Comptroller's Handbook

Safety and Soundness

Capital Adequacy (C) | Asset Quality (A) | **Management (M)** | Earnings (E) | Liquidity (L) | Sensitivity to Market Risk (S) | Other Activities (O)

Model Risk Management

Version 1.0, August 2021

References to reputation risk have been removed from this booklet as of March 20, 2025. Removal of reputation risk references is identified by a strikethrough. Refer to OCC Bulletin 2025-4.

Office of the Comptroller of the Currency

Contents

Introduction **1**
Background 1
Risks Associated With the Use of Models 4
Strategic Risk 6
Operational Risk 6
~~Reputation Risk ..... 7~~
Compliance Risk 8
Credit Risk 9
Liquidity Risk 9
Interest Rate Risk 10
Price Risk 10

Risk Management **12**
Governance 13
Board and Management Oversight 15
Personnel 16
Model Owners 17
Independent Risk Management Staff 18
Internal Audit 19
Policies and Procedures 21
Risk Assessment 24
Planning 25
Model Inventory 26
Documentation 28
Data Management 29
Model Development, Implementation, and Use 30
Model Development and Implementation 31
Testing 32
Ongoing Development 33
Model Use 33
Model Overlays and Adjustments 34
Reporting 35
Model Validation 36
Evaluation of Conceptual Soundness 39
Ongoing Monitoring 42
Process Verification 43
Benchmarking 44
Outcomes Analysis 45
Back-Testing 47
Third-Party Risk Management 48
Third-Party Models and Data 48
Engaging Third Parties for Model Risk Management Activities 50
IT Systems 51

Examination Procedures 53
Scope 53
Quantity of Risk 55
Quality of Model Risk Management 58
Conclusions 82
Internal Control Questionnaire 84

Glossary 103

References 105

Introduction

The Office of the Comptroller of the Currency's (OCC) *Comptroller's Handbook* booklet, "Model Risk Management," is prepared for use by OCC examiners in connection with their examination and supervision of national banks, federal savings associations, and federal branches and agencies of foreign banking organizations (collectively, banks). Each bank is different and may present specific issues. Accordingly, examiners should apply the information in this booklet consistent with each bank's individual circumstances.

This booklet aligns with the principles laid out in the "Supervisory Guidance on Model Risk Management" conveyed by OCC Bulletin 2011-12, "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management" (MRM Supervisory Guidance). This booklet

- is designed to guide examiners in performing consistent, high-quality model risk management examinations.
- presents the concepts and general principles of model risk management.
- informs and educates examiners about sound model risk management practices that should be assessed during an examination.
- provides information needed to plan and coordinate examinations on model risk management, identify deficient practices, and conduct appropriate follow-up.

Supervisory Guidance on Model Risk Management

Throughout this booklet, information from the "Supervisory Guidance on Model Risk Management" is identified in boxes like this one. Refer to OCC Bulletin 2011-12 for the full text of the supervisory guidance.

Certain laws or regulations apply to specific **models**.[1] This booklet does not focus on specifics regarding compliance with these laws and regulations, as this booklet's focus is on a bank's model risk management for all models. Model risk management should be commensurate with the extent and complexity of model usage at a bank.

Background

Supervisory Guidance on Model Risk Management

For the purposes of this document, the term model refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. A model consists of three

[1] For example, certain banks must comply with ongoing model review, approval, and validation requirements as part of the advanced approaches risk-based capital rules, set forth at 12 CFR 3, subpart E, and the market risk rule, set forth at 12 CFR 3, subpart F. Terms that are **boldfaced** upon first mention in this booklet are defined in appendix A of this booklet.

components: an information input component, which delivers assumptions and data to the model; a processing component, which transforms inputs into estimates; and a reporting component, which translates the estimates into useful business information. Models meeting this definition might be used for analyzing business strategies, informing business decisions, identifying and measuring risks, valuing exposures, instruments or positions, conducting stress testing, assessing adequacy of capital, managing client assets, measuring compliance with internal limits, maintaining the formal control apparatus of the bank, or meeting financial or regulatory reporting requirements and issuing public disclosures. The definition of model also covers quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature. (See note 1.)

Note 1: While outside the scope of this guidance, more qualitative approaches used by banking organizations— i.e., those not defined as models according to this guidance—should also be subject to a rigorous control process.

A model may combine assumptions, data, and hypotheses about the behavior of markets or individuals, and process these inputs into quantitative estimates, forecasted outcomes, or predictions.

Supervisory Guidance on Model Risk Management

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

Because assumptions are typically simplifications of the actual relationships between inputs and outputs, and hypotheses about behavior are imprecise, there is some uncertainty associated with a model's estimate of the outputs, resulting in prediction errors.

Various models may focus on discriminatory power or predictive power as measures of model accuracy. Discriminatory power assesses a model's rank-ordering property, while predictive power focuses on the model output's prediction accuracy. A model focusing on discriminatory power need not produce the most accurate prediction, in the same way a model with the most accurate predictive power need not produce maximum rank-ordering.

In contrast to a model, a quantitative tool not meeting the definition of a model described in the MRM Supervisory Guidance may apply deterministic rules or algorithms[2] to process information and produce outcomes defined by the deterministic rules. For example, a tool

[2] An algorithm is a set of computational rules to be followed to solve a mathematical problem. More recently, the term has been adopted to refer to a process to be followed, often by a computer.

can include spreadsheet calculations using algebraic formulas, such as summation, or values for which the output is certain. Outputs produced by quantitative tools that are not models generally do not rely on sensitivity analysis or other methods to develop quantitative estimates, forecasted outcomes, or predictions. The determination by a bank of whether a quantitative tool is considered a model is bank-specific, and a conclusion regarding the tool's categorization should be based on a consideration of all relevant information. Risk management should be commensurate with the extent and complexity of the quantitative tool used. Risk management for quantitative tools that do not meet the definition of a model described in the MRM Supervisory Guidance may be significantly less robust than risk management for models.

Supervisory Guidance on Model Risk Management

Banks rely heavily on quantitative analysis and models in most aspects of financial decision making. They routinely use models for a broad range of activities, including underwriting credits; valuing exposures, instruments, and positions; measuring risk; managing and safeguarding client assets; determining capital and reserve adequacy; and many other activities.

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

Models can help increase automation, transparency, and consistency of bank activities. The number, scope, and complexity of models continue to increase over time. Examples of model uses include

- underwriting and managing credits.
- valuing trading exposures.
- pricing.
- risk hedging.
- managing client assets.
- measuring compliance with
  - internally established limits.
  - laws and regulations (including consumer protection-related laws and regulations).
- estimating the allowance for credit losses (ACL) and capital adequacy.
- issuing public disclosures.
- preventing and detecting fraud and money laundering.

The expanded use of models combined with their increasing complexity and value in decision making underscore the importance of sound model risk management. Additionally,

the incorporation of alternative data[3] contributes to model complexity while expanding access to credit and producing benefits for consumers.

Technological and analytical advances are contributing to increased model complexity and use. For example, **artificial intelligence** (AI),[4] including **machine learning**,[5] is used in a variety of ways. AI is broadly defined as the application of computational tools to address tasks traditionally requiring human analysis. Examples of AI uses in banks include fraud detection and prevention, marketing, chatbots, credit underwriting, credit and fair lending risk management, robo-advising (i.e., an automated digital investment advisory service), trading algorithms and automation, financial marketing analysis, cybersecurity, Bank Secrecy Act/anti-money laundering (BSA/AML) suspicious activity monitoring and customer due diligence, robotic process automation, and audit and independent risk management. Some AI may meet the definition of a model noted in the MRM Supervisory Guidance. While AI outputs are not always quantitative in nature, AI is typically based on complex mathematical techniques. Regardless of how AI is classified (i.e., as a model or not a model), the associated risk management should be commensurate with the level of risk of the function that the AI supports.

Risks Associated With the Use of Models

From a supervisory perspective, risk is the potential that events will have an adverse effect on a bank's current or projected financial condition[6] and resilience.[7] The OCC has defined eight categories of risk for bank supervision purposes: credit, interest rate, liquidity, price, operational, compliance, strategic, ~~and reputation~~. These risks are not mutually exclusive. Any product or service may expose a bank to multiple risks. Risks may also be interdependent and positively or negatively correlated. Examiners should be aware of and assess this interdependence. Examiners also should be alert to concentrations that can significantly elevate risk. Concentrations may accumulate within and across products, business lines, geographic areas, countries, and legal entities. Refer to the "Bank Supervision

[3] For more information, refer to OCC Bulletin 2019-62, "Consumer Compliance: Interagency Statement on the Use of Alternative Data in Credit Underwriting." Examples of alternative data uses in modeling by banks include using enhanced assessments of repayment capacity, including cash flow data, to evaluate the creditworthiness of consumers who currently may not obtain credit in the mainstream credit modeling system.

[4] AI can be used for such tasks as natural language processing, predictive analytics, recommendation engines, or recognition of images, patterns, or speech.

[5] Machine learning, a subcategory of artificial intelligence, is a method of designing a sequence of actions to solve a problem that optimizes automatically through experience and with limited or no human intervention. Refer to "Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications," Financial Stability Board (November 2017).

[6] Financial condition includes impacts from diminished capital and liquidity. Capital in this context includes potential impacts from losses, reduced earnings, and market value of equity.

[7] Resilience recognizes the bank's ability to withstand periods of stress. For more information on the risk assessment system, refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook*.

Process" booklet of the *Comptroller's Handbook* for an expanded discussion of banking risks and their definitions.

Model use can affect risk in all eight categories of risk. The use of models can increase or decrease risk in each risk category depending on the models' purpose, use, and the effectiveness of any relevant model risk management. Conceptually, model risk is a distinct risk that can influence aggregate risk across all risk categories. Model risk can increase due to interactions and dependencies among models, such as reliance on common assumptions, inputs, data, or methodologies.

Supervisory Guidance on Model Risk Management

The use of models invariably presents model risk, which is the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports. Model risk can lead to financial loss, poor business and strategic decision making~~, or damage to a bank's reputation~~. Model risk occurs primarily for two reasons:

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

Banks should identify the sources of risk and assess the magnitude. Model risk increases with greater model complexity, higher uncertainty about inputs and assumptions, broader use, and larger potential impact. Banks should consider risk from individual models and in the aggregate. Aggregate model risk is affected by interaction and dependencies among models; reliance on common assumptions, data, or methodologies; and any other factors that could adversely affect several models and their outputs at the same time. With an understanding of the source and magnitude of model risk in place, the next step is to manage it properly.

The risks associated with model use can occur at any point during a model's development, implementation, use, and **validation**. A bank's risk profile can increase depending on a model's complexity, the technologies used to implement models, higher uncertainty about inputs and assumptions, broader model use, larger potential impact on the bank's financial condition or compliance with laws and regulations, and weaknesses in model governance. It is important to consider risk from individual models and in the aggregate.

Inaccurate measurement of risk or relying on models that are not used as originally intended can result in poor decision making. Without proper model risk management, model input errors, inaccurate assumptions, and untimely or missing validations can result in risk measurements that are inaccurate or misrepresented, and therefore board and management decisions that are based on inaccurate or irrelevant model outputs. More generally, inadequate governance over models' development, implementation, use, and validation can increase risk. It is important for a bank's decision makers to understand a model's limitations to avoid using a model in ways not originally intended or if the model has not been validated.

Strategic Risk

Strategic risk is the risk to current or projected financial condition and resilience arising from adverse business decisions, poor implementation of business decisions, or lack of responsiveness to changes in the banking industry and operating environment.

The board of directors and senior management are the key decision makers that drive the strategic direction of the bank and establish a governance framework for using models. The absence of an appropriate governance framework for developing, implementing, using, and validating models poses strategic risk. A bank's strategic risk can increase if models and associated risk management do not keep pace with strategic changes, the capability of employees, the operating environment, and regulatory requirements. For example, failure to adjust model inputs and assumptions for current and anticipated market conditions, the macroeconomic environment, and consumer behaviors could expose the bank to strategic risk, which may translate into financial losses.

Operational Risk

Operational risk is the risk to current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events.

Operational risk is the primary risk associated with the use of models. Failed or inadequate processes and systems and errors or misconduct by personnel can significantly affect the predictive value of a model. Operational risk can result from fundamental errors in a model when viewed against the design objective and intended business uses without sufficient use of **model overlays**[8] and adjustments when model limitations become apparent. Personnel who do not have sufficient skills and training to develop, implement, use, and validate the

[8] A model overlay is a judgmental or qualitative adjustment to model inputs or outputs to compensate for model, data, or other known limitations. A model overlay is a type of override.

bank's models can increase operational risk. Modeling errors or omissions can occur in the application of theory, data inputs, algorithms, assumptions, shortcuts, simplifications, and approximations, which can lead to inaccurate outputs.

Management's failure to engage in appropriate model risk management to prevent errors and improper use of models can increase operational risk. For example, operational risk can increase when algorithms are based on biased, insufficient, incomplete, or inaccurate information, or are not properly tested and validated. Models can fail because of inadequate internal controls, such as insufficient processes for controlling the quality of the data inputs. The absence of an appropriate change management process for new technologies, products, or service offerings related to models can also increase operational risk.

Operational risk can increase when the information technology (IT) environment supporting the bank's models does not have appropriate internal controls. Security weaknesses, including poorly constructed application program interfaces (API)[9] and weaknesses in the controls for the access, transmission, and storage of sensitive customer information, could expose a bank to increased operational risk. Weak or lax controls can compromise the confidentiality or integrity of sensitive customer data.

Third-party risk management weaknesses related to a bank's use of third parties providing models or related products and services could increase operational risk, particularly when management does not fully understand a third-party model's capabilities, applicability, and limitations. New technologies, products, and services, such as AI and data aggregation, can increase third-party access to banks' IT systems. When a bank allows third parties to connect to the bank's models and systems and to access customer information, there can be substantial operational risk. Poorly drafted contracts could increase operational risk. Important considerations include the ability of the third party to resell, assign, or permit access to the bank's data and IT systems to other entities and how the data will be transmitted, accessed, and used.

~~Reputation Risk~~

~~Reputation risk is the risk to current or projected financial condition and resilience arising from negative public opinion. Reputation risk may impair the bank's competitiveness by affecting its ability to establish new relationships or services, or continue servicing existing relationships.~~

~~Inadequate policies and processes, operational breakdowns, or other weaknesses in any aspect of model risk management or governance can increase reputation risk. A bank could incur reputation risk from biased data outcomes, data losses, noncompliance with regulations, fraud, downtime, and insufficient consumer protections. Biased data outcomes can result in potential disparate treatment or disparate impact on borrowers on a prohibited basis. Third-party risk management weaknesses and wrongful acts by third parties could increase~~

[9] API is software code that allows two or more programs to communicate with each other. For more information, refer to the Federal Financial Institutions Examination Council's IT Examination Infobase's Glossary.

~~reputation risk. A sound corporate culture is the foundation of a sound governance framework and helps form a positive public perception of the bank.~~

Compliance Risk

Compliance risk is the risk to current or projected financial condition and resilience arising from violations of laws or regulations, or from nonconformance with prescribed practices, internal bank policies and procedures, or ethical standards.

Compliance risk is elevated when banks do not comply with model-related laws and regulations. For example, risk-weighted asset regulations dictate requirements for certain banks' capital measurement models.[10] Compliance risk is also elevated when models result in potential discrimination on a prohibited basis or other violations of consumer protection-related laws and regulations.

A bank's compliance risk can increase when models used in the bank's BSA/AML[11] and Office of Foreign Assets Control (OFAC) programs inaccurately reflect the risk of a bank's business model, products, services, customer base, and geographic footprint. One example is setting and tuning thresholds in a BSA/AML or OFAC model without taking differences in risk levels across lines of business, products, services, customer types, and geographies into account.[12]

A bank's fair lending compliance risk could increase when a bank's credit decisioning models include algorithms, variables, or other processes that result in disparate impact on credit applicants or customers based on prohibited factors, such as race, ethnicity, or sex.[13] The source of the bias may be obscured by the model's complexity if management does not properly understand and manage the model. Even when individual variables are not inherently biased on a standalone basis, the complex interactions typical of some models (e.g., models using AI approaches) could lead to unintended impacts or outcomes.

[10] Certain banks must comply with ongoing model review, approval, and validation requirements as part of the advanced approaches risk-based capital rules, set forth at 12 CFR 3, subpart E, and the market risk rule, set forth at 12 CFR 3, subpart F.

[11] The "Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance" conveyed by OCC Bulletin 2021-19, "Bank Secrecy Act/Anti-Money Laundering: Interagency Statement on Model Risk Management for Bank Systems Supporting BSA/AML Compliance and Request for Information," addresses the unique risks relating to BSA/AML and the objectives and structures of BSA models. This statement specifically addresses how the risk management principles described in the MRM Supervisory Guidance relate to systems or models used by banks to assist in complying with the requirements of BSA/AML laws and regulations.

[12] The objectives and structure of BSA/AML models (models used in a bank's BSA/AML program) may differ from those in other business units because the objectives of most BSA/AML models place greater emphasis on coverage over efficiency. BSA/AML models may require quick adjustments to reflect the changing nature of criminal behavior or the bank's risk profile. Likewise, testing and performance monitoring for some BSA/AML models may not include the same techniques as other models because of various factors, such as the lack of information about realized outcomes (e.g., Suspicious Activity Reports).

[13] For more information, refer to the "Fair Lending" booklet of the *Comptroller's Handbook*.

Compliance risk can be elevated if management does not understand the requirements of consumer protection-related laws and regulations and the enhanced controls that should be implemented when using alternative data in models.[14]

Credit Risk

Credit risk is the risk to current or projected financial condition and resilience arising from an obligor's failure to meet the terms of any contract with the bank or otherwise perform as agreed. Credit risk exists any time bank funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether reflected on or off the balance sheet.

Banks use models to increase efficiency in all stages of lending, including marketing; underwriting; pricing; collateral valuation; risk ratings for obligors, counterparties, and transactions; stress testing individual loans; portfolio monitoring; and risk mitigation. If credit risk models do not incorporate underwriting changes in a timely manner, flawed and costly business decisions could occur. In addition, model error or ineffective model risk management can lead to credit decisions inconsistent with the bank's policy or risk appetite and higher credit risk exposure than projected. Conversely, models that are well-designed and effectively managed can help management make prudent risk selection and monitor and manage credit risk.

Banks may rely on a model to estimate the ACL, or uncollectible amounts maintained through charges to a valuation reserve adjusted through a bank's operating income. Models used to estimate ACL do not create credit risk. Rather, the ACL quantifies the credit risk inherent in the bank's assets. A deficient model can mask credit risk in financial assets, hinder effective identification of higher-risk assets, delay the recognition of credit losses, and result in an inappropriate ACL balance.

Liquidity Risk

Liquidity risk is the risk to current or projected financial condition and resilience arising from an inability to meet obligations when they come due.

Liquidity risk can increase because of inaccurate or untimely inputs, assumptions, model adjustments, and outputs. Accurate information on the bank's liquidity position is necessary to monitor liquidity risk. Inaccurate or unreasonable model assumptions related to funding access (e.g., deposit flows, wholesale funding availability, and timing) can increase liquidity risk. Management's failure to adjust model inputs based on changes in market conditions can increase liquidity risk. For example, inaccurate pricing models may hinder a bank's ability to liquidate assets quickly for a reasonable price. Examples of some common sources of liquidity risk in modeling are unsupported or unreasonable contingent funding assumptions; stress scenarios that do not consider all relevant legal or regulatory constraints; and

[14] For more information, refer to OCC Bulletin 2019-62.

inaccurate or unsupported behavioral assumptions (e.g., budgets, loan pipelines, rollover, and embedded optionality).

Interest Rate Risk

Interest rate risk is the risk to earnings or capital arising from movements in interest rates. Interest rate risk arises from differences in the timing of rate changes and the timing of cash flows, from changing rate relationships among yield curves or across maturities, and interest-related embedded options in bank products.

A bank's interest rate exposure depends on (1) the sensitivity of an instrument's expected income/expense and economic value to a given change in market rates, and (2) the magnitude and direction of this change in market interest rates. Interest rate risk models depend on assumptions to accurately project cash flows from assets (e.g., prepayments, embedded options, and complex loan terms), liabilities (e.g., non-maturity deposit pricing, decay assumptions, and embedded options), and off-balance-sheet items. Scenario design is highly dependent on reasonable assumptions for time horizon, rate structure, and magnitude of stress scenarios. Examples of some common interest rate modeling issues are (1) failing to assess potential exposures over a sufficiently wide range of interest rate movements to identify vulnerabilities and stress points; (2) failing to modify or vary assumptions for products with embedded options to reflect individual rate scenarios; (3) basing assumptions solely on past customer behavior and performance without considering how the bank's competitive market and customer base may change; and (4) failing to periodically assess the reasonableness and accuracy of assumptions.[15]

Price Risk

Price risk is the risk to current or projected financial condition and resilience arising from changes in the value of either trading portfolios or other obligations that are entered into as part of distributing risk. These portfolios typically are subject to daily price movements and are accounted for primarily on a mark-to-market basis.

A bank incurs heightened price risk when trading instruments with prices that are hard to model. Examples include

- instruments that are illiquid or trade infrequently, because of limited data.
- newer instruments, because of limited data.
- instruments whose pricing model assumes a certain relationship between two variables (typically correlation), because that relationship can change.
- instruments with fair value that depends on accurately modeling human behavior (e.g., prepayment speeds and deposit betas), because human behavior is often unpredictable.

[15] For more information on interest rate risk models, refer to the "Interest Rate Risk" booklet of the *Comptroller's Handbook*; OCC Bulletin 2012-5, "Interest Rate Risk Management: FAQs on 2010 Interagency Advisory on Interest Rate Risk Management"; and OCC Bulletin 2010-1, "Interest Rate Risk: Interagency Advisory on Interest Rate Risk Management."

Banks use models (primarily value-at-risk and similar expected shortfall models) to measure trading activities' aggregate price risk. Value-at-risk and similar expected shortfall models determine how much capital a bank with significant trading activity should hold against the bank's trading book. Management's improper use of models to manage price risk could result in inadequate capital allocation relative to the size and nature of trading exposures. Compounding the problem, models may depend on other models, as one of the key inputs to a value-at-risk model is the fair value of the trading book, which can depend significantly on pricing models.

Risk Management

Each bank should identify, measure, monitor, and control risk by implementing an effective risk management system appropriate for the size and complexity of its operations. When examiners assess the effectiveness of a bank's risk management system, they consider the bank's policies, processes, personnel, and control systems. Refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook* for an expanded discussion of risk management.

Supervisory Guidance on Model Risk Management

Model risk should be managed like other types of risk.

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

Details may vary from bank to bank, as practical application of this guidance should be customized to be commensurate with a bank's risk exposures, its business activities, and the complexity and extent of its model use. For example, steps taken to apply this guidance at a community bank using relatively few models of only moderate complexity might be significantly less involved than those at a larger bank where use of models is more extensive or complex.

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

Appropriate model risk management governs the use of models, fits into the bank's overall governance framework, and helps confirm a bank's risk-taking activities are aligned with its strategic objectives and risk appetite.[16]

[16] Key components of a governance framework include the bank's risk culture, risk appetite, and risk management system. For more information, refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook.*

Model risk management should be commensurate with the extent and complexity of model usage at a bank. The extent and rigor of a bank's model risk management should be tailored to the material impact on business decisions. For example, failure to manage risks associated with capital and liquidity planning models could have a particularly harmful impact on a bank's financial condition.

Sound risk management should be applied to models and tools not meeting the definition of a model described in the MRM Supervisory Guidance. Risk management of AI, as with any other innovative technology, should be commensurate with the materiality and complexity of the model or tool and the activity's risk or business process that the AI is supporting. Sound AI risk management typically includes

- appropriate due diligence and risk assessments as AI is implemented.
- sufficiently qualified staff to implement, operate, and control the risks associated with AI.
- an inventory of AI uses.
- identification of the level of risk associated with each AI use.[17]
- establishment of clear and defined parameters governing the use of AI.
- effective processes to validate that AI use provides sound, fair, and unbiased results.
- effective technology controls, such as system and data access, identity and authorization, system integration, separation of duties, configuration management, vulnerability management, encryption, malware controls, business resilience, system change control, monitoring and logging, data management, and other similar controls.

Supervisory Guidance on Model Risk Management

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

Governance

Sound model governance includes board and management oversight, policies and procedures, a system of internal controls, internal audit, a model inventory, and documentation. A common risk management system used in many banks, formally or informally, involves three lines of defense: (1) frontline units, business units, or functions that create risk; (2) independent risk management (IRM), loan review, compliance officer, and chief credit officer to assess risk independent of the units that create risk; and (3) internal audit, which provides independent

[17] The level of risk may be higher for AI used to aid with a bank's compliance with laws, protect customer information, or perform critical operational functions.

assurance.[18] Effective communication among the lines of defense, while maintaining independence, promotes sound model risk management.

Personnel providing effective challenge[19] and critical analysis over model risk management should have appropriate training and knowledge. Personnel providing effective challenge should be able to recommend appropriate actions and escalation of issues, if warranted. Examiners should assess the extent to which personnel providing effective challenge have explicit authority and stature within the bank, and commitment and support from higher levels of management.

Supervisory Guidance on Model Risk Management

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

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

The responsibilities for risk controls may be assigned to individuals, committees, or a combination of the two, and include risk measurement, limits, and monitoring. Other responsibilities include managing the independent validation and review process to ensure that effective challenge takes place.

In small, noncomplex banks, model risk management and internal controls are often integrated in the frontline units. The bank should have additional controls when model development and validation functions are structured in the same line of defense and reporting to one individual. An example of additional controls includes a process to escalate conflicting views between the model development and validation groups. Protocol could include escalating conflicts to a management committee that votes to ultimately decide and resolve the conflict. If the individual responsible for regular oversight of model development and validation is a member of the designated management committee, the individual is typically recused from the vote.

Supervisory Guidance on Model Risk Management

A guiding principle for managing model risk is "effective challenge" of models, that is, critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate changes. Effective challenge depends on a combination of incentives,

[18] For more information, refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook.*

[19] For the purposes of this booklet, effective challenge is synonymous with credible challenge. For more information on credible challenge, refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook*.

competence, and influence. Incentives to provide effective challenge to models are stronger when there is greater separation of that challenge from the model development process and when challenge is supported by well-designed compensation practices and corporate culture. Competence is a key to effectiveness since technical knowledge and modeling skills are necessary to conduct appropriate analysis and critique. Finally, challenge may fail to be effective without the influence to ensure that actions are taken to address model issues. Such influence comes from a combination of explicit authority, stature within the organization, and commitment and support from higher levels of management.

Board and Management Oversight

Supervisory Guidance on Model Risk Management

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

While the board is ultimately responsible, it generally delegates to senior management the responsibility for executing and maintaining an effective model risk management framework. Board members should ensure that the level of model risk is within their tolerance and direct changes where appropriate. These actions will set the tone for the whole organization about the importance of model risk and the need for active model risk management.

Model risk governance should reflect a sound corporate culture. The board is responsible for setting the tone at the top and overseeing management's role in fostering and maintaining a sound corporate culture that does not condone or encourage imprudent risk taking, unethical behavior, or the circumvention of laws, regulations, or safe and sound policies and procedures in pursuit of profits or objectives. Risk culture, an important subset of corporate culture, pertains to the bank's approach to model risk management, and is critical to a sound governance framework.

The board typically delegates specific duties and authorities for managing risk to board committees, management committees, and senior management. Senior management is responsible for day-to-day implementation of sound model risk management.

Supervisory Guidance on Model Risk Management

Duties of senior management include establishing adequate policies and procedures and ensuring compliance, assigning competent staff, overseeing model development and implementation, evaluating model results, ensuring effective challenge, reviewing validation and internal audit findings, and taking prompt remedial action when necessary. In the same manner as for other major areas of risk, senior management, directly and through relevant committees, is responsible for

regularly reporting to the board on significant model risk, from individual models and in the aggregate, and on compliance with policy.

A bank's risk appetite for model use reflects the level and types of risk that the board and management are willing to assume. Defining parameters around exceptions, management **overrides**,[20] policy deviations, and limits on model use helps management operate within the bank's risk appetite. Targets for model accuracy, which are reasonable and acceptable limits for a model to deviate from estimated or predicted results, are important measures for assessing adherence to the risk appetite.

Sound governance encourages all key stakeholders to have effective communication, be transparent, and actively participate in model risk management. Sound governance includes effective challenge of models and their related governance and risk management processes. The board and management should promote a working environment that supports and encourages effective challenges to risk analysis, validation, testing, development, and other processes related to a bank's model risk management.

Appropriate change management before implementing or when changing models and related technologies is an important component of model governance. Change management processes address changes in such areas as model development and implementation, personnel, policies, testing and validation, IT systems, regulatory requirements, and internal controls. Some banks hire third parties with specialized expertise in the technologies used to develop models, underscoring the importance of appropriate third-party risk management.[21]

Board and board committee meeting minutes can provide evidence of appropriate board oversight of model risk management. Well-documented meeting minutes generally include sufficient information to reflect that directors are fully informed about the relevant facts and understand the risks associated with a bank's use of models, deliberate significant issues, act independently, provide effective challenge when necessary, make decisions based on the best interests of the bank, and approve previous meeting minutes.[22]

Personnel

The bank should have competent and qualified personnel[23] to execute and oversee model risk management. Effective training and communication help ensure that relevant personnel understand the bank's models. Sufficient personnel resources should be allocated for model activities and functions.

[20] Overrides occur when model output is ignored, altered, or reversed.

[21] Refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"; OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures"; and OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29."

[22] The "Corporate and Risk Governance" booklet of the *Comptroller's Handbook* provides more information regarding board and board committee minutes.

[23] Personnel are the bank managers and staff who execute or oversee a bank's policies, standards, and processes.

The skills and expertise of management and other personnel should be commensurate with the nature, extent, and complexity of the use of models. It is important to have personnel with the skills to appropriately manage, maintain, test, and validate models. Technical knowledge and modeling skills are necessary to conduct meaningful analysis and challenge with respect to a model's development, implementation, use, and validation. The bank should have personnel with the requisite skills to manage IT systems supporting a bank's models, and the models' related controls. It is also important to have personnel who can communicate information in nontechnical terms to the board.

Well-thought-out personnel development, recruiting, succession planning, and compensation processes promote successful hiring and retention of individuals with highly technical skills for model development and for model risk management across the three lines of defense. Training and professional development programs are important for developing and maintaining a talent pool and further developing required skills and knowledge, particularly as the bank's complexity and extent of model use increase. Incentive compensation programs should be designed to appropriately balance risk taking and reward.[24]

Model Owners

Supervisory Guidance on Model Risk Management

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

Model owners typically are in individual business units. In addition to the responsibilities outlined in the MRM Supervisory Guidance model owners are generally responsible for

- implementing policies, standards, and processes for model risk management within the business unit.
- establishing and maintaining
  - processes for identifying, measuring, monitoring, and controlling the risks associated with the business unit's models, consistent with the established risk appetite.
  - internal controls that are properly designed, tested, and work effectively.
  - testing during model development, implementation, and use.
  - documentation standards for processes and related decisions for business unit models, for example, documentation of decisions resulting in changes to the model components.

[24] For more information regarding compensation, refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook*. For guidance regarding incentive compensation programs, refer to OCC Bulletin 2010-24, "Incentive Compensation: Interagency Guidance on Sound Incentive Compensation Policies."

Independent Risk Management Staff

Supervisory Guidance on Model Risk Management

Model risk taken by business units should be controlled. Appropriate resources should be assigned for model validation and for guiding the scope and prioritization of work. Issues and problems identified through validation and other forms of oversight should be communicated by risk-control staff to relevant individuals and business users throughout the organization, including senior management, with a plan for corrective action. Control staff should have the authority to restrict the use of models and monitor any limits on model usage. While they may grant exceptions to typical procedures of model validation on a temporary basis, that authority should be subject to other control mechanisms, such as timelines for completing validation work and limits on model use.

As the second line of defense, IRM typically oversees business unit risk-taking and risk management activities.[25] IRM validates and challenges business unit testing and other first-line model risk management processes. IRM validation is done independently from model owners (e.g., business unit personnel) and model developers (including third parties). IRM's access to the board or board committees to discuss concerns identified through risk management and validation activities promotes independence and effective challenge. IRM typically is responsible for

- implementing policies, standards, and processes for model risk management within the business unit.
- establishing and implementing processes for identifying, measuring, monitoring, and controlling risks enterprise-wide, for individual models and in the aggregate.
- validating[26] the model inputs and outputs.
- confirming that the bank's models are performing as intended.
- validating controls established by the business units and introducing additional controls, such as automated processes, user access controls, and documentation standards.
- assessing identified issues for themes or patterns.
- providing effective challenge to business unit risk management processes.
- independently measuring risk.
- reporting to senior management and the board
  - business units' adherence to the bank's risk appetite.
  - differences in risk opinion between business units and IRM.
  - on monitoring of risks enterprise-wide and providing input into key risk decisions.

[25] For the purposes of this booklet, "control staff" is synonymous with IRM.

[26] The validation process is described in more detail in the "Model Validation" section of this booklet.

Internal Audit

As the third line of defense, internal audit reviews model governance and risk management and provide independent assurance to the board on the effectiveness of governance, risk management, and internal controls. Internal audit is independent from the other lines of defense. Internal audit tests the validation conducted by IRM. Well-planned, properly structured audit programs are essential to effective risk management and internal control systems and are also a critical defense against fraud.[27] Internal audit has an important role in confirming that model validation is conducted appropriately, and effective challenge is being provided independently.

Supervisory Guidance on Model Risk Management

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

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

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

[27] For more information on effective audit functions, refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook.*

Internal audit is typically responsible for

- assessing the overall effectiveness of model risk management, including the framework's ability to address model risk for individual models and in the aggregate.
- evaluating whether model risk management is comprehensive, rigorous, and effective.
- verifying that acceptable policies are in place and are appropriately adhered to.
- documenting and reporting its findings to the board or the audit committee in a timely manner.
- verifying records of model use and validation to test whether
  - validations are performed in a timely manner.
  - models are subject to controls that appropriately account for any weaknesses in validation activities.
- assessing the accuracy and completeness of the model inventory.
- evaluating the processes for establishing and monitoring limits on model usage.
- determining whether procedures for updating models are clearly documented, and testing whether those procedures are being carried out as specified.
- assessing adherence to documentation standards, including risk reporting.
- performing assessments of supporting operational systems.
- evaluating the reliability of data used by models.
- assessing potential biases in the data that may result in heightened risk, such as fair lending concerns (either for disparate treatment or disparate impact on a prohibited basis).
- evaluating the objectivity, competence, and organizational standing of the key validation participants, with the ultimate goal of ascertaining whether those participants have the right incentives to discover and report deficiencies.
- assessing if personnel involved in model development and model use are independent from model validators, to the extent possible.
- reviewing the validation activities conducted by internal personnel and third parties, with the same rigor, to assess the appropriateness of validation activities.
- assessing whether there is sufficient reporting to the board and senior management to evaluate whether bank management is operating within the bank's risk appetite and limits for model risk.

Audits must be performed by independent and competent staff who are objective in evaluating the bank's control environment.[28] Qualified personnel leading model development and model validation typically have highly technical and very similar skill sets. Because of this, such individuals may tend to discuss issues and consult with one another on an ad hoc or informal basis, which could jeopardize independence of the two functions, and the separation of first and second lines of defense.

Many banks outsource or co-source internal audits, particularly when the in-house internal audit staff do not have the sufficient technical skills. Banks should exercise appropriate due diligence before entering a third-party relationship and should implement effective oversight

[28] Refer to 12 CFR 30, appendix A, II.B, "Internal Audit System."

and controls afterward.[29] Small or noncomplex banks, particularly those with limited model use, may not have a standalone model audit. In those instances, examiners should consider how internal audits' reviews of other areas assess model risk management. Examiners should assess the qualifications and expertise of in-house, outsourced, or co-sourced audit staff.

Policies and Procedures

Supervisory Guidance on Model Risk Management

Consistent with good business practices and existing supervisory expectations, banks should formalize model risk management activities with policies and the procedures to implement them. Model risk management policies should be consistent with this guidance and also be commensurate with the bank's relative complexity, business activities, corporate culture, and overall organizational structure. The board or its delegates should approve model risk management policies and review them annually to ensure consistent and rigorous practices across the organization. Those policies should be updated as necessary to ensure that model risk management practices remain appropriate and keep current with changes in market conditions, bank products and strategies, bank exposures and activities, and practices in the industry. All aspects of model risk management should be covered by suitable policies, including model and model risk definitions; assessment of model risk; acceptable practices for model development, implementation, and use; appropriate model validation activities; and governance and controls over the model risk management process.

Policies should emphasize testing and analysis, and promote the development of targets for model accuracy, standards for acceptable levels of discrepancies, and procedures for review of and response to unacceptable discrepancies. They should include a description of the processes used to select and retain vendor models, including the people who should be involved in such decisions.

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

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

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

[29] For more information, refer to the "Internal and External Audits" booklet of the *Comptrollers Handbook* and OCC Bulletin 2013-29.

Policies and procedures regarding model risk management, which may vary based on the type and objectives of the bank's models, may

- describe governance and controls over the model risk management process.
- establish model risk management internal controls.
- describe the model risk management framework and how the framework is applied to different types of models.
- require maintenance of detailed documentation of all aspects of the model risk management framework.
- include definitions of a model and model risk and criteria for when model risk management policies should be applied.
- describe the process for assessing model risk.
- define acceptable practices for model development, including redevelopment; implementation; use; and validation for all models, including third-party models.
- identify roles and responsibilities of stakeholders with clear detail on expertise, authorities, reporting lines, and continuity.
- include standards for an inventory of models in use.
- describe how models will be used for business decisions and strategies.
- include fair lending considerations, including standards that help ensure models do not cause or promote discrimination (either through disparate treatment or disparate impact) on a prohibited basis under the Equal Credit Opportunity Act or Fair Housing Act.
- describe controls for model development, implementation, and use such as
  - controls to ensure data quality and relevance for effective modeling.
  - model approval and change management processes.
  - limits on model use (e.g., when model deficiencies are known and/or waiting to be remedied through appropriate testing and analysis).
  - supplementing model results with other analysis and information.
  - authorities to restrict model usage.
  - controls to protect access to sensitive customer information and data.
  - controls to monitor for potential discriminatory outputs or results.
  - testing the accuracy and completeness of data feeds, confirming related systems are properly integrated, and conducting parallel testing and user acceptance testing before implementation.
  - requirements for approving changes for models moving into production.
- define acceptable practices for the use of models with outputs that are dependent on other models as inputs or the use of models that are part of a model suite.[30]
- include standards for the development of thresholds for model accuracy and other performance measures.
- include procedures for reviewing and responding to unacceptable discrepancies.
- include standards for acceptable levels of discrepancies between model outcomes and actual or benchmark outcomes.
- include standards for determining the sensitivity of model inputs.

[30] For purposes of this booklet, a model suite is a group of models that work together.

- include standards for documentation of model choices with supporting rationale, for example, key assumptions, data inputs, model design, conservative adjustments and other adjustments, data exclusions, and logic underlying the model.
- include standards for documentation of conceptual understanding of models, including AI approaches.
- define acceptable practices for the review, approval, use, and back-testing of model overlays, or other adjustments to the bank's models.
- define appropriate model validation activities, which may include
  - a program of ongoing monitoring and evaluation of model performance based on the risk of the model, with appropriate benchmarking and back-testing.
  - the prioritization, scope, and frequency of validation activities, including AI models' underlying algorithms and parameters that are frequently updated as new data arrive.
  - standards for the extent of validation that should be performed before models are put into production.
  - standards for the extent of revalidation that should be performed before models are put in use after material changes are made.
  - standards for the review and decision process when a model should be removed from production.
  - procedures for responding to problems that appear.
  - requirements for validation of third-party models.
  - standards for documenting model validation results.
  - controls on the use of external resources for validation.
- describe escalation processes and remediation actions for model issues, limit breaches, and policy exceptions.
- describe standards for timely resolution of model issues.
- require documentation of model issues and the resolution of issues.
- describe the bank's methodology for assessing model risk.
- include standards for periodically reviewing and updating, when warranted, model risk assessments.
- describe model risk reporting processes that address data/information, distributions to all relevant stakeholders, and escalation protocols to the board and, when necessary, the OCC.
- establish communication standards for the communication of risk culture, appetite, controls, and related responsibilities and accountability throughout the bank.
- describe the process used to select and retain third-party models, including the staff who should be involved in such decisions.
- define expectations for personnel and third parties regarding accessing, transferring, sharing, storing, and securing sensitive customer information used in models.
- reference other relevant policies related to third-party risk management.
- include standards for contract provisions that protect the bank's needs and rights, including privacy and customer information protection and providing for regulator access to information.
- define expectations for ongoing monitoring of third parties.
- include standards for the establishment of contingency plans for instances in which third-party models are no longer available or serviced or are no longer reliable.

- describe the methodology to periodically reassess the reasonableness and accuracy of model assumptions.
- include standards for data management, such as standards for
  - assessment of data sources, quality, limitations, completeness, and relevance.
  - using **data proxies**, i.e., data that are closely related to and serve in place of data that are either unobservable or immeasurable.
  - using third-party data.
  - using alternative data.
  - securing data.

Risk Assessment

Supervisory Guidance on Model Risk Management

Banks should consider risk from individual models and in the aggregate. Aggregate model risk is affected by interaction and dependencies among models; reliance on common assumptions, data, or methodologies; and any other factors that could adversely affect several models and their outputs at the same time.

Assessing risk includes identifying and measuring the sources and magnitude of risks associated with model use. This is particularly important as a bank increases in size and complexity, the use of models becomes more widespread, or model results significantly influence decision making. Interrelationships among models, assumptions, and data can increase a bank's risk profile. To properly identify risk, each model's capabilities and limitations should be identified and well understood.

Examiners should assess model risk assessment processes. Many banks use a model rating methodology to assess the risk associated with their models. A sound model risk assessment process generally

- identifies risk both from individual models and models in the aggregate.
- identifies the model's capabilities and limitations.
- measures the risks associated with model activities accurately and in a timely manner.

Assessing risk is a continual process. Rating methodologies are often based on the model type and objectives; complexity, uncertainty, and materiality; interrelationships; data; and capabilities and limitations. Banks also typically use model risk assessments to help determine the types, frequency, and extent of model validation activities and allocated resources. If the bank uses AI models, examiners should assess if model ratings take **explainability**[31] into account.

Identifying and measuring risks associated with the use of models is critical for banks undergoing mergers and consolidations, to appropriately address risks arising from each

[31] In the context of AI, explainability is the extent to which AI decisioning processes and outcomes are reasonably understood by bank personnel.

bank's individual models, and in the aggregate. Model-related risk assessments in mergers or consolidations often begin with understanding the target bank's model inventory and aligning uniform definitions of models and their sources of risk. Any open issues related to the target bank's models or model risk management are also considered.

Planning

Effective governance for modeling begins with appropriate planning. A clear statement of purpose is typically the first step to developing models aligned with the intended use. Management typically performs a comprehensive and objective risk assessment before selecting a new model.[32]

Board and management decisions to implement new models or revise models should be based on sound, complete information, realistic assessments of the risks involved, management's expertise, and the bank's operating capacity. Banks generally implement change management processes that cover changes in bank strategy, regulatory requirements, or new technologies, products, and services. For example, AI uses large amounts of data and may connect to multiple systems, which could necessitate coordination of pre-implementation changes in personnel, policies, processes, IT systems, and internal controls. Some key planning considerations include:

- Has management identified all stakeholders and other users that are affected by implementation of new or revised models and coordinated accordingly?
- Has management performed an appropriate risk assessment, including assessing the risk of potential critical third parties, before designing or selecting new models?
- Is management's decision to implement new models or revise models based on sound and complete information, realistic assessments of the risks involved, management's expertise, and the bank's operating capacity?
- Has senior management identified which technology, products, and services associated with models would best fit with its overall strategic plan, goals, risk appetite, and, as appropriate, specific model objectives?
- Has management identified the impact of changes in economic conditions and the business environment that could affect model risk?
- Does senior management understand the purpose of models, models' limitations, and how models work?
- Can new technology and data management associated with new models be integrated with the bank's legacy systems?
- Are there appropriate controls for monitoring outputs or results that are potentially discriminatory on a prohibited basis?
- Are there appropriate controls for protecting sensitive customer information?
- Are policies, processes, and staffing appropriate for supporting the model? If not, are appropriate changes to policies, process, and staffing planned?

[32] For more information, refer to the "Risk Assessment" section of this booklet.

- Is the technology supporting the model or the model's management information systems (MIS) scalable (e.g., will the technology be able to handle an increased customer base, processing volumes, and data, and be able to adjust to consumer wants and needs)?
- Do personnel have appropriate expertise to carry out plans effectively and in a manner that is consistent with the bank's model risk management framework?

Examiners should consider how senior management determines the effect of new products and services on the bank's existing models. Appropriate controls should be implemented before any model or related technology is implemented. New products and services[33] may warrant adjustments to models and controls to manage associated risks. In some cases, model replacement could be appropriate.

Examiners should assess the appropriateness of the bank's resiliency plan for potential interruptions in the functioning of critical models, such as power outages or natural disasters. Sound model resiliency planning provides for

- identifying, in a timely manner, performance deterioration due to interruptions.
- modifying model risk management processes when significant interruptions occur.
- considering new data points from unprecedented scenarios (e.g., pandemics or other significant disruptions) and determining whether these should be included in model assumptions to help ensure the reasonableness of model outputs.

Model Inventory

Supervisory Guidance on Model Risk Management

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

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

[33] For more information on new products and services, refer to OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles."

A comprehensive set of information for models (model inventory) may include the following:

- Model identifier.
- Model version.
- Whether the model was developed in-house or by a third party.
- Model dependency, describing whether the outcome of one model is being used as input into another model.
- Model owner and user(s) by title or group (e.g., chief compliance officer or compliance department).
- Status of model (e.g., in development, production, decommissioned).
- Approval date of model, or timeline for approval.
- Description of the purpose and products for which the model is designed.
- Description of actual or expected usage.
- Description of any restrictions on use or other controls (e.g., more frequent monitoring and appropriate benchmarking).
- Type and source of inputs used by each model and underlying components of each model (which may include other models).
- Description of the type of technology or approach used.
- Model outputs and their intended use.
- Identification of individuals responsible for various aspects of the model development and validation.
- Type (e.g., credit, compliance) and level of risk.
- Dates of completed and planned validation activities, ongoing monitoring frequency, and description of validation results/status (e.g., fit for purpose, approval), and changes made to the models that management deems to be material. For example, if a bank makes any material change to a model, the model should be validated. That information should be captured in the "planned validation activities" in the inventory.
- Description of any model issues or limitations.
- Summary of model issue status (e.g., work in progress, partially completed).
- Description of any model overlays.
- Indication of whether models are functioning properly.
- Description of when the model was last updated.
- A list of any exceptions to policy.[34]
- Time frame that the model is expected to remain valid.

Some quantitative tools may not meet the definition of a model in the MRM Supervisory Guidance. Sound risk management typically includes maintaining an inventory of all quantitative tools.

[34] Exceptions to policy are generally temporary. In some cases, senior management or the board grant provisional approval to implement or continue using a model pending resolution of exceptions or other issues.

Documentation

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

Documentation benefits model developers, users, and risk management personnel. The mathematical calculations and quantification underlying any model generally involve application of theory, choice of sample design (e.g., cross-section versus time-series cross-section), numerical routines, selection of inputs and exclusions, estimation, and implementation in different information systems. It is important that these choices be transparent and explainable in documentation, with particular attention to model capabilities, merits, and limitations. Documentation should be updated with changes in the model components, operating environment, and how the model is used.

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

Sound documentation of model selection, development, and validation typically includes information supporting decisions related to model selection, testing, governance, development, internal controls, and third-party risk management, for example,

- model assumptions and limitations in consideration of the model's use.
- theoretical approach and supporting research, as appropriate.
- model design and formulas.
- data coverage, sources, quality, and limitations.
- description and interpretation of testing diagnostics, model outcomes, and expected performance under a variety of economic conditions and business environments.

- an explanation of the degree to which underlying input-output relationships predict model outcomes.
- change logs.
- ongoing monitoring plans.
- description, frequency, and standards of monitoring for each model, including performance measures used in ongoing monitoring, **performance thresholds**,[35] and supporting rationale.
- business uses.

Understanding and documenting how each model interacts with other models is important to understand the scope of the individual risks associated with a bank's models, and aggregate risks arising from interactions or interdependencies among models, data, and processes across the bank. Understanding model end-to-end processes may also reveal areas of control or risk management weaknesses.

Supervisory Guidance on Model Risk Management

For cases in which a bank uses models from a vendor or other third party, it should ensure that appropriate documentation of the third-party approach is available so that the model can be appropriately validated.

When a bank uses third-party models, the extent of documentation that the bank has is typically not as extensive as for models developed in-house. Examiners should determine if documentation is sufficient for bank management to appropriately use and validate third-party models. Refer to the "Third-Party Risk Management" section of this booklet for a detailed discussion of third-party models and associated risk management.

Data Management

Supervisory Guidance on Model Risk Management

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

[35] Performance threshold refers to a value or range of values of a performance measure that determines the acceptance or rejection of a model's performance.

To measure risk effectively, the data inputs for models should be reliable. Banks ordinarily document the major data sources used in the risk measurement process. Sound risk management involves providing reasonable and reconcilable support for qualitative factors used to account for environmental differences between quantitative estimates and current market and economic conditions. Analysis of the integrity and applicability of internal and external information sources and related controls, and API and other software allowing connectivity to models and data, should be regularly performed to determine if revisions or updates are necessary.

Model Development, Implementation, and Use

Supervisory Guidance on Model Risk Management

Model risk management begins with robust model development, implementation, and use.

Model risk management should include disciplined and knowledgeable development and implementation processes that are consistent with the situation and goals of the model user and with bank policy. Model development is not a straightforward or routine technical process. The experience and judgment of developers, as much as their technical knowledge, greatly influence the appropriate selection of inputs and processing components. The training and experience of developers exercising such judgment affects the extent of model risk. Moreover, the modeling exercise is often a multidisciplinary activity drawing on economics, finance, statistics, mathematics, and other fields. Models are employed in real-world markets and events and therefore should be tailored for specific applications and informed by business uses. In addition, a considerable amount of subjective judgment is exercised at various stages of model development, implementation, use, and validation. It is important for decision makers to recognize that this subjectivity elevates the importance of sound and comprehensive model risk management processes. (See note 2)

Note 2: Smaller banks that rely on vendor models may be able to satisfy the standards in this guidance without an in-house staff of technical, quantitative model developers. However, even if a bank relies on vendors for basic model development, the bank should still choose the particular models and variables that are appropriate to its size, scale, and lines of business and ensure the models are appropriate for the intended use.

Defined roles and responsibilities for clear communication of model limitations and assumptions are key for sound model risk management. The model development process should also provide for effective challenge from qualified personnel. For example, in large or complex banks, IRM typically provides effective challenge related to model limitations and assumptions.

Personnel involved in model development should have adequate technical knowledge, training, and experience, and demonstrate sound judgment. These factors influence the appropriate selection of model inputs and processing components. When relying on third-party models, bank personnel should confirm models are appropriate for intended use and choose models and model variables that are tailored to the bank's size, complexity, and risks.[36]

[36] For more information, refer to the "Third-Party Risk Management" section of this booklet.

Model Development and Implementation

Supervisory Guidance on Model Risk Management

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

A sound development process will produce documented evidence in support of all model choices, including the overall theoretical construction, key assumptions, data, and specific mathematical calculations, as mentioned in Section IV [of the "Supervisory Guidance on Model Risk Management"].

While they may not be classified as a model, algorithms, mathematical formulas, computer code, software, and IT systems implementing the model should be subject to rigorous quality control and change control processes to confirm that the code is correct, that it cannot be altered except by approved parties, and that all changes are logged and can be audited.[37]

Supervisory Guidance on Model Risk Management

As a first step, banks should ensure that there are appropriate processes in place for selecting vendor models. Banks should require the vendor to provide developmental evidence explaining the product components, design, and intended use, to determine whether the model is appropriate for the bank's products, exposures, and risks. Vendors should provide appropriate testing results that show their product works as expected. They should also clearly indicate the model's limitations and assumptions and where the product's use may be problematic.

Banks often purchase generic third-party models (e.g., models developed on data pooled from many lenders from the credit bureaus, such as credit scores). In these cases, while bank personnel are not involved in the variable selection process, sound risk management involves understanding how a model works before making a purchase decision. Refer to the "Third-Party Risk Management" section of this booklet for a more comprehensive discussion.

[37] Refer to the "Development and Acquisition" booklet of the *Federal Financial Institutions Examination Council Information Technology Handbook.*

Testing

Supervisory Guidance on Model Risk Management

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

The nature of testing and analysis will depend on the type of model and will be judged by different criteria depending on the context. For example, the appropriate statistical tests depend on specific distributional assumptions and the purpose of the model. Furthermore, in many cases, statistical tests cannot unambiguously reject false hypotheses or accept true ones based on sample information. Different tests have different strengths and weaknesses under different conditions. Any single test is rarely sufficient, so banks should apply a variety of tests to develop a sound model.

Banks should ensure that the development of the more judgmental and qualitative aspects of their models is also sound. In some cases, banks may take statistical output from a model and modify it with judgmental or qualitative adjustments as part of model development. While such practices may be appropriate, banks should ensure that any such adjustments made as part of the development process are conducted in an appropriate and systematic manner, and are well documented.

Examples of judgmental or qualitative aspects of models that may be tested during model development include inputs or adjustments to outputs. For example, in some cases, banks take statistical output from a model and modify it with judgmental or qualitative adjustments. Sound testing processes help management confirm that judgmental or qualitative aspects of models are appropriate. Using similar data in the model implementation process and the development process helps to determine if the model is accurately producing the outcomes in the production environment as expected. Appropriate documentation generally includes the description of the nature and magnitude of adjustments made as well as the rationale and methodology.

Examiners should determine whether bank personnel have developed and implemented appropriate policies, standards, processes, and controls for testing the bank's models.

A model should be validated before it is put into use. Validation activities before implementation should be comprehensive, and the rigor of validation should be

commensurate with the potential risk presented by use of the model. For more information, refer to the "Model Validation" section of this booklet.

Ongoing Development

Supervisory Guidance on Model Risk Management

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

Examiners should determine whether banks have appropriate processes to validate adjusted or redeveloped models before implementation.

Model Use

Supervisory Guidance on Model Risk Management

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

However, challenge from model users may be weak if the model does not materially affect their results, if the resulting changes in models are perceived to have adverse effects on the business line, or if change in general is regarded as expensive or difficult. User challenges also tend not to be comprehensive because they focus on aspects of models that have the most direct impact on the user's measured business performance or compensation, and thus may ignore other elements and applications of the models.

Finally, such challenges tend to be asymmetric, because users are less likely to challenge an outcome that results in an advantage for them. Indeed, users may incorrectly believe that model risk is low simply because outcomes from model-based decisions appear favorable to the institution. Thus, the nature and motivation behind model users' input should be evaluated carefully, and banks should also solicit constructive suggestions and criticism from sources independent of the line of business using the model.

Model users can provide insight as to whether models are functioning as intended and assess model performance as models are in use. The strength of user challenge may vary based on how model results affect model users' business lines. Examiners should determine if banks have adequate processes to address feedback from users. Examiners should determine if the bank's process for assessing model use over time is effective.

Model Overlays and Adjustments

Many banks use model overlays, which are judgmental or qualitative adjustments to model inputs or outputs to compensate for model, data, or other known limitations. A bank sometimes overrides a model's output by applying a model overlay or directly adjusting the model inputs or assumptions (e.g., model coefficients, input variables). Sound model risk management includes policies and processes regarding the review, approval, use, and back-testing of model overlays and adjustments. Fair lending and consumer protection-related laws and regulations are important considerations when applying overlays and adjustments. Model validators should have appropriate technical and substantive knowledge of the model being validated, including knowledge of the type of model, to understand and review performance, overlays, and adjustments. Examiners should assess bank management's support for model overlays and in-model adjustments. Model overlays and adjustments should not be viewed as a solution that dissuades the bank from making improvements to the model. Banks typically have a process to monitor and analyze overlays and adjustments over time and address underlying limitations and issues through data enhancements, model recalibration, or redevelopment.

The development and use of model overlays, applied both within the model and at model output, should be a well-documented, transparent process with appropriate justification related to specific model issues and limitations. As part of the process, model adjustments should be clearly outlined and consistent with assumed scenario conditions, and model results should be provided with and without adjustments.

Supervisory Guidance on Model Risk Management

An understanding of model uncertainty and inaccuracy and a demonstration that the bank is accounting for them appropriately are important outcomes of effective model development, implementation, and use. Because they are by definition imperfect representations of reality, all models have some degree of uncertainty and inaccuracy. These can sometimes be quantified, for example, by an assessment of the potential impact of factors that are unobservable or not fully incorporated in the model, or by the confidence interval around a statistical model's point estimate. Indeed, using a range of outputs, rather than a simple point estimate, can be a useful way to signal model uncertainty and avoid spurious precision. At other times, only a qualitative assessment of model uncertainty and inaccuracy is possible. In either case, it can be prudent for banks to account for model uncertainty by explicitly adjusting model inputs or calculations to produce more severe or adverse model output in the interest of conservatism. Accounting for model uncertainty can also include judgmental conservative adjustments to model output, placing less emphasis on that model's output, or ensuring that the model is only used when supplemented by other models or approaches. (See note 3.)

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

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

Note 3: To the extent that models are used to generate amounts included in public financial statements, any adjustments for model uncertainty must comply with generally accepted accounting principles.

Reporting

Supervisory Guidance on Model Risk Management

Reports used for business decision making play a critical role in model risk management. Such reports should be clear and comprehensible and take into account the fact that decision makers and modelers often come from quite different backgrounds and may interpret the contents in different ways.

Effective reporting enables senior management and the board to understand the bank's model risk. Reports should be accurate, timely, relevant, complete, and sufficiently detailed for management and the board, in the respective roles, to oversee the bank's safe and sound operation. Information needed for effective reporting, particularly the number and variety of reports, depends on the bank's size, complexity, and risks. The information should be sufficient to keep relevant parties informed of model performance. For example, effective reports clearly explain model assumptions and limitations. The information should evolve as the bank grows in size and complexity, and as the bank's risk profile changes.

Supervisory Guidance on Model Risk Management

Reports that provide a range of estimates for different input-value scenarios and assumption values can give decision makers important indications of the model's accuracy, robustness, and stability as well as information on model limitations.

Reports presented to the board typically highlight performance measures, trends, and variances, rather than presenting the information as raw data. Reports often contain risk appetite metrics or data on other key risk indicators for model risk. Comparing performance with business unit or bank-wide risk limits helps decision makers to assess whether the bank is operating within the board's risk appetite. Model risk management reports may include measures on

- the volume of models considered high risk.
- models with temporary exemptions or provisional approvals.
- status of model issues (e.g., work in progress, partially completed).
- underperforming models.
- models with past-due validations.
- models in use without validation.
- model development efforts in progress.

Model Validation

Supervisory Guidance on Model Risk Management

Another essential element [of model risk management] is a sound model validation process.

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

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

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

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

Validation activities should continue on an ongoing basis after a model goes into use, to track known model limitations and to identify any new ones. Validation is an important check on model use during periods of benign economic and financial conditions, when estimates of risk and potential loss can become overly optimistic, and when the data at hand may not fully reflect more stressed conditions. Ongoing validation activities help to ensure that changes in markets, products, exposures, activities, clients, or business practices do not create new model limitations. For example, if credit risk models do not incorporate underwriting changes in a timely manner, flawed and costly business decisions could be made before deterioration in model performance becomes apparent.

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

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

An effective validation framework should include three core elements:

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

A model should be validated before it is put into use. The rigor of validation before implementation should be commensurate with the potential risk presented by use of the model. If the bank has not fully validated models before implementation, examiners should assess the bank's compensating controls and other measures to mitigate risks. Model reviews and validations (in whole or in part) are generally performed using a risk-based approach, and with a frequency appropriate for, or when, there are changes to a bank's risk profile.

Material changes to models may warrant validation. Appropriate validation reports generally include the review of conceptual soundness of a model for its intended purpose and the results of ongoing monitoring, process verification, benchmarking, and outcomes analysis.

A sound validation process generally includes

- defined purpose and goals.
- scope, validation approach, schedule, resources, and types and extent of validation activities and tasks.
- specific actions that must be taken to complete individual validation activities and tasks.
- detailed and sufficient documentation to demonstrate that all validation procedures are appropriately completed.

While control staff may grant exceptions to typical procedures of model validation on a temporary basis, that authority should be subject to other control mechanisms, such as timelines for completing validation work and limits on model use.

Supervisory Guidance on Model Risk Management

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

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

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

Staff conducting validation work should have explicit authority to challenge developers and users and to elevate their findings, including issues and deficiencies. The individual or unit to whom those staff report should have sufficient influence or stature within the bank to ensure that any

issues and deficiencies are appropriately addressed in a timely and substantive manner. Such influence can be reflected in reporting lines, title, rank, or designated responsibilities. Influence may be demonstrated by a pattern of actual instances in which models, or the use of models, have been appropriately changed as a result of validation.

Independent validation may be performed in-house, by a third party, or a combination thereof.[38] In large or complex banks, model validation is typically conducted by IRM (e.g., model risk management function in a second line of defense) or by an independent third party. Sometimes, particularly for small or noncomplex banks, some validation work may be most effectively done by model developers or users. In such cases, an independent party with appropriate technical knowledge typically provides critical review and effective challenge, and conducts additional activities to confirm proper validation.

Supervisory Guidance on Model Risk Management

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

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

Examiners should determine if bank management has appropriate processes in place to validate models. In assessing the effectiveness of model validation processes, examiners generally evaluate the extent and clarity of documentation, issues identified by the validation, and the actions bank management takes to address such issues.

Evaluation of Conceptual Soundness

Supervisory Guidance on Model Risk Management

This element [of validation] involves assessing the quality of the model design and construction. It entails review of documentation and empirical evidence supporting the methods used and variables selected for the model. Documentation and testing should convey an understanding of model limitations and assumptions. Validation should ensure that judgment exercised in model design and construction is well informed, carefully considered, and consistent with published research and

[38] For more information, refer to the "Third-Party Risk Management" section of this booklet.

with sound industry practice. Developmental evidence should be reviewed before a model goes into use and also as part of the ongoing validation process, in particular whenever there is a material change in the model.

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

Evaluation of conceptual soundness generally includes such activities as the following, as appropriate:

- Evaluating the quality and extent of developmental evidence and conducting additional testing as necessary.
- Assessing whether the model achieves the intended purpose.
- Comparing alternative model theories and approaches.
- Justifying the choice of a particular model theory and approach.
- Assessing key assumptions and variables, with analysis of their impact on model outputs and particular focus on any potential limitations, including model transparency and explainability for AI approaches.
- Evaluating the relevance of the data used to build the model to validate that data are reasonably representative of the model's inputs, such as the bank's portfolio, account activity, or market conditions, depending on the type of model. This is particularly important when a bank uses external data or the model is used for new activities.
- Sensitivity analysis and stress testing.

An evaluation of conceptual soundness may be difficult for some complex models (e.g., those that use AI approaches) because the underlying theory and logic may not be transparent. Transparency and explainability are key considerations that are typically evaluated as part of effective risk management regarding the use of complex models. The appropriate level of explainability of a model outcome depends on the specific use and level of risk associated with that use. Models applied to significant operations or decisions (e.g., credit underwriting decisions) should be supported by thorough understanding of how the model arrived at its conclusions and validation that it is operating as intended. There may be challenges with explaining some models based on complexity or, in some cases, limited documentation provided for third-party models. Examiners should discuss with bank management the bank's process for exploring various approaches to determine whether bank personnel have an understanding of how models function and make decisions, including identifying any limitations and use of compensating controls.

Supervisory Guidance on Model Risk Management

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

By changing the input data, the user can test the results of these changes on the output results to assess a model's limitations.

Supervisory Guidance on Model Risk Management

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

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

Examiners should assess if the validation process includes an evaluation of conceptual soundness and determine if the validation process

- provides appropriate critical review of model selection and development.
- determines the model reflects sound theory and business practice.
- verifies model stability and accuracy.
- verifies the effectiveness of model performance with respect to the range of model inputs and assumptions.
- assesses whether biases are present in data and model outcomes.

Ongoing Monitoring

Supervisory Guidance on Model Risk Management

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

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

Monitoring reports should be timely and accurate, and should be distributed to appropriate individuals, including the board, when needed. Ongoing monitoring generally includes

- assessment of adherence to the established risk appetite.
- assessment of adherence to internal limits on model use and targets for model accuracy or reliability.
- mechanisms for the board to hold management accountable for operating within limits on model use and targets for model accuracy or reliability.
- analysis of overrides, including evaluating the reasons for, and reasonableness of, overrides, and tracking and analyzing override performance.
- assessment of model limitations identified in the development stage.
- sensitivity analysis and other checks for robustness and stability.[39]
- review of risk measurements and performance thresholds.
- early-warning analysis with interpretation of testing metrics and performance diagnostics to support conclusions.
- escalation processes and risk mitigation actions when a significant breach of a performance threshold occurs.
- timely system updates.
- timely updates to reflect changes in laws and regulations (e.g., through the bank's compliance management systems (CMS)).
- analysis of the integrity and applicability of internal and external information sources, including information provided by third parties.
- process verification and benchmarking.
- procedures for responding to, and escalating, identified issues.

[39] For more information, refer to the "Evaluation of Conceptual Soundness" section of this booklet.

Supervisory Guidance on Model Risk Management

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

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

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

Examiners should determine if the validation process includes ongoing monitoring, including an analysis of overrides. Examiners should determine if ongoing monitoring identifies specific areas within the model that warrant sensitivity analysis or stress testing (e.g., in accordance with bank policy), and determine how the results are communicated and contribute to the overall assessment of the model for validation purposes. Examiners should determine if bank management has designed a program of ongoing monitoring and evaluation of model performance, including process verification and benchmarking, and procedures for responding to any problems that appear.[40] When reviewing ongoing monitoring, examiners should assess if the frequency and depth of monitoring is commensurate with the risks involved.

Process Verification

Supervisory Guidance on Model Risk Management

Process verification checks that all model components are functioning as designed. It includes verifying that internal and external data inputs continue to be accurate, complete, consistent with model purpose and design, and of the highest quality available. Computer code implementing the model should be subject to rigorous quality and change control procedures to ensure that the code is correct, that it cannot be altered except by approved parties, and that all changes are logged and can be audited. System integration can be a challenge and deserves special attention because the model processing component often draws from various sources of data, processes large amounts of

[40] For more information, refer to the "Process Verification" and "Benchmarking" sections of this booklet.

data, and then feeds into multiple data repositories and reporting systems. User-developed applications, such as spreadsheets or ad hoc database applications used to generate quantitative estimates, are particularly prone to model risk. As the content or composition of information changes over time, systems may need to be updated to reflect any changes in the data or its use. Reports derived from model outputs should be reviewed as part of validation to verify that they are accurate, complete, and informative, and that they contain appropriate indicators of model performance and limitations.

Examiners should determine if bank management has conducted process verification. Process verification typically includes

- verifying that internal and external data inputs remain accurate, complete, consistent with model purpose and design, and of sufficient quality.
- verifying inputs are processed as expected and used in models in a timely manner.
- reviewing reports derived from model outputs as part of validation to verify that they are accurate, complete, and informative, and that they contain appropriate indicators of model performance and limitations.

Benchmarking

Supervisory Guidance on Model Risk Management

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

A benchmark may be estimates from alternative internal or external data or models. A benchmark model, sometimes referred to as an alternative model or challenger model, is typically constructed during model development and compared against the model intended to be used in production. The performance differences between the benchmark model and the model intended to be used in production are then analyzed and documented. Validators may also develop a benchmark model to track model performance over time. During ongoing monitoring, the performance of both models is typically monitored and compared to identify the underlying weaknesses of the model used in production. If there are unexplained differences between the two and the model used in production is deemed underperforming, then the benchmark model can be a useful guide for model overlays and adjustments, or it can be used temporarily until the issues of the model used in production are resolved.

Supervisory Guidance on Model Risk Management

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

Examiners should determine if bank management has included benchmarking as a component of model development and validation activities.

Outcomes Analysis

Supervisory Guidance on Model Risk Management

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

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

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

Outcomes analysis helps to evaluate model performance by establishing expected ranges for actual outcomes in relation to the intended objectives, and assessing the reasons for, and reasonableness of, observed variation between the two. When a model relies on expert judgment, quantitative outcomes analysis helps to evaluate the quality of that judgment. Outcomes analysis approaches used may vary depending on the characteristics and objectives of a model. When assessing the process for evaluating model outcomes, examiners should determine which techniques are used to evaluate outcomes and if those techniques are appropriate.

Outcomes analysis approaches may be adapted based on model type to support the specific objectives and methodologies used. For instance, back-testing may not be the best form of outcomes analysis for BSA/AML models,[41] which are designed to assist in identifying suspicious activity; or for fair lending models, which are designed to identify lending disparities that may indicate fair lending risk. Back-testing may not be possible for many BSA/AML models because there is no definitive way to measure the total amount of suspicious activity that actually occurred during a given time period to compare with activity detected by the system.

A common alternative to traditional back-testing for BSA/AML models is evaluating "above-the-line" and "below-the-line" performance of the model in a certain time period. Evaluating above-the-line performance entails reviewing the activity alerted by the model as potentially suspicious. Alert productivity metrics are a common way to evaluate above-the-line performance. Examples of alert productivity metrics include (1) false positive rate, (2) the proportion of alerts generated by the model that are escalated to the next level of manual review, and (3) the proportion of alerts that result in a Suspicious Activity Report.[42] Evaluating below-the-line performance entails reviewing activity that does not result in an alert by the model, and typically involves drawing a sample of this activity to determine if the rate of false negatives[43] is within the bank's risk tolerance.

For fair lending models, an alternative to traditional back-testing could include manual file review to assess the results from the statistical model. Specifically, the file review may help highlight whether there are data errors. The file review may also identify factors that were not incorporated into the statistical model and assess whether those additional factors may explain the remaining differences between the prohibited basis group members and control group members. If possible, data on the factors that were not incorporated into the statistical model could be collected and used to update the statistical models.

[41] For more information, refer to the "Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance" conveyed by OCC Bulletin 2021-19.

[42] False positives are transactions that are incorrectly reported by the model as potentially suspicious but found to not represent suspicious activities requiring a Suspicious Activity Report.

[43] False negatives are transactions that represent potentially suspicious activities but are incorrectly not reported by the model.

Back-Testing

Supervisory Guidance on Model Risk Management

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

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

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

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

A comparison of early model performance over a period against the model performance observed over the same time horizon on an earlier sample of data (e.g., the development sample) is generally a component of a well-developed early warning analysis.

Examiners should evaluate how bank management incorporates back-testing results into the modeling process. Examiners should assess the appropriateness of how back-testing results are communicated and whether models are considered for recalibration or redevelopment based on back-testing results.

Third-Party Risk Management

Banks may benefit from third-party relationships by gaining operational efficiencies or improving the banks' competitive edge. A bank's use of third parties does not diminish the responsibility of the bank's board and senior management to ensure that the bank operates in a safe and sound manner and in compliance with applicable laws and regulations. The OCC expects banks to have more comprehensive and rigorous management of third-party relationships that involve critical activities.[44]

Some banks use third-party models, engage third parties for model development, use third-party data, or engage third parties to perform services related to model risk management. Third-party models can include models developed on data pooled from many lenders or data from the credit bureaus, such as credit score models.[45] OCC Bulletin 2013-29 is relevant when a bank uses a third-party model or uses a third party to assist with model risk management, as is OCC Bulletin 2011-12. Accordingly, third-party models should be incorporated into the bank's third-party risk management and model risk management processes. Management should conduct appropriate due diligence on the third-party relationship and on the model itself.[46]

Third-Party Models and Data

Supervisory Guidance on Model Risk Management

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

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

[44] Refer to OCC Bulletins 2013-29 and 2020-10.

[45] For guidance specific to credit scoring models, refer to OCC Bulletin 1997-24, "Credit Scoring Models: Examination Guidance."

[46] Refer to OCC Bulletins 2013-29 and 2020-10.

When a bank uses a third-party model, the bank typically obtains information from the third party to support the bank's model risk management. Such information typically includes

- developmental evidence explaining the model's components, design, and intended use, to determine whether the model is appropriate for the bank's products and risk exposures.
- information regarding the data used to develop the model, including use and effect of alternative data.
- sufficiently detailed testing results that show the third party's product works as expected.
- documentation on the model's limitations and assumptions and about when the model's use may be problematic.
- clear instructions for model implementation, including any decisions that should be made regarding parameters or thresholds.

Supervisory Guidance on Model Risk Management

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

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

Bank management should understand and evaluate the results of validation and risk control activities that are conducted by third parties.[47] Bank management's understanding of how the third-party model operates is an important foundation to effectively negotiate contracts that protect the bank's needs and rights, including privacy and customer information protection. Bank management should conduct a risk-based review of each third-party model to determine whether it is working as intended and if the existing validation activities are sufficient. Banks should expect the third party to conduct ongoing performance monitoring and outcomes analysis of the model, disclose results to the bank, and make appropriate modifications and updates to the model over time, if applicable.[48] Banks typically obtain

[47] Ibid.

[48] Ibid.

information from the third party to confirm that the model's performance meets the bank's needs (e.g., consumer protection needs).

Engaging Third Parties for Model Risk Management Activities

Supervisory Guidance on Model Risk Management

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

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

If the bank lacks sufficient expertise in-house, a bank may decide to engage external resources (i.e., a third party) to help execute certain activities related to model risk management and the bank's ongoing third-party monitoring responsibilities. These activities could include model validation and review, compliance functions, or other activities in support of internal audit. Bank management should understand and evaluate the results of validation and risk control activities that are conducted by third parties. Bank management typically designates an internal party to[49]

- determine whether the third-party performed work meets the standards and controls set forth in the bank's model risk governance framework.
- verify that the scope of work as defined with a contract or agreement has been completed by the third party.
- evaluate and track identified issues and ensure they are addressed in a timely manner.
- make sure completed work is incorporated into the bank's model risk management and third-party risk management processes.

Many third parties provide banks with reports of independent certifications or validations of the third-party model. Validation reports provided by a third-party model provider should

[49] Ibid.

identify model aspects that were reviewed, highlighting potential deficiencies over a range of financial and economic conditions (as applicable), and determining whether adjustments or other compensating controls are warranted. Effective validation reports include clear executive summaries, with a statement of model purpose and a synopsis of model validation results, including major limitations and key assumptions. Validation reports should not be taken at face value. Bank management should understand any of the limitations experienced by the validator in assessing the processes and codes used in the models.[50]

IT Systems

Banks should have appropriate risk management to maintain adequate IT systems that result in appropriate and accurate model outputs. Banks should maintain data used to support models and data generated from models in accordance with internal or regulatory record retention requirements.[51]

Supervisory Guidance on Model Risk Management

Models typically are embedded in larger information systems that manage the flow of data from various sources into the model and handle the aggregation and reporting of model outcomes. Model calculations should be properly coordinated with the capabilities and requirements of information systems. Sound model risk management depends on substantial investment in supporting systems to ensure data and reporting integrity, together with controls and testing to ensure proper implementation of models, effective systems integration, and appropriate use.

Systems, applications, and technologies used by the bank's models should be appropriately managed. It is critical that the IT environment supporting the bank's models has appropriate controls before model implementation. Security weaknesses, including poorly constructed APIs and third-party applications, and weaknesses in the controls for the access, authentication, transmission, and storage of sensitive customer information, including privileged access, expose a bank to increased operational risk. The capabilities and requirements of the bank's IT systems, and controls to protect sensitive customer information should be assessed before developing or implementing a model.

The model processing component often draws from various data sources, processes large amounts of data, and then feeds into multiple data repositories and reporting systems. This underscores the importance of appropriate controls to protect sensitive customer information, and appropriate security controls related to how the bank and any third parties access, transfer, share, and store information and maintain availability, including data backup and replication, of information.[52]

[50] Ibid.

[51] For example, BSA record retention requirements are outlined in 31 CFR Chapter X, "Financial Crimes Enforcement Network, Department of the Treasury."

[52] For more information, refer to the "Business Continuity Management" and "Information Security" booklets of the *Federal Financial Institutions Examination Council IT Examination Handbook*.

Supervisory Guidance on Model Risk Management

As the content or composition of information changes over time, systems may need to be updated to reflect any changes in the data or its use.

Examination Procedures

This booklet contains expanded procedures for examining specialized activities or specific products or services that warrant extra attention beyond the core assessment contained in the "Community Bank Supervision," "Federal Branches and Agencies Supervision," and "Large Bank Supervision" booklets of the *Comptroller's Handbook*. Examiners determine which expanded procedures to use, if any, during examination planning or after drawing preliminary conclusions during the core assessment.

Scope

These procedures are designed to help examiners tailor the examination to each bank and determine the scope of the model risk management examination. This determination should consider work performed by internal and external auditors and other independent risk control functions and by other examiners on related areas. Examiners need to perform only those objectives and steps that are relevant to the scope of the examination as determined by the following objectives. Seldom will every objective or step of the expanded procedures be necessary.

Model risk management examinations may warrant coordination with the OCC's Risk Analysis Division (RAD) within the Economics Department for examination assistance or advisement. The decision to coordinate with RAD and the type of work RAD will perform are determined on a case-by-case basis through discussion with the supervisory office[53] and the Economics Department.

Objective: To determine the scope of the model risk management examination and identify examination objectives and activities necessary to meet the needs of the supervisory strategy for the bank.

1. Review the following sources of information to identify issues related to model risk management that require follow-up:

   - Supervisory strategy.
   - Examination scope memorandum.
   - Previous supervisory activity work papers.
   - Internal and external audit reports and management's responses.
   - Reports detailing the status of open audit, regulatory, and self-identified (e.g., by model owners or IRM) issues related to model risk management.

2. Obtain and review policies, procedures, board and committee meeting minutes, and reports bank management uses to supervise the use of models.

[53] For community and midsize banks, the OCC supervisory office means the assistant deputy comptroller. For large banks, including large federal branches with a related large bank affiliate, the supervisory office includes the EIC or deputy comptroller, depending on the circumstances.

3. In discussions with bank management, determine if there have been any significant changes since the prior examination of model risk management and the reason for significant changes. Consider changes in

   - policies, procedures, or processes.
   - personnel.
   - control systems.
   - use of data.
   - models.
   - model performance.
   - information systems.
   - third-party relationships.
   - products or services.
   - delivery channels or volumes.
   - markets.
   - economic environment.
   - geographies.

4. Based on an analysis of information obtained in the previous steps, as well as input from the EIC, determine the scope and objectives of the model risk management examination. Through discussion with the supervisory office and Economics Department, determine if coordination with RAD is warranted.

5. Select from the following examination procedures the necessary steps to meet examination objectives and the supervisory strategy.

Quantity of Risk

Conclusion: The quantity of each associated risk is (low, moderate, or high).

Objective: To determine the quantity of each risk associated with the bank's model use. Model use can affect risk in all eight categories of risk. The use of models can increase or decrease risk in each risk category depending on the models' purpose, use, and the effectiveness of model risk management. Conceptually, model risk is a distinct risk that can influence aggregate risk across all risk categories. Model risk can increase from interactions and dependencies among models, such as reliance on common assumptions, inputs, data, or methodologies.

1. Analyze the quantity of strategic risk associated with the bank's model use. Consider

   - the nature, extent, and complexity of models the bank uses.
   - the extent to which models contribute to strategic decision making.
   - whether any strategic objectives (e.g., new activities) depend on the use of models.
   - whether the bank has an established governance framework for developing, implementing, using, and validating models.
   - whether models evolve to keep pace with changes in strategy, capabilities of employees, the operating environment, and regulatory requirements.
   - whether model inputs and assumptions are adjusted for current and anticipated
     − market conditions.
     − macroeconomic environment.
     − consumer behaviors.
     − characteristics and usage of the bank's financial product .
   - whether model outputs are accurate and if any adjustments are applied to model outputs.
   - the materiality of portfolios and decisions for which models are used.
   - whether data used for current or planned models are sufficient and relevant.

2. Analyze the quantity of operational risk associated with the bank's model use. Consider

   - the nature, extent, and complexity of models the bank uses.
   - the nature and extent of the bank's reliance on third parties for models, model development, data, or services related to model risk management.
   - the volume of operational losses resulting from modeling weaknesses, such as weaknesses in data, assumptions, estimations, or testing.
   - the level of uncertainty or inaccuracy of model inputs and assumptions.
   - the frequency of ongoing monitoring of the bank's models.
   - the extent to which models contribute to decision making.
   - extent of turnover of personnel responsible for executing or overseeing the bank's model risk management policies, standards, and processes.
   - the nature and extent of operational breakdowns related to model use.

3. Analyze the quantity of compliance risk associated with the bank's model use. Consider

    - the nature, extent, and complexity of models used in the bank's CMS. Consider models used
        - in the bank's BSA/AML and OFAC compliance programs.
        - for fair lending or Community Reinvestment Act analysis or monitoring.
        - for consumer or small business loan underwriting, account management, pricing, or loss mitigation.
        - for marketing loan and deposit products.
        - for other aspects of the bank's CMS.
    - any consumer protection-related issues, including fair lending issues, raised as a result of the bank's models, including disparate impact or disparate treatment of loan applicants or customers on a prohibited basis.
    - the level of uncertainty or inaccuracy of model inputs and assumptions.
    - the frequency of the ongoing monitoring of the bank's models.
    - the extent to which models contribute to compliance-related decision making.
    - the extent to which models contribute to regulatory reporting.

4. Analyze the quantity of credit risk associated with the bank's model use. Consider

    - the nature, extent, and complexity of models used for lending, credit administration, risk management, or estimating credit losses or regulatory capital.
    - the level of uncertainty or inaccuracy of the model inputs and assumptions.
    - the accuracy and reasonableness of model assumptions and the relevance of data used to develop the model.
    - the level of uncertainty of model outputs and the significance of overlays and adjustments applied to model outcomes.
    - the extent to which models contribute to credit-related decision making.

5. Analyze the quantity of liquidity risk associated with the bank's model use. Consider

    - the nature, extent, and complexity of models used for liquidity risk management.
    - the level of uncertainty or inaccuracy of model inputs and assumptions, including behavioral and contingent funding assumptions.
    - the reasonableness of the magnitude of liquidity stress scenarios and their impact to the models' outputs.
    - whether stress scenarios consider all relevant legal or regulatory constraints.
    - the extent to which models contribute to liquidity risk-related decision making.

6. Analyze the quantity of interest rate risk associated with the bank's model use. Consider

    - the nature, extent, complexity, and technologies of models the bank uses for interest rate risk management.

- the level of uncertainty or inaccuracy of interest rate measurement model inputs and assumptions (e.g., the volume of instruments with embedded options or complex structures).
- the reasonableness of the magnitude of stress scenarios and their impact on the models' outputs.
- the extent to which models contribute to interest rate risk-related decision making.

7. Analyze the quantity of price risk associated with the bank's model use. Consider

   - the nature, extent, and complexity of models the bank uses.
   - the accuracy of the model's estimate of financial instruments' prices, including
     – whether there are enough data on prices for the same or similar instruments.
     – the material factors that affect the instruments' prices.
   - the volume of trading instruments with prices that are hard to model.
   - the level of uncertainty or inaccuracy of model inputs and assumptions.
   - the extent to which models contribute to price risk-related decision making.

~~8. Analyze the quantity of reputation risk associated with the bank's model use. Consider~~

   - ~~the nature, extent, and complexity of models the bank uses.~~
   - ~~the level of uncertainty or inaccuracy of model inputs and assumptions.~~
   - ~~the extent to which models contribute to reputation risk-related decision making.~~
   - ~~the extent of compliance issues (e.g., noncompliance with consumer protection-related laws and regulations or BSA/OFAC requirements) related to model use.~~
   - ~~the adequacy of policies and processes; weaknesses in any aspect of model risk management, governance, or third-party risk management; and wrongful acts by third parties.~~
   - ~~the adequacy of internal controls over data, including internal controls in place to prevent biased outcomes.~~
   - ~~whether models consider all relevant legal or regulatory requirements and constraints.~~

9. Consider the information in procedures 1 through 8 and analyze the overall quantity of risk associated with the bank's model use.

Quality of Model Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, insufficient, or weak).

The conclusion on risk management considers all risks associated with a bank's model use.

Policies

Policies are statements of actions adopted by a bank to pursue certain objectives. Policies guide decisions, often set standards (on risk limits, for example), and should be consistent with the bank's underlying mission, risk appetite, and core values. Policies should be reviewed periodically for effectiveness and approved by the board of directors or designated board committee.

Objective: To determine whether the board has adopted policies for model risk management that are consistent with sound risk management practices and are commensurate with the bank's size, complexity, business activities, model usage, corporate culture, and organizational structure. Policies may vary based on the type and objectives of the bank's models.

1. Evaluate model risk management policies to determine whether they provide appropriate guidance for governance over the model risk management framework. Consider whether the bank's policies

   - describe governance and controls over model risk management.
   - establish model risk management internal controls.
   - describe the model risk management framework and how the framework is applied to different types of models.
   - require maintenance of detailed documentation of all aspects of the model risk management framework.
   - include definitions of a model and model risk and criteria for when model risk management policies should be applied.
   - describe the process and standards for assessing model risk.
   - define acceptable practices for model development, including redevelopment; implementation; use; and validation for all models, including third-party models.
   - identify roles and responsibilities with clear detail on staff expertise, authorities, reporting lines, and continuity.
   - include standards for an inventory of models in use.
   - provide a description of how models will be used for business decisions and strategies.
   - include fair lending considerations, including standards designed to ensure models do not cause or promote discrimination (either through disparate treatment or disparate impact) on a prohibited basis under the Equal Credit Opportunity Act or Fair Housing Act.

2. Evaluate model risk management policies to determine whether they provide appropriate standards over model development, implementation, and use. Consider whether the bank's policies

    - describe controls for model development, implementation, and use, such as
        - controls over data quality and relevance.
        - model approval and change management processes.
        - limits on model use, particularly for models with issues.
        - supplementing model results with other analysis and information.
        - authorities to restrict model usage.
        - controls to protect access to sensitive customer information and data.
        - controls to monitor for potential discriminatory outputs or results.
        - testing the accuracy and completeness of data feeds, confirming related systems are properly integrated, and conducting parallel testing and user acceptance testing before implementation.
        - requirements for approving changes for models moving into production.
    - define acceptable practices for the use of models with outputs that are dependent on other models as inputs or the use of models that are part of a model suite.
    - include standards for the development of thresholds for model accuracy and other performance measures.
    - include procedures for reviewing and responding to unacceptable discrepancies.
    - include standards for acceptable levels of discrepancies between model outcomes and actual or benchmark outcomes.
    - include standards for determining the sensitivity of model inputs.
    - include standards for documentation of model choices with supporting rationale, for example, key assumptions, data inputs, model design, conservative adjustments and other adjustments, data exclusions, and logic underlying the model.
    - include standards for documentation of conceptual understanding of models, including AI approaches.
    - define acceptable practices for the review, approval, use, and back-testing of model overlays, or other adjustments to the bank's models.

3. Evaluate model risk management policies to determine whether they provide appropriate guidance for validation activities. Consider whether the bank's policies define appropriate model validation activities, which may include

    - a program of ongoing monitoring and evaluation of model performance based on the risk of the model, with benchmarking and back-testing, as appropriate.
    - a process to capture timely and forward-looking information for effective ongoing monitoring and outcomes analysis.
    - the prioritization, scope, and frequency of validation activities of all models, including AI models' underlying algorithms and parameters that are frequently updated as new data arrive.
    - standards for the extent of validation that should be performed before models are put into production.

- standards for the extent of revalidation that should be performed before models are put in use after models materially change.
- Standards for the review and decision process when a model should be removed from production.
- procedures for responding to problems that appear.
- requirements for validation of third-party models.
- standards for documenting model validation results.
- controls on the use of external resources for validation.

4. Evaluate model risk management policies to determine whether they provide appropriate issues management and escalation guidance. Consider whether the bank's policies

   - describe escalation processes and remediation actions for model issues, limit breaches, and policy exceptions.
   - describe standards for timely resolution of model issues.
   - require documentation of model issues and the resolution of issues.

5. Evaluate model risk management policies to determine whether they provide appropriate guidance for assessing risk. Consider whether the bank's policies

   - describe the bank's model methodology for assessing model risk.
   - include standards for periodically reviewing and updating, when warranted, model risk assessments.
   - describe model risk reporting processes that address data/information, distributions to relevant stakeholders, and escalation protocols to the board and, when necessary, the OCC.
   - establish communication standards for clearly communicating risk culture, appetite, controls, and related responsibilities and accountability throughout the bank.

6. Evaluate model risk management policies to determine whether they provide appropriate guidance for third-party risk management. Consider whether the bank's policies

   - describe the process used to select and retain third-party models, including the staff who should be involved in such decisions.
   - define expectations for personnel and third parties regarding accessing, transferring, sharing, storing, and securing sensitive customer information used in models.
   - reference other relevant policies related to third-party risk management.
   - include standards for contracts provisions that protect the bank's needs and rights, including privacy and customer information protection and providing for regulator access to information.
   - define expectations for ongoing monitoring of third parties.
   - include standards for the establishment of contingency plans for instances in which third-party models are no longer available or serviced or are no longer reliable.

7. Evaluate model risk management policies to determine whether they provide appropriate guidance regarding model assumptions. Consider whether the bank's policies describe the methodology to periodically reassess the reasonableness and accuracy of model assumptions.

8. Evaluate model risk management policies to determine whether they provide appropriate guidance over data management. Consider whether the bank's policies include standards for data management, such as standards for

   - assessing data sources, quality, limitations, completeness, and relevance.
   - using data proxies.
   - using third-party data.
   - using alternative data.
   - data security.

9. Determine if the bank's model risk management policies are

   - commensurate with the bank's size, complexity, business activities, corporate culture, overall organizational structure, risk appetite, and extent and type of models used.
   - sufficiently detailed to allow personnel to fully understand the nature and extent of their responsibilities.
   - adjusted to new technologies, products, and services associated with its models.
   - periodically reviewed and approved by the board, or a designated committee.
   - reviewed and updated annually or as necessary to remain appropriate and keep current with changes in market conditions, industry practices, bank products and strategies, and bank exposures and activities.

Processes

Processes are the procedures, programs, and practices that impose order on a bank's pursuit of its objectives. Processes define how activities are carried out and help manage risk. Effective processes are consistent with the underlying policies and are governed by appropriate checks and balances (such as internal controls).

Objective: To determine the adequacy of management's planning over the use of models.

1. Evaluate the adequacy of management's planning before implementing new or revised models. Consider whether

   - management identifies all stakeholders and other users that are affected by implementation of new or revised models and coordinates accordingly.
   - management performs an appropriate risk assessment, including assessing the risk from potential critical third parties, before designing or selecting new models.

- management's decision to implement new models or revise models is based on sound and complete information, realistic assessments of the risks involved, management's expertise, and the bank's operating capacity.
- management has identified which technologies, products, and services associated with models would best fit with the bank's overall strategic plan, goals, risk appetite, and specific model objectives.
- management has identified the impact of changes in economic conditions and the business environment that could affect model risk.
- management understands the purpose of models, models' limitations, and how models work.
- new technology and data management associated with new models can be integrated with the bank's legacy systems.
- there are appropriate controls for monitoring outputs or results that are potentially discriminatory on a prohibited basis.
- there are appropriate controls for protecting sensitive customer information.
- policies, processes, and staffing are appropriate for supporting the model or, if not, whether appropriate changes are planned.
- the technology supporting the model or the model's MIS is scalable (e.g., will the technology be able to handle an increased customer base, processing volumes, and data, and be able to adjust to consumer wants and needs).
- personnel have appropriate expertise to carry out plans effectively and in a manner that is consistent with the bank's model risk management framework.

2. Consider how management determines the effect of new activities on the bank's existing models.

3. Determine whether management implements appropriate controls before putting a model or related technology into production.

4. Assess the appropriateness of the bank's resiliency plans. Determine whether management

   - plans for potential interruptions in the effectiveness and functioning of all critical models, such as power outages and natural disasters.
   - identifies any performance deterioration due to interruptions in a timely manner.
   - considers and modifies any resulting effects on model risk management when significant interruptions occur.
   - incorporates new data points provided by unprecedented scenarios (e.g., pandemics or other significant disruptions) into model assumptions to ensure the validity of outputs.

Objective: To determine the adequacy of the bank's model risk assessment processes.

1. Determine whether the bank's risk assessment process

   - identifies risk both from individual models and models in the aggregate.

- identifies the model's capabilities and limitations.
- measures the risks associated with model activities accurately and in a timely manner.

2. For a bank undergoing mergers or consolidations, determine whether the bank has assessed

   - if there are any open issues related to its models or model risk management.
   - sources of risk within models acquired.
   - alignment of model definitions.
   - the target bank's model inventory.

3. Assess if the bank's model risk assessment rating methodology considers model

   - types and objectives.
   - complexity, uncertainty, and materiality.
   - interrelationships.
   - assumptions.
   - data.
   - capabilities and limitations.
   - validation activities, frequency, and resources.
   - explainability for AI models.

Objective: To determine the adequacy of management's maintenance of a comprehensive set of information (e.g., model inventory) for models in use, under development, or recently retired.

1. Verify that the bank maintains an up-to-date, bank-wide model inventory and has assigned responsibility for maintaining the inventory.

2. Determine if the level of information included in the bank's inventory is commensurate with the type, complexity, and objectives of each model and the bank's overall level of model usage. Consider whether the model inventory includes the following:

   - Model identifier
   - Model version
   - Whether the model was developed in-house or by a third party
   - Model dependency, describing whether the outcome of one model is being used as input into another model
   - Model owner and user(s) by title or group (e.g., chief compliance officer or compliance department)
   - Status of model (e.g., in development, production, decommissioned)
   - Approval date of model, or timeline for approval
   - Description of the purpose and products for which the model is designed
   - Description of actual or expected usage
   - Description of any restrictions on use or other controls (e.g., more frequent monitoring and appropriate benchmarking)

- Type and source of inputs used by each model and underlying components of each model (which may include other models)
- Description of the type of technology or approach used
- Model outputs and their intended use
- Identification of individuals responsible for various aspects of the model development and validation
- Type (e.g., credit, compliance) and level of risk
- Dates of completed and planned validation activities, ongoing monitoring frequency, and description of validation results/status (e.g., fit for purpose, approval), and changes made to the models that management deems to be material. For example, if a bank makes any material change to a model, the model should be validated. That information should be captured in the "planned validation activities" in the inventory.
- Description of any model issues or limitations
- Summary of model issue status (e.g., work in progress, partially completed)
- Description of any model overlays
- Indication of whether models are functioning properly
- Description of when the model was last updated
- A list of any exceptions to policy
- Time frame that the model is expected to remain valid.

Objective: To determine the adequacy of the bank's documentation for model selection, development, and validation. Select a sample of model documentation for review. For more information regarding judgmental and statistical sampling, refer to the "Sampling Methodologies" booklet of the *Comptroller's Handbook.*

1. Verify that model documentation includes information supporting decisions related to model selection, testing, governance, development, internal controls, and third-party risk management. Consider whether documentation includes

   - model assumptions and limitations in consideration of the model's use.
   - theoretical approach and supporting research, as appropriate.
   - model design and formulas.
   - data coverage, sources, quality, and limitations.
   - description and interpretation of testing diagnostics, model outcomes, and expected performance under a variety of economic conditions and business environments.
   - an explanation of the degree to which underlying input-output relationships predict model outcomes.
   - change logs.
   - ongoing monitoring plans.
   - a description, frequency, and standards of monitoring for each model, including performance metrics used in ongoing monitoring, performance thresholds, and supporting rationale.
   - business uses.

2. Analyze documentation for model development and validation and determine if it is sufficiently detailed so that parties unfamiliar with the model can understand how the model operates, its limitations, and its key assumptions.

3. Determine whether the bank maintains a detailed record of model change history that tracks model version, rationale and support, related tests, and approvals.

4. If the bank uses models from a third party, verify that bank management maintains appropriate documentation of the third party's approach so that the model can be appropriately validated.

Objective: To determine the adequacy of the quality, integrity, and management of the data and other information used to develop a model.

1. Through discussions and review, determine if developers are able to demonstrate that the data and other information used to develop the model are suitable for the model's purpose and use and are consistent with the theory behind the approach and with the chosen methodology. Consider the following:

   - If data proxies are used, determine whether proxies are appropriately identified, justified, and documented.
   - If data and information are not representative of the bank's current portfolio or business practices, or if assumptions are made to adjust the data and information, determine whether these factors are properly tracked and analyzed so users are aware of potential limitations.
   - Determine whether the model implementation process uses similar data as used in the model development process.

2. Evaluate if the bank documents the major data sources used in the risk measurement process. Consider whether there is

   - reasonable and reconcilable support for the qualitative factors used to account for environmental differences between quantitative estimates and current market conditions.
   - regularly performed analysis of the integrity and applicability of internal and external information sources and related controls.
   - regularly performed analysis of the software, such as APIs, allowing connectivity to models and data.

Objective: To determine the adequacy of the bank's model development process.

1. Evaluate the model development process to assess its effectiveness. Consider whether

   - the process begins with a clear statement of purpose to ensure that model development is aligned with its intended use.
   - alternative theories and approaches are compared and documented.

- the design, theory, and logic underlying the model are well-documented and appropriately supported by published research or sound industry practice, based on the type and complexity of the model.
- the model methodologies and processing components that implement the theory, including the mathematical specification and the numerical techniques and approximations, are explained in detail with particular attention to merits and limitations.
- the components work as intended, are appropriate for the intended business purpose, and are conceptually sound and mathematically and statistically correct.
- all model choices and specifications, including the overall theoretical construction, key assumptions, data, and specific mathematical calculations, are supported by documented empirical evidence and appropriate sensitivity analysis.
- the process provides for effective challenge (e.g., regarding model limitations and assumptions) and approval from qualified personnel.

2. Determine whether the algorithms, mathematical formulas, computer code, software, IT systems, and other critical elements implementing the model are subject to appropriate quality control and change control procedures to confirm that the code is correct, that it cannot be altered except by approved parties, and that all changes are logged and can be audited.

3. Assess the appropriateness of the bank's processes for selecting third-party models, including purchasing generic third-party models. Consider whether management requires that the third parties provide

   - developmental evidence explaining the model components, design, structure, data, and intended use.
   - appropriate testing and performance results that show their product works as expected.
   - clear indication of the model's limitations and assumptions and where the product's use may be problematic.
   - clear explanation and instructions for model implementation, including any decisions that must be made in terms of parameters or thresholds.

4. Determine whether bank personnel have developed and implemented appropriate policies, standards, processes, and controls for testing the bank's models. Consider whether the testing

   - checks the model's accuracy.
   - demonstrates the model is robust and stable.
   - assesses potential limitations.
   - evaluates the model's behavior by conducting sensitivity analysis over a range of input values.
   - assesses the impact of assumptions.
   - identifies situations where the model performs poorly or becomes unreliable.

- applies testing to circumstances under a variety of market, financial, or environmental conditions, including scenarios that are outside the range of ordinary expectations.
- evaluates extreme values for inputs and establishes caps and floors on the range of inputs to identify any boundaries of model effectiveness.
- covers the variety of products or applications for which the model is intended.
- evaluates the impact of model results on other models that rely on those results as inputs.
- includes the purpose, design, and execution of test plans, summary results with commentary and evaluation, and detailed analysis of informative samples.
- is appropriately documented, including documentation of adjustments made as well as the rationale and methodology.
- evaluates whether the development of judgmental or qualitative aspects of models (e.g., inputs, or adjustments to outputs) are appropriate, conducted in a systematic manner, and well-documented.
- assesses whether third-party models are working as expected.
- indicates third-party models' limitations and assumptions.

5. Assess the appropriateness of the bank's processes to validate models that have been adjusted or redeveloped before implementation. Consider whether material changes in model structure or technique and all model redevelopment are subject to validation activities of appropriate range and rigor before implementation.

Objective: To determine if the bank has adequate procedures to address feedback from model users and personnel independent from the line of business using the model.

1. Evaluate the bank's process for soliciting feedback and insights from model users.

2. Evaluate the bank's process for soliciting feedback from sources independent of the line of business using the model.

3. Assess the adequacy of the bank's process for tracking the effectiveness of model use over time.

4. Evaluate the adequacy of processes regarding the review, approval, use, and back-testing of model overlays and adjustments. Consider whether

   - the development and use of model overlays, applied both within the model and at model output, are a well-documented and transparent process with appropriate justification related to specific model issues and limitations.
   - model adjustments are clearly outlined and consistent with assumed scenario conditions, and model results are provided with and without adjustments.
   - to the extent that a bank claims that model outputs are conservative, the bank substantiates the claim and includes a definition and measurement of that conservatism that is communicated to model users.

- model validators or other reviewers have appropriate technical and substantive knowledge of the model being validated, including knowledge of the type of model, to understand and review performance, overlays, and adjustments.
- the bank has a process to monitor and analyze overlays and adjustments over time and address the underlying limitations and issues through data enhancements, model recalibration, or redevelopment.
- management considers potential fair lending implications and other consumer protection-related laws and regulations when applying overlays and adjustments.

5. Assess management's support for model overlays and adjustments.

Objective: To determine the adequacy of model risk management reports.

1. Evaluate the adequacy of the reports used by senior management and the board for model risk. Evaluate whether the reports

   - are comprehensible, accurate, timely, relevant, complete, and sufficiently detailed.
   - clearly explain model assumptions and limitations.
   - include sufficient information to keep relevant parties informed of model performance.
   - evolve as the bank grows in size and complexity, and as the bank's risk profile changes.
   - give decision makers important indicators and thresholds of the model's accuracy, robustness, stability, and limitations.
   - clearly define and escalate, as appropriate, proposed changes and expected impacts of those changes.

2. Assess the adequacy of reports presented to the board. Determine if reports

   - highlight performance measures, trends, and variances.
   - compare performance with business unit or bank-wide limits.
   - contain risk appetite metrics or data on other key risk indicators for model risk.
   - explain model performance variances and provide action plans and recommendations for addressing significant deterioration and issues.

Objective: To assess the adequacy of the bank's model validation process. Select a sample of validation reports for review. For more information regarding judgmental and statistical sampling, refer to the "Sampling Methodologies" booklet of the *Comptroller's Handbook.*

1. Determine if the range and rigor of the bank's model validation process are commensurate with the bank's overall use of models; the complexity, materiality, types, and objectives of its models; and the size and complexity of the bank's operations. Consider whether

   - the validation process includes a defined purpose and goals.

- validators have the authority to effectively challenge model developers and users and escalate validation findings, including issues and limitations, for timely and appropriate resolutions.
- the scope, validation approach, schedule, resources, and types and extent of validation activities and tasks are appropriate.
- the validation process notes specific actions that must be taken to complete individual validation activities and tasks.
- all models, including those developed in-house and those purchased from or developed by third parties, are subject to sufficient validation.
- each model receives a periodic review to determine whether it is working as intended, if documentation is appropriate, and if existing validation activities are sufficient.
- models undergo the full validation process at fixed intervals, including updated documentation of all activities.
- validation documentation is detailed and demonstrates that all validation procedures are appropriately completed.
- all model components, including input, processing, and reporting, are subject to validation.

2. Verify that the bank's model validation process includes the following three core elements:

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

3. Assess the adequacy of validation activities before a model is put into use. Consider whether

   - the rigor of validation is commensurate with the potential risk presented by use of the model.
   - the bank prohibits using models with validations showing significant issues. If not, consider whether the bank permits use of such models only under tight constraints and until the issues are resolved.
   - there are appropriate risk mitigations or compensating controls for models with issues or exceptions (e.g., model implemented without being fully validated).

4. Assess the adequacy of validation reports. Consider whether validation reports

   - articulate model aspects that were reviewed.
   - highlight potential issues over a range of financial and economic conditions.
   - determine whether adjustments or other compensating controls are warranted.
   - include
     - clear executive summaries.
     - a statement of model purpose.

  - an accessible synopsis of model and validation results, including major limitations and key assumptions.
  - the results of ongoing monitoring, process verification, benchmarking, and outcomes analysis.

Objective: To determine the adequacy of the evaluation of the conceptual soundness element within the bank's model validation process.

1. Determine whether the evaluation of conceptual soundness

   - assesses whether the model achieves the intended purpose.
   - assesses the quality of the model design and construction.
   - entails review of documentation and empirical evidence supporting the methods used and variables selected for the model.
   - evaluates the quality and extent of developmental evidence.
   - provides appropriate critical review of model selection and development.
   - determines if the model reflects sound theory and business practice.
   - compares alternative theories and approaches.
   - verifies model stability and accuracy.
   - assesses key assumptions and variables, with analysis of their impact on model outputs and particular focus on any potential limitations.
   - evaluates the relevance and sufficiency of the data used to build the model to validate it is reasonably representative of the inputs for the model, such as the bank's portfolio, account activity, or market conditions, depending on the type of model.
   - verifies the effectiveness of model performance with respect to the range of model inputs and assumptions.
   - assesses whether biases are present in data and model outcomes, and the extent and implications of any such biases.
   - includes sensitivity analysis and stress testing, as appropriate.

2. For models that may be difficult to evaluate for conceptual soundness, determine whether the level of transparency and explainability is appropriate to the specific model's use and risks associated with that use.

3. When appropriate to a particular model, determine whether validation employs sensitivity analysis. Consider whether the validation

   - checks the impact of small changes in inputs and parameter values on model outputs to determine whether they fall within an acceptable range.
   - varies several inputs simultaneously to identify unexpected interactions.
   - checks performance over a wide range of inputs and parameter values, including extreme values, to verify the model's robustness.

- helps establish the boundaries of model performance by identifying the acceptable range of inputs as well as the conditions under which the model may become unstable or inaccurate.
- is repeated periodically.

4. Evaluate how management uses the results of sensitivity analysis or other quantitative testing.

Objective: To determine the adequacy of the ongoing monitoring element of the bank's model validation process.

1. Determine whether the ongoing monitoring includes

   - assessment of adherence to the established risk appetite.
   - assessment of adherence to internal limits on model use and targets for model accuracy or reliability.
   - mechanisms for the board to hold management accountable for operating within limits on model use and targets for model accuracy or reliability.
   - analysis of overrides, including evaluating the reasons for, and reasonableness of, overrides, and tracking and analyzing override performance.
   - assessment of model limitations identified in the development stage.
   - sensitivity analysis and other checks for robustness and stability.
   - review of risk measurements and performance thresholds.
   - early-warning analysis with interpretation of testing metrics and performance diagnostics to support conclusions.
   - escalation processes and risk mitigation actions when a significant breach of a performance threshold occurs.
   - timely systems updates.
   - timely updates to reflect changes in laws and regulations (e.g., through the bank's CMS).
   - analysis of the integrity and applicability of internal and external information sources, including information provided by third parties.
   - process verification and benchmarking.
   - procedures for responding to, and escalating, identified issues.

2. Confirm that monitoring begins when the model is first implemented and that it continues at a frequency appropriate for the nature of the model, the availability of new data or modeling approaches, and the magnitude of risks involved.

3. Determine whether ongoing monitoring includes an analysis of overrides. Assess the reasonableness of the bank's assessment of the rate of overrides.

4. Determine whether monitoring reports are timely and accurate, and distributed to appropriate individuals including the board, when appropriate.

Objective: To determine the adequacy of process verification, as part of ongoing monitoring.

1. Determine whether process verification

   - verifies that internal and external data inputs continue to be accurate, complete, consistent with model purpose and design, and of sufficient quality.
   - verifies inputs are processed as expected.
   - includes a review of reports derived from model outputs as part of validation to verify that they are accurate, complete, and informative, and that they contain appropriate indicators of model performance and limitations.

2. Determine whether computer code implementing the model is subject to rigorous quality and change control procedures to confirm that the code is correct, that it cannot be altered except by approved parties, and that all changes are logged and can be audited.

Objective: To determine the adequacy of benchmarking activities, as part of ongoing monitoring.

1. Assess the appropriateness of

   - the types of benchmarking activities conducted.
   - the accuracy and completeness of benchmark data.
   - how any discrepancies between the model output and benchmarks are investigated.
   - the validation work of the benchmark model, including third-party models, as applicable.

Objective: To determine the adequacy of the outcomes analysis element of the bank's model validation process.

1. Determine whether outcomes analysis, as appropriate,

   - compares the model estimates and outputs to actual outcomes.
   - helps to evaluate model performance, by establishing expected ranges for actual outcomes in relation to the intended objectives and assesses the reasons for observed variation between the two.
   - includes effective performance monitoring commensurate with the objectives of the model.
   - includes appropriate tests, such as assessment of the accuracy of estimates or forecasts or an evaluation of rank-order ability.
   - relies on statistical tests or other quantitative measures or includes subjective or qualitative measures derived from expert judgement.
   - includes multiple tests, since one individual test will have weaknesses (e.g., some tests are better at checking a model's ability to rank-order or segment observations on a relative basis, whereas others are better at checking absolute forecast accuracy).
   - tests whether the model continues to perform in line with design objectives and business uses and is conducted on an ongoing basis.

2. Assess the appropriateness of the types of testing and techniques used in outcomes analysis. Verify the selection is appropriate and based on the model's methodology, its complexity, data availability, and the magnitude of potential model risk to the bank.

3. If outcomes analysis produces evidence of poor performance, determine whether the bank takes appropriate action, including escalating findings of poor performance and adjusting, recalibrating, or redeveloping the model, to address those findings.

4. Determine if the bank employs outcomes analysis consisting of "early warning" metrics designed to measure performance beginning shortly after model implementation and trend analysis of performance over time.

Objective: To determine the adequacy of back-testing as part of outcomes analysis.

1. Determine whether back-testing

   - compares the actual outcomes with model forecasts during a sample time period not used in the model development, and at an observation frequency that matches the forecast horizon or performance window of the model.
   - analyzes model performance after the model is used in production on a regular basis as new performance data arrive.
   - uses expected ranges or statistical confidence intervals around the model forecasts.

2. Determine whether models with long forecast horizons are back-tested and supplemented by evaluation over shorter periods.

3. If back-testing outcomes fall outside performance thresholds, determine whether the bank analyzes the discrepancies and investigates the causes that are significant in terms of magnitude and frequency to determine whether the differences stem from

   - omission of material factors from the model.
   - errors with regard to other aspects of model specification.
   - factors that are purely random, temporary, and consistent with acceptable model performance.
   - changes in the economic environment or business practices.
   - data anomalies or data quality issues.

4. Assess the adequacy of how bank management incorporates back-testing results into the model development, use, and risk management.

5. Assess the appropriateness of how back-testing results are communicated and how models are recalibrated based on back-testing results.

Objective: Assess the adequacy of the bank's risk management over third-party models, third-party data, or third parties used for model development or for performing services related to model risk management.

1. If the bank uses third-party models, engages third parties for model development, uses third-party data, or engages third parties to perform services related to model risk management, determine if such third parties are incorporated into the bank's broader third-party risk management and model risk management process. Refer to OCC Bulletins 2013-29, 2020-10, 2017-7, 2011-12.

2. If the bank uses a third-party model and obtains information from the third party to support the bank's model risk management, determine whether the information includes

   - developmental evidence explaining the product components, design, and intended use to determine whether the model is appropriate for the bank's products and risk exposures.
   - information regarding the data used to develop the model.
   - sufficiently detailed testing and validation results derived from application of the models on the bank's data that show that the third party's product works as expected.
   - documentation on the model's limitations and assumptions and about where the product's use may be problematic.
   - clear explanation and instructions for model implementation, including any decisions that must be made in terms of parameters or thresholds.

3. If the bank uses models developed by third parties, determine whether the bank independently validates such models using the same principles as for in-house models, with the understanding that processes may be somewhat modified. Consider whether

   - bank management conducts a risk-based review of each third-party model to determine whether it is working as intended and if the existing validation activities are sufficient.
   - the bank understands and makes reasoned determinations for the customization choices of third-party models, and whether the customization choices are documented and justified as part of the bank's validation.
   - the relevance and appropriateness of data and assumptions are validated, if the third parties provide input into data and assumptions.
   - any validation reports provided by a third-party model provider identifies model aspects that were reviewed, highlights potential limitations or issues over a range of financial and economic conditions (as applicable), and determines whether adjustments or other compensating controls are warranted.
   - management understands any limitations experienced by validators of third-party-provided validation reports in assessing models.

4. Through discussions with management, assess if it obtains an understanding of how third-party models operate before purchasing.

5. Determine if management effectively negotiates contracts that protect the bank's needs and rights, including privacy and customer information protection, and provide for regulator access to information.

6. Confirm that bank personnel's customization choices for third-party models are justified, documented, and properly implemented, and determine whether bank personnel understand the customization choices that are necessary or appropriate for the model.

7. If third parties provide input data or assumptions, or use them to build models, determine if bank personnel assess their relevance for the bank's situation, and if the bank's assessment is reasonable.

8. Confirm that the bank has a contingency plan in case the third party or bank terminates the contract, the third party is no longer in business, the model is no longer available, or the model cannot be supported by the third party. The contingency plan may include a plan for the bank to have as much knowledge in-house as possible.

9. Verify the bank conducts ongoing monitoring and outcomes analysis of third-party model performance using the bank's own outcomes and acts on any adverse findings.

10. When the bank engages external resources (i.e., a third party) to help execute certain activities related to model risk management or the bank's ongoing third-party monitoring responsibilities, determine if the bank understands and evaluates the results of validations and risk control activities that are conducted by third parties. Consider if management designates an internal party to

    - determine whether the work performed by the third party meets the standards and controls set forth in the bank's model risk governance framework.
    - verify that the scope of work as defined with a contract or agreement has been completed by the third party.
    - evaluate and track identified issues and ensure they are addressed in a timely manner.
    - make sure completed work is incorporated into the bank's model risk management and third-party risk management processes.

11. Assess the adequacy of validation reporting provided by third parties. Consider whether validation reports

    - include clear executive summaries, with a statement of model purpose and a synopsis of model validation results, including major limitations and key assumptions.
    - identify model aspects that were reviewed.
    - highlight potential limitations or issues over a range of financial, economic, or environmental conditions (as applicable).
    - determine whether adjustments or other compensating controls are warranted.
    - include any limitations experienced by the validator in assessing models.

Personnel

Personnel are the bank staff and managers who execute or oversee processes. Personnel should be qualified and competent, have clearly defined responsibilities, and be held accountable for their actions. They should understand the bank's mission, risk appetite, core

values, policies, and processes. Banks should design compensation programs to attract and retain personnel, align with strategy, and appropriately balance risk-taking and reward.

Objective: To determine the adequacy of board oversight and senior management's implementation of model risk management.

1. Assess the board's oversight of model risk management. Determine if the board

   - establishes the bank's risk appetite for model use.
   - confirms the level of model risk is within its tolerance.
   - directs changes when appropriate.
   - promotes a working environment that supports and encourages effective challenges to risk analysis, validation, testing, development, and other processes related to a bank's model risk management.
   - delegates specific duties and authorities for managing risk to board committees, management committees, and senior management.

2. Given the scope and complexity of the bank's model usage, assess the adequacy of management's oversight of model risk management. Consider

   - management's expertise and training.
   - the expertise, training, and number of staff.
   - the establishment of position descriptions that include model risk management, as appropriate.
   - the establishment of a performance appraisal process and compensation programs that include model risk management, as appropriate.
   - whether reporting lines encourage open communication regarding model risk management issues and limit the chances of conflicts of interest.
   - management's ability and willingness to address identified model issues.
   - management's responsiveness to regulatory, accounting, industry, and technological changes relevant to model risk management.

3. Evaluate the adequacy of senior management's implementation of sound model risk management. Consider whether management

   - establishes adequate policies and procedures and holds staff accountable for adhering to policies and procedures.
   - promotes a working environment that supports and encourages effective challenges to risk analysis, validation, testing, development, and other processes related to a bank's model risk management.
   - assigns competent and sufficient staff, budget, and other resources.
   - implements a performance appraisal process to reinforce responsibility and accountability for personnel responsible for model risk management.
   - oversees model development and implementation.
   - evaluates model results.

- engages in effective challenge.
- reviews validation and internal audit findings.
- takes prompt remedial action when necessary.
- reports to the board on significant model risk, for both individual models and for models in the aggregate, and on adherence to policies.

4. Review board and other committee minutes for model risk management-related information. Assess the adequacy of information reviewed by the board or committees. Well-documented minutes generally include sufficient information that reflects whether directors

   - are fully informed about the relevant facts.
   - understand the risks associated with the bank's use of models.
   - deliberate significant issues.
   - act independently.
   - provide effective challenge to risk analysis, validation, testing, development, and other processes related to model risk management, when necessary.
   - make decisions based on the best interest of the bank.
   - approve previous meeting minutes.

5. Determine if senior management has well-thought-out personnel development, recruiting, succession planning, and compensation processes to continue to meet the need for individuals with highly technical skills for model development, and for model risk management across the three lines of defense, as appropriate.

6. Assess performance management and compensation programs as they relate to model risk management. Consider whether these programs measure and reward performance that aligns with the bank's strategic objectives and risk appetite.

   If the bank offers incentive compensation programs, determine whether they (1) provide employees with incentives that appropriately balance risk and reward; (2) are compatible with effective controls and risk management; and (3) are supported by strong corporate governance, including active and effective oversight by the bank's board of directors. For more information about incentive compensation, refer to OCC Bulletin 2010-24.

Objective: To determine the adequacy of model risk management personnel in executing their responsibilities.

1. Evaluate the adequacy of personnel responsible for model risk management. Consider whether

   - personnel have the skills and technical knowledge to appropriately manage, maintain, test, and validate models, including the ability to
     - conduct meaningful analysis and challenge with respect to a model's development, implementation, use, and validation.
     - communicate information in nontechnical terms to the board.

- personnel receive sufficient training to carry out their responsibilities.
- IT personnel have the requisite skills to manage IT systems that support the bank's models and model-related controls.

2. Evaluate the adequacy of model owners (i.e., the first line of defense) in carrying out their responsibilities. Consider whether model owners

   - establish and implement policies, standards, and processes for model risk management within the business unit.
   - maintain accountability for model use and performance within the framework set by bank-wide policies and procedures.
   - oversee proper model development, implementation, and use.
   - adhere to the bank's validation and approval processes.
   - identify new or changed models promptly.
   - provide all necessary information for validation activities.
   - establish and maintain
     – processes for identifying, measuring, monitoring, and controlling the risks associated with the business unit's models, consistent with the established risk appetite.
     – internal controls that are properly designed, tested, and work effectively.
     – testing during model development, implementation, and use.
     – documentation standards for processes and related decisions for business unit models, including, for example, documentation of decisions resulting in changes to the model components.

3. Assess the adequacy of technical expertise of the personnel responsible for model validation to determine if expertise is commensurate with the complexity and type of the models, both in structure and how they are applied. Consider whether the validators

   - have a significant degree of familiarity with the line of business using the model and the model's intended use.
   - have explicit authority to challenge developers and users, and evaluate their findings, including issues and deficiencies.
   - have compensation and performance evaluation standards that are tied directly to the quality of model validations and the degree of critical, unbiased review.
   - have a reporting structure that provides sufficient incentive, influence, and stature within the bank to ensure that any material issues are appropriately addressed in a timely manner.

Control Systems

Control systems are the functions (such as internal and external audits and quality assurance) and information systems that bank managers use to measure performance, make decisions about risk, and assess the effectiveness of processes and personnel. Control functions should

have clear reporting lines, sufficient resources, and appropriate access and authority. Management information systems should provide timely, accurate, and relevant feedback.

Objective: To determine whether control systems support effective model risk management.

1. Evaluate the effectiveness of monitoring systems to identify, measure, and track exceptions to policies and established limits.

2. Evaluate whether MIS provide timely, accurate, and useful information to evaluate risk levels and trends in the bank's model risk management.

3. Assess the IT systems that support models. Consider whether the bank confirms

   - the accuracy and timeliness of data and reporting integrity of the bank's IT systems.
   - that IT systems are coupled with controls and testing to assess proper implementation of models, effective IT system integration, and appropriate use.

4. Determine whether management assesses and coordinates the capabilities and requirements of the bank's IT systems and controls before the development or implementation of a model. Consider the impact of

   - security weaknesses, such as poorly constructed APIs or third-party applications.
   - weaknesses in the controls for the access, authentication, sharing, transmission, and storage of sensitive customer information.

5. Determine whether system integration is subject to change management and control procedures.

Objective: To determine the adequacy of IRM's (i.e., control staff) oversight of model risk management.

1. Determine whether IRM communicates issues and problems identified through validation and other forms of oversight to relevant individuals and business users throughout the organization, including senior management, with a plan for corrective action.

2. Assess the adequacy of processes to periodically evaluate model risk management internal controls.

3. Evaluate the adequacy of IRM in carrying out its role as control staff. Consider whether IRM

   - implements policies, standards, and processes for model risk management within the business unit.
   - has the authority to restrict the use of models and monitor any limits on model usage.
   - establishes and implements processes for identifying, measuring, monitoring, and controlling risks enterprise-wide, for individual models and in the aggregate.

- validates the model inputs and outputs independently of business unit testing.
- confirms that the bank's models are working properly and as originally intended.
- validates controls and introduces additional controls, such as automated processes, user access controls, and documentation standards.
- assesses identified issues for themes or patterns.
- provides effective challenge to business unit risk management processes.
- independently measures risk.
- reports to senior management and the board
  - business units' adherence to the bank's risk appetite.
  - differences in risk opinion between business units and IRM.
  - on monitoring of risks enterprise-wide and providing input into key risk decisions.

Objective: To determine the adequacy of internal audit of model risk management.

1. Evaluate the adequacy of internal audit. Assess the scope, frequency, effectiveness, and independence of audits of model risk management. Evaluate whether internal audit

   - independently and objectively performs its duties.
   - operates with the proper incentives.
   - encompasses the appropriate skills and training.
   - operates with adequate stature in the bank.
   - assesses the overall effectiveness of model risk management, including from the framework's ability to address model risk for individual models and in the aggregate.
   - evaluates whether model risk management is comprehensive, rigorous, and effective.
   - verifies that acceptable policies are in place and are appropriately adhered to.
   - documents and reports its findings to the board or the audit committee in a timely manner.
   - verifies records of model use and validation to test whether
     - validations are performed in a timely manner.
     - models are subject to controls that appropriately account for any weaknesses in validation activities.
     - model issues are appropriately addressed in a timely manner
   - assesses the accuracy and completeness of the model inventory.
   - evaluates the processes for establishing and monitoring limits on model usage.
   - determines whether procedures for updating models are clearly documented, and tests whether those procedures are being carried out as specified.
   - assesses adherence to documentation standards, including risk reporting.
   - performs assessments of supporting operational systems.
   - evaluates the reliability of data used by models.
   - identifies and assesses potential biases in the data that may give rise to fair lending concerns (including concerns of disparate treatment or disparate impact on a prohibited basis), and identifies and assesses management's understanding and oversight of any potential biases.

- evaluates the objectivity, competence, and organizational standing of the key validation participants, with the ultimate goal of ascertaining whether those participants have the right incentives to discover and report issues.
- reviews the validation activities conducted by internal personnel and third parties, with the same rigor, to assess the appropriateness of validation activities.
- assesses whether there is sufficient reporting to the board and senior management.

2. For a bank that does not have a standalone model audit, consider how internal audits' reviews of other areas assess model risk management.

3. Assess the qualifications and expertise of in-house, outsourced, or co-sourced audit staff.

4. Determine if the bank exercised appropriate due diligence when entering into audit-related third-party relationships and if the bank implemented effective oversight and controls afterward.

Objective: To determine the adequacy of management's actions in response to findings identified by IRM, validation activities, and audit reviews.

1. Evaluate the effectiveness of communication standards between IRM and management regarding findings identified through validation and other forms of oversight.

2. Determine whether IRM and audit findings, and management responses to those findings, are documented and tracked for adequate follow-up.

3. Evaluate whether management gives identified findings appropriate and timely attention.

4. Assess whether management's actions taken in response to findings have been verified and reviewed by senior management and the board.

Conclusions

Conclusion: The aggregate level of each associated risk is (low, moderate, or high). The direction of each associated risk is (increasing, stable, or decreasing).

Objective: To determine, document, and communicate overall findings and conclusions regarding the examination of model risk management.

1. Determine preliminary examination findings and conclusions and discuss with the EIC, including

   - quantity of associated risks (as noted in the "Introduction" section).
   - quality of risk management.
   - aggregate level and direction of associated risks.
   - violations and deficient practices.

Summary of Risks Associated With a Bank's Model Use				
Risk category	**Quantity of risk** (Low, moderate, high)	**Quality of risk management** (Weak, insufficient, satisfactory, strong)	**Aggregate level of risk** (Low, moderate, high)	**Direction of risk** (Increasing, stable, decreasing)
Credit				
Interest rate				
Liquidity				
Price				
Operational				
Compliance				
Strategic				
~~Reputation~~				

2. If substantive safety and soundness concerns remain unresolved that may have a material adverse effect on the bank, further expand the scope of the examination by completing verification procedures.

3. Discuss examination findings with bank management, including violations, deficient practices, and conclusions about risks and risk management practices. If necessary, obtain commitments for corrective action.

4. Compose conclusion comments, highlighting any issues that should be included in the report of examination or supervisory letter. If necessary, compose matters requiring attention (MRA) and violation write-ups.

5. Update the OCC's supervisory information systems and any applicable report of examination schedules or tables.

6. Document recommendations for the supervisory strategy (e.g., what the OCC should do in future model risk management examinations in the bank, including time periods, staffing, and workdays required).

7. Update, organize, and reference work papers in accordance with OCC policy.

8. Appropriately dispose of or secure any paper or electronic media that contain sensitive bank or customer information.

Internal Control Questionnaire

An internal control questionnaire (ICQ) helps an examiner assess a bank's internal controls for an area. ICQs typically address standard controls that provide day-to-day protection of bank assets and financial records. The examiner decides the extent to which it is necessary to complete or update ICQs during examination planning or after reviewing the findings and conclusions of the core assessment.

Applicability: This checklist can be used to help evaluate model risk management. The concepts apply to all model types and can be used to evaluate risk management practices.

Note: Negative responses may indicate a higher level of risk that warrants stronger risk management practices. In such cases, further review may be necessary to determine appropriate practices to mitigate the risks.

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
Board and senior management oversight			
1. Have the board and senior management established an effective model risk management framework that applies to all models and fits into the broader risk management of the bank?			
2. Does the framework apply to the full range of models in use?			
3. Does the framework include standards for model development, implementation, use, and validation?			
4. Do the board and management promote a working environment that supports and encourages effective challenges to risk analysis, validation, testing, development, and other processes related to a bank's model risk management?			
5. Are formal policies and procedures governing model use and oversight commensurate with the bank's complexity, business activities, corporate culture, overall organizational structure, and extent and types of models used?			
6. Is there a clear escalation process that permits significant issues with model use and policy compliance to reach appropriate levels of senior management and the board?			
7. Are board reports tailored to the bank's size, complexity, risks, and model usage?			
8. Do board and management reports clearly explain model assumptions and limitations?			
9. Do model risk management reports include measures on			
• the volume of models considered high risk?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
• models with temporary exemptions or provisional approvals?			
• status of model issues (e.g., work in progress, partially completed).			
• underperforming models?			
• models with past-due validations?			
• models in use without validation?			
• model development efforts in progress?			
Personnel			
1. Are the skills and expertise of management and other personnel commensurate with the nature, extent, and complexity of the use of models?			
2. Is there sufficient cross-training of bank staff so that any aspect of model risk management is not dependent on one employee?			
3. Does each model have a defined owner accountable for use and performance within the framework set by bank policies and procedures?			
4. Are model owners responsible for implementing policies, standards, and processes for model risk management within the business unit?			
5. Are model owners responsible for establishing and maintaining			
• processes for identifying, measuring, monitoring, and controlling the risks associated with the business unit's models, consistent with the established risk appetite?			
• internal controls that are properly designed, tested, and work effectively?			
• testing during model development, implementation, and use?			
• documentation standards for processes and related decisions for business unit models, for example, documentation of decisions resulting in changes to the model components?			
6. Is control staff (i.e., IRM) independent from model owners and model developers, to the extent possible?			
7. Is control staff (i.e., IRM) responsible for			
• implementing policies, standards, and processes for model risk management within the business unit?			
• establishing and implementing processes for identifying, measuring, monitoring, and controlling risks enterprise-wide, for individual models and in the aggregate?			
• validating the model inputs and outputs?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
• confirming that the bank's models are performing as intended?			
• validating controls and introducing additional controls, such as automated processes, user access controls, and documentation standards?			
• assessing identified issues for themes or patterns?			
• providing credible effective challenge to business unit risk management processes?			
• independently measuring risk?			
• reporting to senior management and the board			
– business units' adherence to the bank's risk appetite?			
– differences in risk opinion between business units and IRM?			
– on monitoring of risks enterprise-wide and providing input into key risk decisions?			
8. Do control processes ensure that			
• appropriate resources are assigned for model validation and for guiding the scope and application of the work?			
• problems identified through validation and control systems are communicated to relevant parties throughout the organization, with a plan and monitoring of corrective action and remediation?			
• control staff has the authority to restrict model use and monitor any limits as necessary?			
• when validation-work exceptions occur, other control mechanisms, such as timeliness for completing validation work and limits on model use, are established?			
Policies and procedures			
1. Do policies and procedures			
• describe governance and controls over the model risk management process?			
• establish model risk management internal controls.			
• describe the model risk management framework how the framework is applied to different types of models?			
• require maintenance of detailed documentation of all aspects of the model risk management framework?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
• include definitions of a model and model risk and criteria for when model risk management policies should be applied?			
• describe the process for assessing model risk?			
• define acceptable practices for model development, implementation, use, and validation for all models, including third-party models?			
• identify roles and responsibilities of stakeholders with clear detail on expertise, authorities, reporting lines, and continuity?			
• include standards for an inventory of models in use?			
• describe how models will be used for business decisions and strategies?			
• include fair lending considerations, including standards that help ensure models do not cause or promote discrimination (either through disparate treatment or disparate impact) on a prohibited basis under the Equal Credit Opportunity Act and/or Fair Housing Act?			
• describe controls for model development, implementation, and use, such as			
– controls to ensure data quality and relevance for effective modeling?			
– model approval and change management processes?			
– limits on model use (e.g., when model deficiencies are known and/or waiting to be remedied through appropriate testing and analysis)?			
– supplementing model results with other analysis and information?			
– controls to protect access to sensitive customer information and data?			
– controls to monitor for potential discriminatory outputs or results?			
– testing the accuracy and completeness of data feeds, confirming related systems are properly integrated, and conducting parallel testing and user acceptance testing before implementation?			
– requirements for approving changes for models moving into production?			
• define acceptable practices for the use of models with outputs that are dependent on other models as inputs or the use of models that are part of a model suite?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
• include standards for the development of thresholds for model accuracy and other performance measures?			
• include procedures for reviewing and responding to unacceptable discrepancies?			
• include standards for acceptable levels of discrepancies between model outcomes and actual or benchmark outcomes?			
• include standards for determining the sensitivity of model inputs?			
• include standards for documentation of model choices with supporting rationale, for example, key assumptions, data inputs, model design, adjustments, data exclusions, and logic underlying the model?			
• include standards for documentation of conceptual understanding of models, including AI approaches?			
• define acceptable practices for the review, approval, and use of using model overlays, or making other adjustments to the bank's models?			
• define appropriate model validation activities, which may include			
– a program of ongoing monitoring and evaluation of model performance based on the risk of the model?			
– the prioritization, scope, and frequency of validation activities of all models, including AI models' underlying algorithms and parameters that are frequently updated as new data arrive?			
– standards for the extent of validation that should be performed before models are put into production?			
– standards for the extent of revalidation that should be performed before models are put in use after material changes are made?			
– standards for the review and decision process when a model should be removed from production?			
– procedures for responding to problems that appear?			
– requirements for validation of third-party models?			
– standards for documenting model validation results?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
– controls on the use of external resources for validation?			
• describe escalation processes and remediation actions for model issues identified, limit breaches, and policy exceptions?			
• describe standards for timely resolution of model issues?			
• require documentation of model issues and the resolution of issues?			
• describe the bank's model methodology for assessing model risk?			
• include standards for periodically reviewing and updating, when warranted, model risk assessments?			
• describe model risk reporting processes that address data/information, distributions to all relevant stakeholders, and escalation protocols to the board and, when necessary, the OCC?			
• establish communication standards for the communication of risk culture, appetite, controls, and related responsibilities and accountability throughout the bank?			
• describe the process used to select and retain third-party models, including the staff who should be involved in such decisions?			
• define expectations for personnel and third parties regarding accessing, transferring, sharing, storing, and securing sensitive customer information used in models?			
• reference other relevant policies related to third-party risk management?			
• include standards for contracts provisions that protect the bank's needs and rights, including privacy and customer information protection and providing for regulator access to information?			
• define expectations for ongoing monitoring of third parties?			
• include standards for the establishment of contingency plans, for instance, in which third-party models are no longer available or serviced or are no longer reliable?			
• describe the methodology to periodically reassess the reasonableness and accuracy of model assumptions?			
• include standards for data management, such as standards for			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
– assessment of data sources, quality, limitations, completeness, and relevance?			
– using data proxies, i.e., data that are closely related to and serve in place of data that are either unobservable or immeasurable?			
– using third-party data?			
– using alternative data?			
– security data?			
Planning			
1. Does management perform an objective risk assessment before selecting a new model?			
2. Does the bank consider the following as part of planning?			
• Has management identified all stakeholders and other users that are affected by implementation of new or revised models and coordinated accordingly?			
• Has management performed a sufficient risk assessment, including assessing the risk of potential critical third parties, before designing or selecting new models?			
• Is management's decision to implement new models or revise models based on sound and complete information, realistic assessments of the risks involved, management's expertise, and the bank's operating capacity?			
• Has senior management identified which technology, products, and services associated with models would best fit with its overall strategic plan, goals, risk appetite, and, as appropriate, specific model objectives?			
• Has management identified the impact of changes in economic conditions and the business environment that could affect model risk?			
• Does senior management understand the purpose of models, models' limitations, and how models work?			
• Can new technology and data management associated with new models be integrated with the bank's legacy systems?			
• Are there appropriate controls for protecting sensitive customer information?			
• Are there appropriate controls for monitoring outputs of results that are potentially discriminatory on a prohibited basis?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
• Are there appropriate controls for protecting sensitive customer information?			
• Are policies, processes, and staffing appropriate for supporting the model? If not, are appropriate changes to policies, process, and staffing planned?			
• Is the technology supporting the model or the model's MIS scalable (e.g., will the technology be able to handle an increased customer base, processing volumes, and data, and be able to adjust to consumer wants and needs)?			
• Do personnel have appropriate expertise to carry out plans effectively and in a manner that is consistent with the bank's model risk management framework?			
Assessing risk			
1. Does the bank's risk assessment process			
• identify risk from individual models and models in the aggregate?			
• identify the model's capabilities and limitations?			
• measure the risks associated with model activities accurately and in a timely manner?			
2. For a bank undergoing mergers or consolidations, has the bank assessed			
• if there are any open issues related to its models or model risk management?			
• sources of risk within models acquired?			
• alignment of model definitions?			
• the target bank's model inventory?			
3. Does the bank's model risk assessment rating methodology consider model			
• types and objectives?			
• complexity, uncertainty, and materiality?			
• interrelationships?			
• assumptions?			
• data?			
• capabilities and limitations?			
• validation activities, frequency, and resources?			
• explainability for AI models?			
Model inventory			
1. Does the bank maintain an up-to-date set of information for models implemented for use,			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
under development for implementation, or recently retired?			
2. Is a specific party responsible for maintaining a bank-wide inventory of all models?			
3. Is any variation of a model that warrants a separate validation included as a separate model and cross-referenced with other variations?			
4. Does the model inventory include the following?			
• Model identifier			
• Model version			
• Whether the model was developed in-house or by a third party			
• Model dependency, describing whether the outcome of one model is being used as input into another model's responsible business unit			
• Model owner and user(s) by title or group (e.g., chief compliance officer or compliance department)			
• Status of model (e.g., in development, production, decommissioned)			
• Approval date of model, or timeline for approval			
• Description of the purpose and products for which the model is designed			
• Description of actual or expected usage			
• Description of any restrictions on use (e.g., more frequent monitoring and appropriate benchmarking)			
• Type and source of inputs used by each model and underlying components of each model (which may include other models)			
• Description of the technology or approach used			
• Model outputs and their intended use			
• Identification of individuals responsible for various aspects of the model development and validation			
• Type (e.g., credit, compliance) and level of risk			
• Dates of completed and planned validation activities, ongoing monitoring frequency, and description of validation results/status (e.g., fit for purpose, approval), and changes made to the models that management deems to be material. For example, if a bank makes any material change to a model, the model should be validated. That information should			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
be captured in the "planned validation activities" in the inventory.			
• Description of any model issues or limitations			
• Description of model issue status (e.g., work in progress, partially completed)			
• Description of any model overlays			
• Indication of whether models are functioning properly			
• Description of when the model was last updated			
• A list of any exceptions to policy			
• Time frame that the model is expected to remain valid			
Documentation			
1. Does documentation related to model selection, testing, governance, development, internal controls, and third-party risk management include			
• model assumptions and limitations in consideration of the model's use?			
• theoretical approach and supporting research, as appropriate?			
• model design and formulas?			
• data coverage, sources, quality, and limitations?			
• description and interpretation of testing diagnostics, model outcomes, and expected performance under a variety of economic conditions and business environments?			
• change logs?			
• ongoing monitoring plans?			
• a description, frequency, and standards of monitoring for each model, including performance metrics used in ongoing monitoring, performance thresholds, and supporting rationale?			
• business uses?			
2. Is documentation for model development and validation sufficiently detailed so that parties unfamiliar with the model can understand how the model operates, its limitations, and its key assumptions?			
3. Does the bank maintain a detailed record of model change history that tracks model version, rationale and support, related tests, and approvals?			
4. When the bank uses models from a third party, is appropriate documentation of the third-party			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
approach available so the model can be properly validated?			
Data management			
1. Does the bank complete a documented assessment of data quality and relevance?			
2. If data proxies are used, are they appropriately identified, justified, and documented?			
3. If data and information are not representative of the bank's current portfolio or business practices, or if assumptions are made to adjust the data and information, are these factors properly tracked and analyzed so that users are aware of potential limitations?			
4. Does the model implementation process use similar data as used in the model development process?			
5. Is analysis of the integrity and applicability of internal and external information sources and related controls and software, such as APIs allowing connectivity to models and data, regularly performed to determine if revisions or updates are necessary?			
6. Does the bank implement enhanced controls when using alternative data in models?			
7. Does management establish controls to protect sensitive customer information and appropriate security controls related to how the bank and any third parties access, transfer, share, store, and maintain availability, including data backup and replication, of information?			
Model development and implementation			
1. Are development and implementation processes consistent with the situation and goals of the model user and with bank policy?			
2. Does the model development process provide for effective challenge and approval from qualified personnel?			
3. Do personnel involved in model development have adequate technical knowledge, training, and experience, and demonstrate sound judgment?			
4. Are models tailored for specific applications and informed by business uses?			
5. When relying on third-party models, does the bank confirm models are appropriate for intended use and choose models and model variables that are tailored to the bank's objectives, complexity, activities, and risks?			
6. Does management identify a clear statement of purpose as a first step to developing models aligned with the intended use?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
7. Are the design, theory, and logic underlying models well-documented and supported by published research or sound industry practice?			
8. Are the model methodologies and processing components, including the mathematical specification and the numerical techniques and approximations, explained in detail with particular attention to merits and limitations?			
9. Do developers ensure that model components work as intended, are appropriate for the intended business purpose, and are conceptually sound and mathematically and statistically correct?			
10. Does the model development process include documented comparison of alternative theories and approaches?			
11. Does the development process produce documented evidence in support of all model choices, including the overall theoretical construction, key assumptions, data, and specific mathematical calculations?			
12. Are algorithms, mathematical formulas, computer code, software, and IT systems implementing models subject to rigorous quality control and change control processes to confirm that the code is correct, that it cannot be altered except by approved parties, and that all changes are logged and can be audited?			
13. Are the various components of a model and its overall functioning evaluated to determine whether the model is performing as intended?			
14. Does model testing include			
• checking the model's accuracy? • the purpose, design, and execution of test plans, summary results with commentary and evaluation, and detailed analysis of informative samples?			
• demonstrating that the model is robust and stable?			
• assessing potential limitations?			
• evaluating the model's behavior by conducting sensitivity analysis over a range of input values?			
• assessing the impact of assumptions?			
• identification of situations where the model performs poorly or becomes unreliable?			
15. Is testing applied to circumstances under a variety of market, financial, or environmental conditions, including scenarios that are outside the range of ordinary expectations?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
16. Are extreme values for inputs evaluated and caps and floors established over a range of inputs to identify any boundaries of model effectiveness?			
17. Does testing cover the variety of products or applications for which the model is intended?			
18. Is the impact of model results on other models that rely on those results as inputs evaluated?			
19. Are testing activities appropriately documented?			
20. Does the bank verify that the development of judgmental and qualitative aspects of its models are sound?			
21. Do testing processes help management confirm judgmental or qualitative aspects of models are appropriate?			
22. Does documentation include the description of the nature and magnitude of adjustments made as well as the rationale and methodology?			
23. Does third-party model testing include the testing of performance on the bank's portfolio?			
24. Are models validated before being put into use?			
25. Do model users provide insight as to whether models are functioning as intended and assess model performance as models are in use?			
26. Does management consider potential fair lending implications and other consumer protection-related laws and regulations when applying overlays and adjustments?			
27. Do model validators have appropriate technical knowledge to understand and review such overlays and adjustments?			
28. Is the process regarding the review, approval, use, and back-testing of model overlays and adjustments, applied both within the model and to outputs, a well-documented and transparent process with appropriate justification related to specific model issues and limitations, and does this process include			
• clearly outlined assumptions that are consistent with assumed scenario conditions?			
• model results with and without adjustments?			
• an evaluation of whether the overlays made to the models are significant and require revalidation efforts or review?			
• monitoring the length of time an overlay is in use?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
Validation			
1. Is each model reviewed to determine whether it is working as intended and that the existing validation activities are sufficient?			
2. Does the bank prioritize the scope and frequency of validation activities?			
3. Are model reviews and validations (in whole or in part) performed using a risk-based approach, and with a frequency appropriate for, or when there are changes to, a bank's risk profile?			
4. Do appropriate validation requirements apply to models developed in-house as well as to those purchased from, or developed by, third parties?			
5. Do model validation exercises include the following three core elements:			
• Evaluation of conceptual soundness, including developmental evidence?			
• Ongoing monitoring, including process verification and benchmarking?			
• Outcomes analysis, such as back-testing, as appropriate?			
6. Do personnel completing validation work			
• have the requisite knowledge, skills, and expertise, including a significant degree of familiarity with the business line using the model and the model's intended use?			
• have any responsibility for development or use of the model and any stake in whether a model is determined to be valid?			
• have explicit authority to challenge model developers and to evaluate their findings, including issues?			
7. When model developers or users complete validation work, is that work subject to critical review by an independent party with requisite knowledge, skills, and expertise who conducts additional activities to ensure proper validation to the extent possible?			
8. Are compensation practices and performance evaluation standards tied directly to the quality of model validations and the degree of critical, unbiased review where appropriate?			
9. Does management consider transparency and explainability for the use of complex models?			
10. Does management employ sensitivity analysis when appropriate in model development and validation to check the impact of small changes in inputs and parameter values on model outputs to make sure they fall within an expected range?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
11. Does management conduct model stress testing when appropriate to check performance over a wide range of inputs and parameter values, including extreme values, to verify that the models are robust?			
12. Does management have a plan for using the results of any sensitivity analysis and other quantitative testing?			
13. Does management evaluate qualitative information and judgment used in model development, including the logic, judgment, and types of information used, to establish the conceptual soundness of the model, and set appropriate conditions for its use?			
14. Are monitoring reports timely and accurate, and distributed to appropriate individuals including the board, when appropriate?			
15. Does the bank's ongoing monitoring process include			
• assessment of adherence to the established risk appetite?			
• assessment of adherence to internal limits on model use and targets for model accuracy or reliability, as appropriate?			
• mechanisms for the board to hold management accountable for operating within limits on model use and targets for model accuracy or reliability?			
• analysis of overrides, including evaluating the reasons for, and reasonableness of, overrides, and tracking and analyzing override performance?			
• assessment of model limitations identified in the development stage?			
• sensitivity analysis and other checks for robustness and stability?			
• review of risk measurements and performance thresholds?			
• early-warning analysis with interpretation of testing metrics and performance diagnostics to support conclusions?			
• escalation processes and risk mitigation actions when a significant breach of a performance threshold occurs?			
• timely system updates?			
• timely updates to reflect changes in laws and regulations (e.g., through the bank's CMS)?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
• analysis of the integrity and applicability of internal and external information sources, including information provided by third parties?			
• process verification and benchmarking, as appropriate?			
• procedures for responding to, and escalating, identified issues?			
16. Is computer code implementing the model subject to rigorous quality and change control procedures?			
17. Are reports derived from model outputs reviewed as part of validation?			
18. When benchmarking, does the bank use accurate and complete benchmark data?			
19. Does management base the choice of outcomes analysis technique on the model's objectives, methodology, complexity, data availability, and the magnitude of potential model risk to the bank?			
20. Does outcomes analysis involve an appropriate range of tests?			
21. When outcomes fall outside expected ranges or performance thresholds, does management analyze discrepancies and investigate the causes that are significant in terms of magnitude or frequency?			
22. Does the bank employ outcomes analysis consisting of "early warning" metrics designed to measure performance beginning shortly after model implementation and trend analysis of performance over time, as appropriate?			
Third-party risk management			
1. Are third-party models incorporated into the bank's third-party risk management and model risk management processes?			
2. Does management conduct appropriate due diligence on the third-party relationship and the model itself?			
3. When relying on third-party models, do bank personnel confirm models are appropriate for intended use and choose models and model variables that are tailored to the bank's size, complexity, and risks?			
4. To support the bank's use of a third-party model, does the bank obtain from the third party			
• developmental evidence explaining the product components, design, and intended use, to determine whether the model is appropriate for the bank's products and risk exposures?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
• information regarding the data used to develop the model, including use and effect of alternative data?			
• detailed testing and validation results derived from application of the models on the bank's data that show their product works as expected?			
• documentation on the model's limitations and assumptions and about where the product's use may be problematic?			
• explanation and instructions for model implementation, including any decisions that must be made in terms of parameters or thresholds?			
5. Does management understand and make determinations for the customization choices of third-party models?			
6. Are third-party customization choices documented and justified?			
7. Is the bank using the most current release of third-party models?			
8. When relying on third-party data or assumptions, does the bank investigate their relevance?			
9. Does management conduct ongoing monitoring and outcomes analysis of third-party model performance using the bank's own outcomes and act on any adverse findings?			
10. Does management conduct a risk-based review of each third-party model to determine whether it is working as intended and if the existing validation activities are sufficient?			
11. When relying on third-party models, does management obtain ongoing performance monitoring and outcomes analysis of the model conducted by third parties?			
12. Do third parties make appropriate modifications and updates to the model over time, if applicable?			
13. Does the bank have contingency plans for third-party models?			
14. When relying on third-party validation and risk control activities, does management understand and evaluate the results?			
15. Does management's analysis of validation and risk control activities include			
• determining whether the third-party performed work meets the standards and controls set forth in the bank's model risk governance framework?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
• verifying that the scope of work as defined within a contract or agreement has been completed by the third party?			
• evaluating and tracking identified issues and ensuring they are addressed in a timely manner?			
• making sure completed work is incorporated into the bank's model risk management and third-party risk management processes?			
16. Do third-party validation reports			
• identify model aspects that were reviewed, highlighting any potential issues over a range of financial and economic conditions (as applicable), and determining whether adjustments or other compensating controls are warranted?			
• include clear executive summaries, with a statement of model purpose and a synopsis of model validation results, including major limitations and key assumptions?			
17. Does management take into consideration any limitations experienced by validators of third-party-provided validation reports in assessing the models?			
Internal audit			
1. Does internal audit assess the overall effectiveness of the model risk management framework for individual models and in the aggregate?			
2. Are model-related findings documented and reported to the board or its appropriately delegated agent?			
3. Does internal audit have the appropriate skills and adequate stature in the organization?			
4. Does internal audit staff possess sufficient expertise to evaluate model development, use, and validation?			
5. If some internal audit staff perform validation activities, are they excluded from the assessment of the overall model risk management framework?			
6. Does internal audit assess whether personnel involved in model development and validation are independent from model users to the extent possible?			
7. Does the internal audit scope include steps to verify that			
• acceptable policies are in place, and that model owners and control groups comply with policies?			

Model Risk Management Internal Control Questionnaire			
	Yes/no	**Document references**	**Comments**
• the model inventory is accurate and complete?			
• validations are performed in a timely manner and models are subject to controls that appropriately account for any weaknesses in validation activities?			
• model owners and control groups are meeting documentation standards, including risk reporting?			
8. As part of its process reviews, does internal audit evaluate			
• processes for establishing and monitoring limits on model use?			
• the reliability of data used by the models?			
• the objectivity, competence, and organizational standing of key validation participants, to determine whether those participants have the right incentives to discover and report issues?			
9. Does internal audit review validation activities conducted by internal and external parties with the same rigor as internal and external parties to see if those activities are conducted in accordance with prescribed standards?			

Glossary

Algorithm: A set of computational rules to be followed to solve a mathematical problem. More recently, the term has been adopted to refer to a process to be followed, often by a computer.

Artificial intelligence: The application of computational tools to address tasks traditionally requiring human analysis.

Back-testing: A form of outcomes analysis that involves the comparison of actual outcomes with modeled forecasts during a development sample time period (in-sample back-testing) and during a sample period not used in model development (out-of-time back-testing), and at an observation frequency that matches the forecast horizon or performance window of the model.

Benchmarking: An alternative prediction or approach used to compare a model's inputs and outputs to estimates from alternative internal or external data or models.

Data proxies: Data that are closely related to and serve in place of data that are either unobservable or immeasurable.

Explainability: Within the context of AI, the extent to which AI decisioning processes and outcomes are reasonably understood.

Information input component: One of the three components of a model. This component delivers assumptions and data to the model.

Machine learning: A subcategory of artificial intelligence. Machine learning is a method of designing a sequence of actions to solve a problem that optimizes automatically through experience and with limited or no human intervention.

Model: A quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. A model consists of three components: an information input component, which delivers assumptions and data to the model; a processing component, which transforms inputs into estimates; and a reporting component, which translates the estimates into useful business information.

Model overlay: Judgmental or qualitative adjustments to model inputs or outputs to compensate for model, data, or other known limitations. A model overlay is a type of override.

Model suite: A group of models that work together.

Ongoing monitoring: One of the three core elements of model validation. Ongoing monitoring confirms that a model is appropriately implemented and is performing and being used as intended.

Outcomes analysis: The comparison of model estimates and outputs to actual outcomes to help evaluate model performance by establishing expected ranges for actual outcomes in relation to the intended objectives and assessing the reasons for observed variation between the two.

Override: Model output or input that is ignored, altered, rejected, or reversed.

Performance threshold: A particular value or range of values of a performance measure or diagnostic that determines the acceptance or rejection of a model's performance.

Process verification: An element of ongoing monitoring that checks that all model components are functioning as designed by verifying that internal and external data inputs continue to be accurate, complete, and consistent with model purpose and design and of the highest quality available.

Processing component: One of the three components of a model. This component transforms inputs into quantitative estimates.

Reporting component: One of the three components of a model. This component translates the estimates into useful business information.

Validation: Set of processes and activities intended to verify that models are sound and performing as expected, in line with their design objectives and business uses.

References

Regulations

12 CFR 3, Subpart E, "Risk–Weighted Assets—Internal Ratings–Based and Advanced Measurement Approaches," and Subpart F, "Risk–Weighted Assets—Market Risk"
12 CFR 30, appendix A, II.B, "Internal Audit System"
31 CFR Chapter X, "Financial Crimes Enforcement Network, Department of the Treasury"

Comptroller's Handbook

"Bank Supervision Process"
"Community Bank Supervision"
"Corporate and Risk Governance"
"Federal Branches and Agencies Supervision"
"Fair Lending"
"Foreword"
"Interest Rate Risk"
"Internal and External Audits"
"Large Bank Supervision"
"Sampling Methodologies"

OCC Issuances

OCC Bulletin 1997-24, "Credit Scoring Models: Examination Guidance"
OCC Bulletin 2010-1, "Interest Rate Risk: Interagency Advisory on Interest Rate Risk Management"
OCC Bulletin 2010-24, "Incentive Compensation: Interagency Guidance on Sound Incentive Compensation Policies"
OCC Bulletin 2011-12, "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management"
OCC Bulletin 2012-5, "Interest Rate Risk Management: FAQs on 2010 Interagency Advisory on Interest Rate Risk Management"
OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"
OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures"
OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles"
OCC Bulletin 2019-62, "Consumer Compliance: Interagency Statement on the Use of Alternative Data in Credit Underwriting"
OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"
OCC Bulletin 2021-19, "Bank Secrecy Act/Anti-Money Laundering: Interagency Statement on Model Risk Management for Bank Systems Supporting BSA/AML Compliance and Request for Information"

Other

Federal Financial Institutions Examination Council's Information Technology Handbook

"Business Continuity Management"
"Development and Acquisition"
"Information Security"

Financial Stability Board

"Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications" (November 2017)