of a model's results against those of other models or calculation methods.

A Regulated Entity should ensure that all mission-critical or significant model validation reports, or a detailed summary of these reports, are provided to senior management and the board (or to the appropriate governance committee of the board) for review. Model validation reports or summaries for less critical models should be reported to senior management and the appropriate management-level governance committee. A Regulated Entity should also make all model validation reports available to examiners and other FHFA personnel.

Elements of an Independent Model Validation

The validators should include, at minimum, the following elements in the independent model validations:

Data and Assumptions

A model validation should include a review of the data and assumptions used as inputs for a model. It also should include a review of the adequacy of the controls in place to ensure the accuracy, integrity, and appropriateness of model inputs. Large, complex enterprises may need to place reliance on data management and control functions for the assessment of data input in certain cases.

Model Theory

A model validation should include an assessment of the statistical, financial, and economic theories underpinning the model. The conceptual review should be evaluated from an empirical, analytical and best-practice perspective. Those responsible for validation should have access to model documentation that contains a clear description of the underlying theory and logic of the model. The validation should include an assessment of whether the theory and logic underlying the model are generally accepted and supportable. The validation should explain the appropriateness of the model for its intended business use. In instances of model failure during the validation process, an explanation should be provided detailing why a model should not be used. For internally-developed models, validation should cover the model development process, including developmental evidence and the pre-implementation phase. With respect to vendor models, the validation should include a review of any vendor information that describes the theory and logic supporting the model and an assessment of whether these are generally accepted and supportable.

Model Code and Mathematics

A model validation should, where possible, examine the model's computer code and mathematical formulae, including calculations performed during data preparation in spreadsheets or other applications external to the primary model, for potential flaws in logic or coding. In the case of proprietary models where vendors will not allow access to computer code and mathematical formulae, a model validation should produce comparable results from alternative models or from mathematical equations that are appropriate for the task.

Model Output Reports

A model validation should include a review of the model's output reports. It should analyze and compare output reports over time to assess their reasonableness and accuracy. Where possible, it should compare output results against those of comparable models or other benchmarks. The model risk management group should establish appropriate tolerance thresholds for differences between the model of record and the benchmark model used for validation purposes. Appropriate performance thresholds may help determine whether valuation differences between the two comparable models identified through an internal independent model validation are reasonable, and

whether differences require further investigation. Where possible, the validation should periodically compare model results to actual results, via back-testing or out-of-sample testing. A model validation should include a review of the adequacy of the audit trail documenting and supporting output reports. This audit trail should provide information on the inputs (data and assumptions) used to generate output reports.

Assessments and Periodic Model Reviews

At least on an annual basis, the model risk management group should conduct a model review, with input from model owners, to determine if risk levels have increased or to identify new emerging risks since the last model validation. Each model owner should be subject to an assessment of the model and a regular attestation as to compliance with model policies and procedures. An annual review consists of an assessment of model performance and any model-related market or industry changes to gauge actual and potential impacts to model risk. This review should be a more streamlined process than a full model validation. The goal of this streamlined review process is to update the risk ratings of models and related findings based on current market conditions and regulations, changes in the application and use of model output, and model performance history and adjustments. The model risk management group should measure the materiality of un-remediated model validation findings and factor these into a model's inherent risk and any aggregated risk information. A Regulated Entity should validate and test for mitigation and/or remediation any elevated risk issues or findings resulting from this assessment. The risk management group may initiate additional targeted validation work or may enhance or modify risk mitigants in place based on the results of this assessment.[6]

Monitoring

Model risk information may originate from sources across a Regulated Entity including audit and regulatory findings, issue tracking reports, model performance tracking, testing activities, and assessments providing useful information to senior management and the board. A Regulated Entity should ensure effective information collection to identify model risk and assess the materiality of such via risk measurement, limits, and ongoing monitoring. Effective monitoring can identify which models need to be updated or replaced. The model risk management group and CRO should play a central role in gathering this information.

Management reports and alerts are essential for senior management and the board to keep abreast of model risk issues facing the organization. The CRO should provide reports on the aggregate level and direction of model risk to the board on a regular basis. This aggregate view should be formed in part from the model and model use inventory, model performance tracking, an inventory

[6] Some examples of actions include on-top adjustments, more frequent performance monitoring or reporting, limited model use, or lower risk limits.

of significant model adjustments and assumptions, a tracking system for significant model changes, an inventory of significant model controls and thresholds, a tracking system of validation findings, and other relevant model-related risk metrics.

Findings and Model Risk Issues Management

Proper tracking and remediation of model validation findings and other identified model risk issues are essential in managing model risk. Model-related findings and identified risk can come from a variety of sources, including internal audit, external audit, FHFA examinations, model validations, and monitoring. Competent parties should be able to provide an objective analysis of model risk and have the authority to properly remediate issues or escalate them to senior management for timely resolution. Model risk issues can include technical limitations on models. Proposed solutions to these limitations may affect a model's use and output. These solutions should be within an acceptable level of model risk to senior management or the board.

Model risk managers should provide regular tracking reports to senior management and governance committees. A Regulated Entity should prioritize model risk remediation efforts to ensure timely resolution. A Regulated Entity can develop longer-term action plans by focusing on more permanent fixes to a model and use short-term solutions (e.g., on-top adjustments tied to a model's business objective) to mitigate risk while a longer term fix is being developed. Higher risk issues should be escalated to appropriate management committees for effective oversight and challenge, especially in cases where short-term solutions may add a different type of model risk. A Regulated Entity should have a clear escalation policy and dispute resolution process in place for challenges to validation findings or other identified model discrepancies. Procedures should clarify how findings are remediated in cases of disagreement. The process should establish time limits for resolutions and an approval process for identified model risk gaps and exceptions to the organization's remediation policy. A Regulated Entity should ensure compliance with policies, procedures, and controls so all parties effectively manage risk in their areas. Appropriate authorities should sign off on all exceptions, and, in the case of the FHLBanks, with notification to FHFA if warranted. All remediation efforts and mitigating actions to address model risk should produce an acceptable level of model risk to senior management and the board.

Model Lifecycle - Development, Implementation and Documentation

A Regulated Entity should ensure that it properly manages its models to achieve optimal performance throughout their lifecycle, including the stage of development, testing, deployment, validation, maintenance, performance tracking, on-going monitoring and timely replacement. This assurance involves effective policies and procedures along with documented evidence of compliance.

Model development should be a disciplined process aligned with the strategic goals and business objectives of a Regulated Entity and the business units it supports. A Regulated Entity should follow policies and procedures for model development of internally-developed as well as vendor models. Model development includes all activities relating to research, development and production implementation of models. Policies and procedures should address establishing business needs (whether a model is built internally or via an external vendor, documentation), data assessment, IT infrastructure, testing, ownership, the review and approval process for putting new models into production, roles and responsibilities of various groups (including separation of development and testing functions), access rights, and an implementation plan. All new models should have a model development plan with a clear statement of purpose to ensure they meet their intended uses. The model development plan should include resources, a general timeline, testing and validation requirements with appropriate thresholds, and an implementation plan. In large, complex enterprises, the model development plan could incorporate or reference other procedures and standards for new model development, but should provide an overall representation of how a Regulated Entity plans to develop and implement the model.

Internal model development requires considerable time, resources, and expertise. The experience and judgment of model developers significantly influence the model's design, inputs and assumptions, and processing components that affect the extent of model risk. Even a model that is technically sound may be incorrect in concept or in application. A Regulated Entity should also have the requisite staff and skill sets to perform adequate oversight over model developers, and controls throughout the development phases of an internal model. Maintaining and developing these capabilities is justified when such activity clearly produces a competitive advantage. A Regulated Entity should continuously weigh the costs against the benefits derived from maintaining internal models.

Regulatory experience at large, complex organizations has shown the value of the model risk management group's active participation in pre-development model planning and prioritization with business units and model owners. This allows the model risk management group to opine earlier in the process on whether planned model changes are on track to remediate outstanding model findings or issues. Senior management support and proper organizational placement are needed to afford the model risk management group the stature and influence necessary to carry out its function effectively. Model development is a support activity that seeks to address the modeling needs of business units, risk management and finance.

Instead of developing models internally, a Regulated Entity may choose to employ a third-party vendor model, procure a modeling service, or have a model externally developed for its sole use. A Regulated Entity should put in place the commensurate level of control and governance surrounding the acquisition, testing and implementation of such models.

When developing a model, the model's design, theory, and logic should be supported by industry practice, published research, and an assessment of alternatives. A Regulated Entity should ensure that a model's methodologies and specifications are well-documented. For internally developed models, this also includes an annotated copy of model computer code. A Regulated Entity should conduct a rigorous assessment of the quality and relevance of data and other information used in the development of such models using supporting documentation.

A Regulated Entity should employ rigorous testing prior to deploying a model or a significant model change, and document the results of this testing. A Regulated Entity should develop a test plan indicating the nature and purpose of testing, how the testing outcome will be judged, and the parties involved. The nature and extent of testing and analysis depends on the type of model as well as its materiality and significance. A Regulated Entity should test and evaluate results using different criteria depending on a model's design and purpose. Model testing should include verification of the model's accuracy and performance as intended, identifying where the model becomes unreliable, demonstrating that the model is robust and stable, assessing potential limitations, evaluating behavior over a wide range of input values or extreme conditions (including out-of-sample data), assessing the impact of assumptions, and assessing the model's impact on other dependent models upstream and downstream.

A Regulated Entity should also ensure that effective controls are in place to monitor and ensure proper model implementation. Prior to implementing a model or model change to production, a Regulated Entity should follow its validation policy and approval practices.

Documentation

Sound model development requires a minimum standard of documentation to prevent key person dependency risk, enables proper operation of a model, facilitates an independent review with minimal assistance, and reduces risk when implementing model changes. Sound documentation requirements address the informational requirements of an independent validation group, and the informational needs of model users, software developers, and model risk and business unit managers. The level of documentation should be commensurate with the relative importance of a model to an entity's decision-making or risk management processes.

In large, complex enterprises, adequate documentation should be maintained through a model's lifecycle including the research and development, implementation and post-implementation phases.

At a minimum, a Regulated Entity should maintain the following documentation:

1. Materials and evidence related to model development, including research, business and technical requirements, and implementation. A model development plan should capture some of this information. For internally developed models, the documentation standard for research

and development will be more detailed than for vendor models. Adequate documentation of model theory and the model development process builds institutional knowledge. Documented business and technical requirements ensures that a model is developed consistent with its intended use and implemented on the appropriate software platform.

2. Documentation from the research and development of vendor models, though available information may differ among vendors. A Regulated Entity may not have access to proprietary information such as the modeling approach, model code and numerical algorithms. A Regulated Entity should, however, have vendors provide developmental evidence explaining a model's components and intended use, information regarding the data used to develop the model, and testing results that show the model works as expected. This documentation should allow a Regulated Entity to assess the assumptions and methodologies underlying a vendor's model in the same manner as for internally developed models. A Regulated Entity should have contingency plans in place for instances where the vendor model is no longer available or cannot be supported by the vendor.

3. An operating manual or model user's guide on how to operate a model or model application that also describes a model's inputs, assumptions, underlying theory, mathematics, output reports, and risk metrics. The manual should include a brief summary that provides a clear description of the purpose of a model and its assumptions and limitations. The manual should also describe the procedures used to operate, maintain, and update a model. The guide should address staff training on a model's use. The manual should be sufficiently detailed to enable a qualified third-party to independently operate and maintain a model.

4. Materials and evidence that a model is being properly maintained, including model specific procedures, performance tracking results and output analysis, and testing and changes in response to validation findings or other identified model discrepancies. A Regulated Entity should store copies of the model documentation in a safe place, preferably off-site, to facilitate disaster recovery.

Conclusion

This advisory bulletin outlined minimum regulatory expectations regarding model risk management using a framework of controls and policies, and management guidelines on how a model's lifecycle risk should be identified, managed and reported across a Regulated Entity by stakeholders. This framework relies on model owners and users taking ownership of managing risk at its source. The framework expects periodic assessments and monitoring of risks along with intermediate mitigations and longer term solutions. Clarifying the primary responsibilities of model developers and model users is meant to encourage a culture of risk management rather than a culture of compliance with management and regulatory requirements.

Advisory Bulletins communicate guidance to FHFA supervision staff and the regulated entities on specific supervisory matters pertaining to the Federal Home Loan Banks, the Office of Finance, Fannie Mae, and Freddie Mac. This bulletin is effective immediately upon issuance. Contact at Kari Walter, Senior Associate Director, Office of Supervision Policy at Kari.Walter@fhfa.gov or (202) 649-3405, Kyle Roberts, Associate Director, Office of Supervision Policy at Kyle.Roberts@fhfa.gov or (202) 649-3005, Michael Lee, Examination Manager, Division of Enterprise Regulation at Michael.Lee@fhfa.gov or (202) 649-3510, or Stefan Szilagyi, Examination Manager, Division of Bank Regulation at Stefan.Szilagyi@fhfa.gov or (202) 649-3515 with comments or questions pertaining to this bulletin. This Advisory Bulletin is a Public document.