sifma

Internal Auditors Society

Internal Audit Guidelines

Model Validation and Governance

October 2015

SIFMA's Internal Auditors Society (IAS), whose members include internal auditors from banks, broker-dealers, insurance companies, mutual funds, public accounting firms, and self-regulatory organizations associated with the securities industry, provides these audit guidelines for information purposes only. The audit risks, audit guidelines, controls, and audit work steps that apply to any particular firm may vary depending on the firm's organizational structure, business activity, and other factors. The IAS recommends that firms seek the advice of their own legal, accounting and/or other advisers with respect to these matters and any questions concerning the application or interpretation of accounting and auditing standards.

TABLE OF CONTENTS

I. INTRODUCTION AND BACKGROUND

Overview

For years, organizations across industries have been using models in key business decision making, for enterprise-wide risk management, and for financial and accounting purposes. Financial services firms use complex models to manage and hedge financial portfolios. Large corporate treasuries use sophisticated models to manage their debt, derivative, and foreign currency positions. Middle market companies use critically important, and sometimes home-grown, models to forecast cash and funding needs. The use of models, irrespective of the size and complexity of the model, can introduce the problem of model risk. As companies have learned, without periodic validation and proper oversight, the tools used to measure risk may themselves become an unintended source of risk.

Financial models are an accepted and valued tool for estimating earnings, assessing values, and evaluating risks. Models have become indispensable and practical necessities to an increasingly complex financial world. However, despite their virtues, an overlooked calculation error or data integrity issue can compromise the results of these models and jeopardize the original modeling objectives – while also potentially costing companies both time and expense to fix. The use and complexity of these models continues to increase with the ever-changing market and business conditions, resulting in increased model risk with banks increasing the use of data-driven, quantitative decision-making tools.

Recent market events and 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. These bodies require that organizations identify key models, conduct periodic objective model validations to confirm their accuracy and are moving towards having validation requirements for inputs such as spreadsheets and other databases. Regulatory authorities such as the Office of the Comptroller of the Currency (OCC)[1], the Federal Reserve[2] and the Federal Housing Finance Board[3] have already issued guidance requiring organizations to validate models on a periodic basis. In addition, there has been a regulatory magnifying lens on the model validation process itself and an increased focus on modeling and model assumptions. In the United States, the issuance of the Financial Accounting Standards Board's (FASB) Accounting Standards Codification (ASC) and globally the International Financial Reporting Standards (IFRS), specifically ASC 820 and IFRS 13 have impacted fair value measurements and disclosures in financial statements.

Understanding Model Limitations is a Critical Component of Model Risk

While model validation plays a critical role in model risk management, sound development, implementation, and use of models are also vital elements. All models have limitations and are subject to the validity of their underlying theory and assumptions. Decision makers must understand the inherent limitations of the model's underlying assumptions, particularly at the development stage, and ensure model limitations and assumptions are covered in model documentation and in ongoing monitoring of model use. Model assumptions and limitations are also assessed as part of the model validation process.

[1] OCC 2011-12 and OCC 2000-16
[2] SR Letter 11-07
[3] FHFA Advisory Bulletin AB 2013-07

Role of Internal Audit in Model Validation

A guiding principle for managing model risk is the "effective challenge" of models. Effective challenge consists of critical analysis by objective and informed parties who can identify model limitations and assumptions and challenge developers on their methodology and approach. Effective challenge requires a combination of appropriate incentives, competence, and influence in the organization.

Although not explicitly defined, the guidelines assume that internal audit performs a significant role in a firm's model validation program. In most large scale financial institutions, especially those defined as a Systemically Important Financial Institution (SIFI), model validation is primarily performed by the model risk/model validation team, under the supervision of a Chief Model Risk Officer (a second line of defense function). Contrastingly, internal audit evaluates whether model validation can effectively and independently challenge the models. An optimum scenario would be that an independent model validation team performs model validation, reviewing and evaluating the model risk around the key model components, (i.e., Information, Data and Assumptions Components, Processing Component and Reporting Component). Internal audit is also involved in the model risk management process, by reviewing the key procedures and controls surrounding the life cycle of model development (i.e., model research and development by the first line of defense, model implementation and validation, and post-implementation review and monitoring).

Typically, staff tasked with reviewing and validating models have some degree of independence from the model developers, owners and users. Incentives to provide effective challenge to models can be easier to implement when there is greater separation from the model development process (where practical) and when challenge is supported by well-designed compensation practices and corporate culture. It is essential that model review & validation staff have the technical knowledge and modeling skills 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.

Although model risk management and model validation are internal processes, a financial institution 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. Whenever external resources are used, banks must have appropriately qualified individuals to review and approve their work.

Model validation should include a review of a model's actual use relative to the intended use defined in development documentation, including evaluation of the model developers' comparison of alternatives, the rationale of model choice, the strength and weakness of each option, as well as its compliance with any applicable regulatory guidelines. Validation reports should also include a comparison of model methodologies to industry-leading practices and any relevant regulatory guidelines. Through the review of assumptions and the evaluation of the model limitations, model validation can help with the ongoing assessment of a model's appropriateness relative to changes in market practice, industry trends, and internal strategic objectives.

A robust model validation approach

A robust model validation process involves a thorough review of the following key components of the model:

I. Information/Governance Component
II. Data and Assumptions Component
III. Processing Component
IV. Reporting Component

I. Information/Governance Component

The information component of a model validation includes a review of the model's development documentation, related policies and procedures, and any other information that will help the validator understand the model. Model risk management policies, including a model validation policy, may form part of a broader Model Risk Management Framework for how organizations should design, use, and oversee the use of models.

Audit Risk: Inadequate governance around model validation

Developing and maintaining strong governance, policies, and controls over model validation is fundamentally important to its effectiveness. A weak governance function will reduce the effectiveness of overall model risk management, including model validation. A strong governance framework provides explicit support and structure to the risk management function through policies defining relevant risk management activities, procedures that implement those policies, effective allocation of resources, and mechanisms for evaluating whether policies and procedures are being carried out as specified. The scope and sophistication of an entity's governance function should align with the scope and sophistication of model usage in the company.

Model validation testing considerations: Model risk governance is provided at the highest level by the board of directors and senior management when they establish an entity-wide approach to model risk management. As part of their overall responsibilities, the board and senior management should establish a strong model risk management framework that fits into the broader risk management function of the organization. Senior management should ensure adequate policies and procedures are in place to ensure compliance. Additionally, they should be assigning competent staff with appropriate segregation of duties (i.e. model validation should be performed by personnel independent from the developer of the model), overseeing model development and implementation, evaluating model results in ensuring effective challenge over models. Senior management should also be actively involved in reviewing validation and internal audit findings, and taking prompt remedial action when necessary through relevant committees and communication with the board on significant model risk, from individual models and in the aggregate, and on compliance with policy.

Audit Risk: Inadequate model documentation

Organizations often lack appropriate model documentation and in some cases there is insufficient clarity regarding the scope, content, and detail required in model documents. This can be caused by a lack of formal policies and procedures, fragmented model development (a first line of defense function) which creates inconsistency, and situations where large groups of models were developed under legacy policies and are not yet compliant with the new model risk framework. This can weaken processes and controls that support model development including model assumptions, data inputs, model updates, and model outputs/reporting. Collectively these weaknesses may increase risk.

Model validation testing considerations: Model validation procedures involve understanding the model's use, limitations, development, change management, ownership and control policies and procedures though a review of all model documentation as well as discussions with model developers, owners, users, support functions, and risk management.

Policies should require appropriate testing and analysis, and set standards for acceptable levels of discrepancies, including procedures for review and mitigation of 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 future validations. 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 policies which outlines the Firm's definition of a model, what should be included and what can be excluded from model inventory, documentation requirements for 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.

II. Data and Assumptions Component

Data includes model inputs, variables, results from calculations, or combinations thereof. Data may come from internal or external sources. Model assumptions are critical components of a model that should be reviewed and approved by management to ensure they are appropriate for the model. For instance, in a cash flow forecasting model, historical cash flows are data inputs, whereas expected growth rates for revenue would be both inputs and assumptions.

Audit Risk: Bad data input

The adage "garbage in, garbage out" is an appropriate metaphor applicable to all models. For example, at the time of valuing an acquisition, the acquirer may erroneously use a weighted average cost of capital that does not reflect the true cost of capital, resulting in a substantial change in the value of the target company. Model dependency relationships also pose an increased audit risk as it may use that model's output as input. In addition, regulatory expectations around identification and documentation of model inputs continues to increase.

Model validation testing considerations: Model validation procedures should include data accuracy, consistency and integrity checks, and a review of the underlying processes used to obtain the data. Data completeness should be ensured by checking control totals at key steps along the data flow. Data inputs may be compared to source documents, market accepted third-party data, published research, sound industry practice or expected input ranges. In addition, testing may include a review of any algorithms that support the data feed, a review of data extraction, and compilation procedures, etc. If model dependency relationships exist, these should be reviewed and documented as it is very common that the model being validated has dependency on another model. Therefore, the quality of the upstream model has a direct impact on the model being validated. Model validators should

document the relationship of the model with all of its upstream models and downstream models (if possible), and assess the risk/impact from upstream models.

Audit Risk: Erroneous assumptions
Models may include assumptions as part of calculations that convert observable data and parameters into results, prices, values, or information. If these assumptions are inappropriate, inaccurate or obsolete, the accuracy of model output will suffer. For example, updating a USD-JPY currency option model with volatility assumptions associated with another currency pair, e.g., EUR-CAD may result in incorrect valuations, incorrect risk assessments, and erroneous P&L.

Model validation testing considerations: Model validation procedures should include a review of critical assumptions to confirm that the assumptions are appropriate for the model's intended use. Assumptions may be compared to observable reference points or other external sources, e.g., market data, historical data, industry research, and academic research. Organizations should ensure that model assumptions are clearly documented (along with documenting the limitations that result from using these assumptions), based on analysis that reflects current market trends, and/or is consistent with market practices and academic literature to establish their appropriateness.

III. Processing Component
The core logic and mathematical underpinnings of the model is referred to as the processing component. It refers to the theory, analytics, and mathematics that transforms data and assumptions into information, data, or output for the purposes of valuation, pricing, risk management, or business decision making.

Inappropriate theory or coding errors will undermine the modeling objectives and can lead to inaccurate results that may adversely affect decision making.

Audit Risk: Calculation errors and errors in model logic
A model- whether simple or complex- is at risk for potential errors. A wrong cell reference in a spreadsheet model or the incorrect implementation of a complex algorithm in a more robust programming language can both lead to incorrect results.

Model validation testing considerations: Model validation procedures should involve detailed testing of the model's processing component over multiple scenarios or conditions, including scenarios that are outside of the range of ordinary expectations. The underlying logic and calculations of the model should be reviewed to assess the model's internal integrity for performing the calculation for future periods. This may include conducting a robust code review, testing the model and market pricing points, and conducting limiting case and extreme value testing. The model may also be tested in parallel against independent models to evaluate its accuracy. In addition, the model theory and math should be periodically reviewed against industry practices and technical literature to confirm that the model is still appropriate given current market conditions and is current with industry practices. Firms should also have an escalation process associated with model validation, and a procedure (or "waterfall") for applying different approaches, when that option exists for hard to price securities.

IV. Model Reporting
Model reporting is used to communicate model results and facilitate decision making. Since key business or risk management decisions are based on model reporting, it is imperative that reports are both relevant and accurate. Typical model reports include information on key model assumptions, outputs, and pertinent factors or limitations. Other reports include scenarios and stresses to provide

additional information to management. For example, a Value-at-Risk (VaR) report, which communicates daily risk, may be augmented with historical or hypothetical stress scenarios to show how the portfolio will perform in periods of unusual volatility or with large shocks to key risk factors.

Model validation testing considerations: Model validations should question the accuracy and relevance of information reported to management in terms of its ability to foster timely and reasonable decision making. Key considerations include:

- Do model reports convey accurate information presented in a timely manner?
- Does model reporting capture the critical elements necessary for management to make informed decisions?
- Is the output data clearly communicated and understandable for the intended audience?
- Is the data supporting the report stored, recoverable, and auditable?
- Are error-checking and peer review processes in place?
- Are calculations and reports aligned with the capabilities and requirements of information systems?
- Is there an escalation process for refuted data, refuted models or refuted inputs?

II. AUDIT GUIDELINES[4]

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
I. Information/Governance Component		
Model Risk Framework The model risk framework is out of date or does not take into account the business objectives and address all of the regulatory requirements.	A model risk framework exists, is well defined, prescribed, updated, reviewed and approved by the board and senior management periodically, or when significant changes occur, to ensure consistency with current best practice, risk appetite, business strategy and regulatory environment. Clear ownership of processes and controls, including those over model validation, are documented with the appropriate persons.	• Obtain the model risk framework and perform a gap analysis against regulatory requirements and industry best practices and assess whether all areas of model validation have been incorporated that allow for effective challenge of models • Obtain evidence that the framework has been approved by the board of directors and/or senior management (i.e. board of directors / committee meeting minutes) and the framework has been approved by the head of the risk department • Assess whether the framework reflects the approved strategy/risk appetite where applicable • Verify that any changes to the framework are communicated in a timely manner to key stakeholders and the business
Model Risk Governance Structure The model risk governance structure does not match the nature, scale, complexity and risk content of the business and model activities.	Up-to-date organizational and governance charts are available showing a clear allocation of roles and responsibilities, management structure, reporting lines, supervision and accountability as it relates to model risk governance, including model validation. The board of directors / senior management reviews and approves on an annual basis the overall appropriateness and efficiency of the governance structure, including suitability	• Obtain the organizational and model risk governance structure: o Confirm with the business that it is up to date and corroborate with current HR listings o Assess the organization and governance structure and determine whether the model validation component of the model risk governance structure is appropriate to provide for effective challenge (i.e. model validation is sufficiently independent from model development and model implementation and has clear reporting lines to the Board of Directors / senior management) • Obtain evidence that the Board of Directors /

[4] Not all audit work steps are fully applicable to all model categories (i.e. risk capital, decision-making, stress testing, valuation/pricing)

	of reporting lines, definition of roles and responsibilities and adequacy of oversight committees.	senior management reviews the roles, responsibilities and resourcing of model risk governance, including model validation, at least annually [this may be documented in committee minutes (e.g. Risk Management Committee)] • Obtain evidence that the Board of Directors / Risk Committee / senior management has reviewed the complexity and risk of the business, linkage to its model activities and assessment against the model risk framework. This may be performed through a risk and control self-assessment (RCSA) with key findings and recommendations presented to the Risk Committee / Board • Review the resumes and credentials of the model governance body's members and assess whether they have sufficient knowledge and expertise to provide effective challenge over the Firms models
Policies & Procedures Policies and procedures do not adequately address regulatory expectations and do not provide a clear mandate to the model validation function. Policies are not maintained or approved.	Policies and Procedures exist for model validation, are well documented, updated, reviewed and approved by senior management periodically, or when significant changes occur impacting the policy, to ensure consistency with current best practice, risk appetite, business strategy and regulatory requirements. Clear ownership of processes and controls are documented and key stakeholders demonstrate awareness. Model documentation does not address the review of business requirements and purpose. The model review does not take into account the model	• Obtain a complete listing of Policies and Procedures and verify that all areas of relevance for Model Validation have been documented: o Model Validation scope and timing o Definition of a Model o Definitions of Model Risk Rankings o Listing of Model Inventory and what constitutes a new model o Model Uses – Identifies the model purpose, applicability, and use as described in model documentation and as understood by management o Model Limitations – Identifies the model restrictions and stated conditions under which the model results are not applicable o Model Development – Identifies the business requirements, design and implementation procedures applied, including user acceptance testing procedures o Model Changes – Identifies significant structural model changes or updates made to the models during the year o Model Ownership – Identifies maintenance, and change control responsibilities

	limitations. Therefore, the model outputs may not be applicable to different business entities or different periods of time. The coefficients of model parameters do not fit the updated data and are not able to provide appropriate prediction. Variable transformation does not fit the updated population and is not able to generate appropriate prediction. If simulation technique is applied, the risk could be caused by incorrect underlying distribution assumption and insufficient number of simulation paths.	○ Model Control – Identifies model control policies, defined responsibilities, documentation, and audit oversight ○ Model Application – Identifies that models and inputs to the models are appropriated applied and incorporated into policy updates (if required). • Obtain evidence that these Policies have been approved by management (i.e. committee meeting minutes) and Procedures approved by the head of the risk department • Assess whether Policies & Procedures reflect the approved strategy/risk appetite where applicable • Determine whether the policies and procedures reflect the most current regulatory requirements • Verify that any changes to Policies & Procedures are approved & communicated in a timely manner to the business • Review model risk ranking and prioritization documentation to assess whether it is measurable and supported by appropriate evidence
Business Strategy The business strategy does not reflect the institution's risk appetite.	The Board of Directors has clearly established strategic objectives which are appropriate from the perspective of model risk management. - The Board approves the overall risk appetite and strategy (and any other policies for integrated risk management) at least annually or more frequently during periods of market turmoil or major strategic changes. Meeting minutes showing discussion and approval are available and have been approved and distributed to those attending.	• Obtain evidence the overall strategic objectives and risk appetite are defined and approved by the Board of Directors at least annually • Obtain evidence that the strategic objectives and risk appetite is communicated appropriately throughout the organization (typically through Policies and Procedures) • Assess whether the model validation policies and procedures are appropriately designed and documented to provide effective challenge over model risks as it relates to the Firms' business strategy (i.e. Are model validation procedures designed to assess whether models are developed and implemented appropriately to meet the Firms business strategy within the firms tolerance for risk)

	- The risk strategy of the business is appropriately communicated to the organization.	
Committee Structure Committees overseeing model validation (and more broadly, model risk management) are not appropriately addressing the key issues, risks and decision making required.	A committee charter is available for each key committee (e.g., Risk Management Committee, Risk Appetite Committee) which defines the mandate of the committee (including roles governing model risk management and model validation), responsibilities of each member, the requisite experience & knowledge of members, required member attendance, delegated authorities and other requirements. - Committee charters are reviewed and approved at least annually by the Board of Directors - An evaluation of the committee members (e.g., experience/knowledge) is performed at least annually by the Board of Directors or their delegate.	• Obtain the committee charter describing each key committee (i.e. Risk Management Committee and the Risk Appetite Committee) and evidence Board of Director review and approval at least annually • Verify the charter includes the committee mandate, responsibilities of each member (and assess whether these include model validation), experience/knowledge of members, required members, delegated authorities and other mandated requirements. Verify that the attendance required appears reasonable • Obtain evidence Board of Directors (or their delegate) review and approval of committee members (e.g. knowledge/experience) at least annually • Obtain a sample of meeting minutes and assess whether there was appropriate attendance in place. In doing so, assess whether a quorum is present when items are voted on at the committee meetings, in accordance with the definition of what constitutes a quorum for the committee. Verify that meetings are being held as planned, and when there are major problems ad-hoc meetings are called
Management Oversight of Model Validation Reporting Validation reports are not adequately reviewed by management. Management makes sub-optimal decisions as a result of information not being clear, detailed and	Validation reports and associated procedures (manual and system) for reporting of validation results are monitored by management at least monthly to ensure the following: - reporting occurs at the frequency required in policy - reports are distributed to the appropriate members of senior management	• Review model validation reporting procedures. Ensure procedures address the timeliness of reporting, escalation of validation findings, review of reports, and the process for mitigating validation findings • For a sample of validation reports, review the distribution of the reports and verify that they have been reported to the correct level of senior management and that the reports were produced and distributed in a timely manner

timely.	- validation reports and findings are distributed in a timely manner - management & model owners take prompt remedial action when necessary	• For a sample of validation reports, verify that the validation results have been accurately derived from validation testing documentation, have an assigned owner and action plan associated with each finding. Furthermore, verify that the actions have been agreed and approved according to policy • For a sample of validation reports with completed action dates, verify that the findings have been appropriately addressed through the action plan implemented by the respective action owner
Model Sampling Models are not being reviewed and validated in a timely manner and not in accordance with their risk profile.	There are policies/processes in place which outline the methodologies and practices for model sampling within all three lines of defense to ensure full coverage of all models within an appropriate life cycle.	• Obtain relevant policies and an understanding of relevant processes. Assess their adequacy and that policy includes documented model sampling life cycle approach including an assessment of model inventory, associated model risks and model application • Review whether the model inventory is complete and accurate • Test whether all models has been included in the validation life cycle
Segregation of Duties The model validation process is not adequately segregated and independent of the model development, model implementation and model use functions within the organization.	The on-going validation of model components are performed/reviewed independently of model developers and users where sufficiently possible (i.e. front office, product control or credit risk management teams).	• Assess whether a clear mandate is in place for the model validation function and whether the ownership of model validation responsibilities is defined • Evaluate the interaction, and degree of reliance placed, between the model validation process with relevant support functions for providing data or other information. Based on the results of this evaluation, assess the adequacy of model validation process' independence in light of its mandate • Within the model validation process verify that adequate segregation exists between functions, both in terms of reporting lines and by actions and outcomes (i.e. incentives and pressures) • Confirm that reviewers' incentives (i.e.

		compensation practices and performance evaluation standards) are not related to models staying in production and model results are aligned with the goals of model validation • Review the Firms code of conduct
Effective Escalation, Tracking and Resolution of issues Inadequate oversight of model risk management practices may increase the risk that inappropriate activities from various sources (i.e. Model Validations, Audit, Regulators, etc.) are not escalated, tracked and resolved properly.	There are policies/processes in place to ensure findings related to model validation are escalated to the appropriate control and risk management committee, tracked and escalated appropriately through to resolution. This includes documentation of investigation, resolution of escalations; required management sign-off and associated timelines.	• Obtain relevant policies and an understanding of relevant processes. Assess their adequacy and that policy includes documented escalations (investigation and resolution) that are signed-off by management • Review a sample of escalations and verify that actions were performed in the appropriate timeframe, by the appropriate risk management function to mitigate the risk in compliance with the escalation policy • Assess whether issues identified from various sources (i.e. Model Validations, Audit, Regulators, etc.) are appropriately documented, tracked and resolved from their various sources in accordance with the firms policies and procedures
Training Model risk professionals within the organization do not attend adequate training or keep up to date with industry trends and developments.	Model risk management teams attend regular training sessions, peer group reviews and are members of appropriate industry groups in order to keep up to date with the latest methodologies and trends within model risk management. Attendance at training is documented. Training requirements are monitored by model validation management.	• Verify that model validation staff attend required model risk training • Sample training records to verify that required training is monitored and approved • Assess the level of training provided to model validation staff to ensure that they keep up to date with latest developments and new products
Adequacy of Resources Staffing levels within model risk management is inadequate to support	Model risk management participates in the firm's annual planning and budgetary process to assess and adequately staff model risk management functions. This	• Assess the adequacy of staffing within the model risk management function, to adequately support the business and to perform the functions required for model validation, particularly where judgment is involved with respect to model assumptions, inputs, calculations and the

its mandate.	annual assessment is reviewed and approved by the Board of Directors and/or appropriate senior management.	interpretation of results. The assessment should also take into consideration the adequacy of staffing • For a sample of model validation professionals in various positions of responsibility, obtain the respective HR defined job descriptions and assess the professional adequacy of those staff • Verify review and approval of the firm's annual planning and budgetary assessment by the Board of Directors and/or appropriate senior management • Review the deployment of the model validation function, systems support and development to ensure that appropriate and adequate resources have been assigned to perform the function in the deployed locations
Outsourcing and Off-Shoring Arrangements The establishment of outsourcing and off-shoring arrangements may create performance issues and control gaps**.**	Functions opting for outsourcing and off-shoring/deployment arrangements have performed a risk assessment (including an analysis of any legal and regulatory requirements) and appropriate risk mitigation plan prior to the deployment and/ or outsourcing of personnel. - Functions have established control and performance standards - Legal agreements and internal service level agreements and procedures documentation exists which defines the range of outsourced and off-shored activities and determine the duties and responsibilities of the service. - Business Continuity Plans exist for the outsourced and/ or deployed function.	• For the in-scope functions, determine whether outsourcing and/or offshoring arrangements exist and determine whether they are significant for the scope of the audit. For outsourcing and off-shoring arrangements identified as requiring review, perform the following: - Assess whether a formal risk assessment was carried out prior to deployment or outsourcing of model validation procedures. - Obtain and review related contracts, service level agreements and procedures. Assess that the contract grants full auditing rights and includes adequate confidentiality clauses. - Evaluate whether control and performance requirements have been defined and Vendor Management Policy is followed. - Thoroughly review key risk indicators and management information to determine whether there are performance issues • Inquire, review, and test that regulatory requirements and restrictions are met • Assess whether the Firm has appropriately qualified individuals to scope, supervise, review and accept the work of external resources and/or

	- Vendor Management Policy is followed for outsourcing.	off-shoring arrangements • Evaluate valuate whether Business Continuity Plans, SOC 1 reports and vendor contingency (in the case of outsourced relationships) have been considered and are adequately documented and tested • Note: Model validation procedures should be similarly and consistently applied to third-party models as they are to internal models
Regulatory Requirements The Firm fails to comply with regulatory requirements (e.g., Fed, OCC, SEC, local regulators).	The model validation team monitors all regulatory requirements and ensures that the firm's validation procedures comply with such requirements. This team also coordinates with model risk management for all regulatory meetings, and interactions. The model validation team ensures new and existing regulatory requirements are met by performing a documented analysis of regulatory requirements and that required changes are implemented to resolve identified gaps.	• Through discussions with the regulatory team, obtain an understanding of all regulations in all jurisdictions that have specific requirements for model risk and model validation • Understand whether there have been any recent regulatory examinations, significant letters from regulators that have been performed/received for model risk, and particularly, model validation. Understand the outcomes, actions and conclusions from such interactions. Understand where there have been projects put in place to address any actions occurring. Document and review the status of such projects • Verify the model validation team's documentation of their regulatory gap analysis along with resolution of identified gaps
Risks not included in models There are inadequate governance procedures around the process for monitoring risks not included in models	Annually, or as required, senior management reviews and approves the governance framework in place for monitoring the process regarding risks not included in each model**.** This framework covers policies necessary to meet regulatory expectations.	• Verify senior management review of the governance framework in place for monitoring risks not included in models • Review the policy for risks not included in these models and ensure that it is adequate and meets regulatory expectations • Review the process for identifying new risks which are not yet included in these models and ensure that it is working in practice • Review that models are updated for new regulatory guidance, interruptions or regulatory violations by other firms.

Access to Systems, Source Code, Documents and Files Unauthorized access to applications, source code, databases, documents and files that support model processing.	Staff roles and responsibilities dictate their assigned user profile for access to applications, source code, databases, documents and files that support model processing. There is an Exit Policy which includes immediate revoking of access to terminated employees. Access review is performed and documented by IT/risk management quarterly.	• Obtain the access lists for applications, source code, databases, documents and files that support model processing • Evaluate access levels related to access privileges of key personnel • Verify access review performed quarterly by IT/risk management supervisors. Verify the review of access log to ensure information has not been tampered with. Verify access is revoked for terminated employees. Assess the resolution of exceptions identified • Assess whether model overrides are properly documented and analyzed by management

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
II. Data and Assumptions Component		
Completeness and Accuracy of Model Inputs Model inputs are not complete and accurate.	There is a controlled process to monitor and test the completeness and accuracy of model inputs. There is a formal governance forum reviewing and approving these inputs.	Utilizing a risk based approach, select a sample of models and perform the following validation procedures over data completeness and accuracy: • Obtain the model inventory and test the completeness of the population in accordance with the policies and procedures • Obtain a listing of the various data inputs for each respective model selected and validate that these inputs have been appropriately documented for each model (i.e. types of inputs allowed, approved sources including both internal and external inputs etc.) • For data inputs which are processed automatically (e.g. fed from a separate internal system / external pricing repository), verify that the data feeds are periodically assessed for completeness of coverage and accuracy of data transmission • For manual inputs, verify the completeness and accuracy to the appropriate internal / external sources as outlined in the model documentation. Data inputs may be compared to source documents, market accepted third-party data, published research, sound industry practice or to expected input ranges. In addition, testing may include reading of the data feeding algorithm, review of data extraction, and compilation procedures • Verify review and approval of assumptions and inputs by a formal governance forum • Verify the completeness of firm's inventory of inputs and consistency of usage with model application.

Model Feeds Feeds into and out of the risk data systems are incomplete.	Models may receive automated feeds from both internal and external systems and send outputs to other systems (i.e. for capital calculations, risk reporting and financial reporting). These feeds should be documented on clear process flow diagrams. Changes to feeds are approved and communicated to the appropriate model risk team.	• Obtain the population of feeds from different sources (both internal and external feeds) and spreadsheets and understand how the staff ensures completeness and accuracy of the feeds • Understand how new feeds or feed change requirements are communicated to the appropriate team. Document the role of staff in the setup of the feeds into the risk systems and the interaction with the different IT teams • Select a sample of feed changes and verify appropriate approval of both changes and/or accuracy • Verify that refuted data and data cleansing from automated feeds are documented and approved.
Data Consistency and Integrity Data inputs and assumptions are not accurately and consistently applied in accordance with the firm's policies, procedures or regulatory expectations.	Data inputs and assumptions should be consistently applied across each model to ensure historical comparability of model outputs.	• Understand the various inputs used by management and how management monitors the consistency and accuracy of the model and governance processes in place (e.g. Model governance committee etc.). Where issues arise with the consistency, integrity or accuracy of the model inputs, ensure that these are appropriately escalated and actions are taken to remediate them • For a sample of data inputs and assumptions, assess whether they have been applied consistently throughout the period under review • Where the basis of inputs and/or assumptions have changed, validate that the changes have been appropriately documented, reviewed and approved by management • Understand any transformations (e.g. calculations, conversions from one data type to another, etc.) occurring to data values and how data integrity is maintained

		• Review the latest back testing reports and ensure that the accuracy levels are within normal parameters. Ensure that the model outputs have remained within normal parameters for the period under review. Understand and assess reasons for any abnormal results • Specifically for credit risk models, validation procedures should include determining the appropriateness of the data analytics method, variable transformation, data calibration steps, and the segmentation.
Model Assumptions Model assumptions used in model development, use, and reporting are not adequately controlled and do not meet regulatory expectations.	Model assumptions are reviewed as part of model validations and annual model reviews. Policies and procedures in place to ensure these reviews are performed. Assumption reviews confirm that model assumptions are appropriate as they relate to any specific regulatory requirements. The methodology test does not address the review of business requirements and purpose.	• Confirm that model assumptions are documented in both model development and model validation documentation • Confirm that model assumptions are reviewed as a part of the annual model review process • Verify senior management review of validation reports and associated policies and procedures • Assess whether documentation address the review of business requirements and purpose for the model
Methodology Development Developments of new methodologies or significant changes to existing methodologies are not appropriately controlled.	An independent risk committee identifies needs, approves development and monitors implementation of new and changes to existing methodologies. This includes review and approval of written analysis before development. Senior management reviews and approves model validation and testing as required by policy. The use of model review	• For a sample of methodology changes, obtain evidence of review and approval of documentation provided to all relevant bodies • Review documentation and test results to assess whether the coefficients of model parameters fit the updated data and are able to provide appropriate prediction. • Verify senior management review and approval of the validation and testing of the implementation of the new methodology and associated policies and procedures prior to implementation

	does not take into account the model limitations. Therefore, the model outputs may not be applicable to different business entities or different periods of time.	• Review of independent model validation report. Verify methodology issues and recommendations identified in the validation report are tracked and followed up • Evaluate whether the testing documentation conveys an understanding of the model limitations and assumptions • Independent model validation could also include code review (not just methodology) performed by appropriately qualified individuals • Assess whether qualitative information and judgment used in model development was evaluated
Model Design and Construction is not in accordance with underlying model documentation, consistent with industry practice or not reflective of recent material changes.	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.	• Review the model documentation and assess whether the model limitations and assumptions are appropriately identified and discussed • During model validation assess that judgment exercised in model design and construction is well informed, carefully considered, and consistent with published research and with sound industry practice
Significant Risk Factors Significant risk factors associated with a model are not identified by risk management and thus are not covered by an appropriate	Model validation involves a detailed review of the key risk factors associated with a model. Assess whether risk factors are documented and communicated to risk	• Identify all products requiring quantitative models for risk management • Obtain all appropriate documentation to support the validation of the underlying model for each product selected

set of limits.	management for inclusion in limit setting and monitoring processes.	• Assess the documentation to ensure that it clearly identifies all key risk factors • Review T+1 risk reporting to ensure all risk factors identified are included for exposure monitoring • Determine whether risk managers are aware of any model limitations and opaque parameters identified. Determine also if market conditions cause model limitations (i.e., Bermuda options)
Data Quality Review Data quality issues are not adequately escalated and issues are not resolved timely.	A governance forum surrounding the model risk data quality metrics meets periodically whereby key personnel from the risk team discusses the data quality issues highlighted in the model risk control report. Issues are escalated and tracked in the forum. There is policy documentation to acknowledge and address data regulatory requirements.	• Ascertain there is sufficient representation on governance forum from business management • Obtain and review a sample of the meeting minutes of the model risk control report and ascertain: - Issues in the model validation reports have been sufficiently discussed - Action items including those to address data regulatory requirements are tracked and monitored for timely resolution - Delays in past due items have been adequately justified - Trends such as unusual trends or deterioration in metrics (e.g. late feeds, regressions, un-run macros) have been discussed

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
III. Processing Component		
Price Comparison Sources for model inputs are not reliable, resulting in inaccurate / unreliable model outputs	Compare the pricing inputs to those from a third party to determine pricing biases	• Perform an independent test by comparing model inputs to an independent third party pricing source • Document findings and report any discrepancies to senior management for consideration
Model Comparison Model calculations / model processing are not reliable and produces inaccurate / unreliable results	Compare the model results to the results from a third party or parallel model using the same data to determine pricing biases or model misspecification, where practical and dependent on availability and capacity	• As an independent test over a sample of models, compare the model results to the results from a third party or parallel model using the same data • Document findings and report any discrepancies to senior management for consideration
Limiting Case or Extreme Value Scenario Testing Stress testing calculations are not accurate potentially resulting in incorrect conclusions	Expose the model to limiting case or extreme values to determine the point at which the model hypothesis is no longer valid	• Adjust model inputs to reflect extreme market moves (both up and down, for key model inputs) • Assess model outputs for reasonableness & review in the context of known model limitations as documented in model development and validation documents
Back Testing Back testing calculations suggest that the model may not be performing as intended	Perform a comparison of model measurements to actual results for the period under review. Assess whether notional and percentage differences are material	• For predictive models (VaR for example) monitor observed values (i.e. actual p/l) vs. the range of values predicted by the VaR model • Confirm that the model produces outliers at a frequency consistent with the confidence interval specified in the model set up
Stress Testing Oversight Management oversight of stress testing is ineffective due to the lack of appropriate reporting	Daily, weekly and monthly stress test results should be reported to management, with adequate commentary and analysis explaining the results. Senior management provides review and effective challenge of the stress results and management's proposed risk-	• For a sample of stress reports for the period under review: o Ensure timely distribution of reports to appropriate parties o Confirm the reports contain an appropriate level of commentary and analysis o Verify review and challenge of stress results from senior management (e.g. committee presentations /reports /minutes of

	reducing strategies as appropriate.	meeting/emails)
Stress Limit Breach Actions taken as a result of stress tests is ineffective due to the lack of an appropriate limit framework	Stress limit breaches are escalated to the appropriate risk committees where mitigating actions are considered. Senior management uses the stress results in supporting their decisions in areas such as risk appetite, limit setting, capital planning and strategic decision-making.	• Verify actions taken and key decisions made by senior management as a result of stress testing (e.g. minutes of meetings) is in conformance with regulatory guidance & internal policy • Determine the extent to which stress testing output is used to support decisions in the following areas: - setting of the firm's risk appetite/tolerance; - setting exposure limits; - capital and liquidity planning; - longer term business planning and strategic decision-making; - assessing the consistency of risk appetite, business strategy and capital planning; - risk mitigation strategies; and - Contingency planning
Back Testing Design Back Testing methodologies do not adequately evaluate models.	Senior management reviews and approves back testing methodologies at least annually and as change is required.	• Obtain documented methodologies for back testing and verify senior management's review and approval • For a sample of back testing, verify that the approved methodology is followed
Back Testing Policies & Procedures Back testing procedures do not meet regulatory requirements.	The organization has a standard back testing policy which is compliant with regulatory requirements. The policy is reviewed and approved by senior management annually and as required.	• Obtain the policy for back testing of model results (e.g. VaR) and verify senior management review and approval • Ensure that policy is accurately reflected in the back testing methodology document • Confirm that back testing methodology is in compliance with applicable regulatory requirements
Back Testing / Stress Testing Calculations Back testing / Stress testing calculations are not performed in accordance with	Senior management reviews and signs-off on a periodic compliance review to ensure that the back and stress testing calculations are performed in accordance with the different	• Confirm that there is a process to monitor changes to regulatory requirements and update the procedures accordingly • Verify senior management's review and sign-off on periodic compliance review of back testing

regulatory requirements. If a simulation technique is applied, the risk could be caused by incorrect underlying distribution assumption and insufficient number of simulation paths.	requirements by each regulator, as well as internal risk management requirements.	calculations • Assess whether the model was stress tested over a wide range of model inputs • Determine whether a sensitivity analysis was performed to test the impact of small changes in inputs • Evaluate whether the stress testing documentation conveys an understanding of the model limitations and assumptions • Verify that the validation results confirm that judgment exercised in model design is well informed, carefully considered and consistent with published research and industry practice • Assess whether the documentation includes comparisons to alternative theories and approaches
Testing Exceptions Exceptions identified have not been investigated.	Management investigates all testing exceptions and provides commentary describing the cause of the exception. Commentary includes the impact due to P&L movements, trade and market movements and impact on risk/missing risk factors.	• Understand the various reporting to communicate back testing exceptions to the appropriate forums monthly • Verify that back testing exceptions are deemed to have occurred for any business day if the clean profit and loss figure for that business day shows a loss, which in absolute magnitude exceeds the firms pre-defined measures (e.g. one-day measure for that business day). • Verify that both positive and negative testing exceptions are identified • Verify that all exceptions have been analyzed and have adequate commentary describing the cause of the exception • Review testing reports produced and ascertain the number of testing exceptions (positive and negative) that have been identified at each level for the year • Identify specific business clusters with a high

		number of testing exceptions and understand the reasons for the high level of exceptions. Ensure that there are plans in place to address these issues including updating the methodology for the business. Verify that decision making is documented in committee minutes
Emergency Changes Emergency changes not properly approved and documented according to procedures.	Emergency changes are documented and approved per the organization's Policy & Procedures.	• Obtain a sample of emergency/unplanned model changes and verify that approvals were obtained in accordance with the organization's Policy & Procedures
Business Continuity Models are unable to continue to perform their required functions during a crisis/ disaster situation.	The firm has developed and implemented an organization-wide Disaster Recovery (DR) / Business Continuity Planning (BCP) planning process and related procedures that include the model risk management functions.	• Review the impact assessment figures for the various model risk processes and ensure that they adequately reflect the risk to the firm • Through inquiry determine the status of the Business Recovery Plan and ensure that it is up to date and accurate. Ensure that an adequate change manager and alternate have been assigned who maintain the plan and keep up to date (i.e. on a periodic basis, typically after 6 months, or whenever there are changes) • Ensure that the following have been documented for model risk management functions and are up to date: - Seating allocations at Disaster Recovery site - Contact details of recovery team - Critical systems - Various disaster scenarios

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps

IV. Reporting Component		
Quality of MIS Daily, monthly and quarterly MIS reports, provided to senior management are inaccurate, incomplete.	A standard reporting package from the risk systems is periodically reviewed by risk management to ensure completeness and accuracy and that user needs are being met.	• Obtain evidence that the standard reporting package from the risk system is periodically reviewed by risk management for completeness and accuracy
Relevance of Information Reported to Management Information reported to management is not relevant resulting in the inability to execute reasonable decision making	Model validations should question the accuracy and relevance of information reported to management in terms of its ability to foster timely and reasonable decision making	For a sample of model validation reports / results, perform the following procedures: • Test whether model results are compiled and reported completely and accurately by agreeing model results back to validation documentation and conclusions reached • Determine whether appropriate review and sign-off by management over validation results and conclusions are evidenced in the model validation documentation/workpapers • Compare the dates of conclusions reached over the effectiveness of models against reports presented to management and verify that findings identified were communicated to senior management in a timely manner and in accordance with the organization's Policy & Procedures • In reviewing model reporting, compare the information captured in the model reports against the requirements outlined in the organization's Policy & Procedures and necessary for management to make informed decisions (e.g. linkage to the entity's KRI's, specific model use etc.) • The output data is clearly communicated and able to be understood by the intended audience with conclusions reached and action plans agreed with model owners, if applicable

		• Verify that the data supporting the report is stored, recoverable, and auditable • In reviewing model validation documentation, verify whether an error-checking and peer review processes is operating effectively and evidenced timely • For a sample of calculations and reports perform recalculations to determine whether the results are properly aligned with the capabilities and requirements of information systems

III. GLOSSARY

The definitions in this section shall apply to the terms used in the guideline. Where terms are not defined in this section or within another chapter, they shall be defined using their ordinarily accepted meanings within the context in which they are used.

Back testing	Back testing is the process of comparing forecasted losses with actual losses. It is intended to act as one of the mechanisms for the ongoing validation of a firm's VaR model and to provide incentives for firms to improve their VaR measures.
Basel Committee on Banking Supervision	The Basel Committee on Banking Supervision provides a forum for regular cooperation on banking supervisory matters. Its objective is to enhance understanding of key supervisory issues and improve the quality of banking supervision worldwide.
FED	The Federal Reserve System. The Federal Reserve System was created on December 23, 1913 and the system is composed of a central, independent governmental agency. The Federal Reserve sets the nation's monetary policy, supervises and regulates banking institutions, maintains the stability of the financial system, and provides financial services to depository institutions, the U.S. government, and foreign official institutions.
Federal Housing Finance Board	FHFA works to strengthen and secure the United States secondary mortgage markets by providing supervision, research, data, and policies. They are an independent regulatory agency responsible for the oversight of vital components of the secondary mortgage markets—the housing government sponsored enterprises of Fannie Mae, Freddie Mac and the Federal Home Loan Bank System.
Financial Modeling	The process by which a firm constructs a financial representation of some, or all, aspects of the firm or given security. The model is usually characterized by performing calculations, and the firm makes recommendations based on that information. The model may also summarize particular events for the end user and provide direction regarding possible actions or alternatives.
Financial Risk Management	The process of evaluating and managing current and possible financial risk at a firm as

	a method of decreasing the firm's exposure to the risk. Financial risk managers must identify the risk, evaluate all possible remedies, and then implement the steps necessary to alleviate the risk. The forms of risk include Market Risk, Liquidity Risk and Credit Risk.
Governance	The overall management approach through which senior executives direct and control the entire organization, using a combination of management information and hierarchical management control structures. Governance activities ensure that critical management information that reaches the executive team is sufficiently complete, accurate and timely. These activities allow for appropriate management decision making, and provide control mechanisms to ensure that strategies, directions and instructions from management are carried out systematically and effectively.
KPI	Key Performance Indicators shed insight about risk events that have already effected the organization.
KRI	Key Risk Indicators monitor potential future shifts in risk conditions or new emerging risks so that management and boards are able to more proactively identify potential impacts on the organization's portfolio of risk.
Mark To Model	The pricing of a specific investment position or portfolio based on internal assumptions or financial models. This contrasts with traditional mark-to-market valuations, in which market prices are used to calculate values as well as the losses or gains on positions. Assets that must be marked-to-model either don't have a regular market that provides accurate pricing, or valuations rely on a complex set of reference variables and time frames. This creates a situation in which guesswork and assumptions must be used to assign value to an asset.
Market Risk	The possibility for an investor to experience losses due to factors that affect the overall performance of the financial markets. Market risk, also called "systematic risk," cannot be eliminated through diversification, though it

	can be hedged against. The risk that a major natural disaster will cause a decline in the market as a whole is an example of market risk. Other sources of market risk include recessions, political turmoil, changes in interest rates and terrorist attacks. Potential future exposure is typically measured using a Value at Risk (VaR) methodology.
Model Risk	A type of risk that occurs when a financial model used to measure a firm's market risks or value transactions does not perform the tasks or capture the risks it was designed to. Model risk is considered a subset of operational risk, as model risk mostly affects the firm that creates and uses the model. Traders or other investors who use the model may not completely understand its assumptions and limitations, which limits the usefulness and application of the model itself.
OCC	The Office of the Comptroller of the Currency charters, regulates, and supervises all national banks and federal savings associations as well as federal branches and agencies of foreign banks. The OCC is an independent bureau of the U.S. Department of the Treasury.
Risk Limits	Risk Limits are established limits suited to each operation and each risk category by examining the details of operations of the various divisions and taking into consideration the position of each division. These limits include risk limits, position limits, loss control limits, etc.
Risk Management	The set of processes through which management identifies, analyzes, and , responds appropriately to risks that might adversely affect realization of the organization's business objectives. Organizations routinely manage a wide range of risks (e.g. technological risks, commercial/financial risks, information security risks, legal risks and compliance risks).
SEC	The mission of the U.S. Securities and Exchange Commission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. The SEC

	oversees the key participants in the securities world, including securities exchanges, securities brokers and dealers, investment advisors, and mutual funds. The SEC is concerned primarily with promoting the disclosure of important market-related information, maintaining fair dealing, and protecting against fraud.
Stress Testing	A simulation technique used on asset and liability portfolios to determine their reactions to different financial situations. Stress tests are also used to gauge how certain stressors will affect a company or industry. They are usually computer-generated simulation models that test hypothetical scenarios.
Value-at-Risk (VaR)	A statistical technique used to measure and quantify the level of financial risk within a firm or investment portfolio over a specific time frame. Value at risk is used by risk managers in order to measure and control the level of risk which the firm undertakes. The risk manager's job is to ensure that risks are not taken beyond the level at which the firm can absorb the losses of a probable worst outcome.

IV. APPENDIX

SR 11-7 Guidance

SR 11-7 Attachment

OCC 2011-12

OCC 200-16 Guidance

AB_2013-07 Guidance