

A background image showing a business meeting. In the foreground, a person's hands are using a pen to point at a tablet displaying a line graph. In the background, another person is working on a laptop. The scene is overlaid with various data visualization elements like pie charts, bar graphs, and network diagrams, all in a blue and white color scheme.

Safety and Soundness: Model Risk Management

OCC MRM Handbook



1| Executive summary

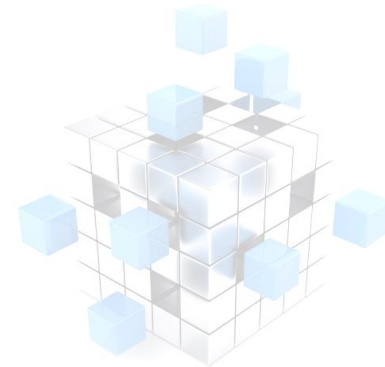
2| Introduction

3| Key take aways for model risk

4| Why Management Solutions

5| Risk Management

6|Annex



List of abbreviations

| Abbreviations | Meaning |
|---------------|---|
| AI | Artificial Intelligence |
| AML | Anti-Money Laundering |
| BSA | Bank Systems Supporting Bank Secrecy Act |
| IRM | Independent Risk Management |
| MRA | Matters Requiring Attention |
| MRM | Model Risk Management |
| OCC | Office of the Comptroller of the Currency |
| OFAC | Office of Foreign Assets Control |

1 | Executive summary

Comptroller's Handbook Content

The OCC MRM booklet guides examiners in performing model risk management examinations, presents concepts and principles of MRM, informs and educates in practices that should be undertaken during an examination and provides information needed to plan examinations and identify deficiencies

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 financial institutions.



A Model is a quantitative method, system or approach that applies statistical, economic and financial, or mathematical theories, techniques and assumptions to process input data into quantitative estimates. It consists of three components:

- **Information input.** Delivers assumptions and data to the model.
- **Processing.** Transforms inputs into estimates.
- **Reporting.** Translates estimates into useful business information

The content of the Handbook is divided into three sections, where the **Risk Management section outlines the key topics of supervision**:

Introduction¹

- Brief overview of models, other quantitative tools, and their usage in banking activities.
- Discussion of risks arising from model use, broken down into eight different types.

Risk Management

- For each step of the model life cycle, the OCC defines typical model risk management (MRM) procedures conducted by examiners and core elements to consider.
- Outlines roles and responsibilities for model developers, users, third parties, auditors, and senior management.
- Specifies distinctions in MRM for AI models, financial crimes models, and vendor models.
- Discussion of the necessary controls and policies that must be established and monitored for effective risk management.

Exam Procedure

- As a follow-up to the previous section, specific lists of questions to consider during each step of the MRM process are defined.
- Procedures include analysis of scope, risk assessment, internal controls, and quality of model risk management.

(1) Overview of models and their used in banking activities is described in [Annex I](#)

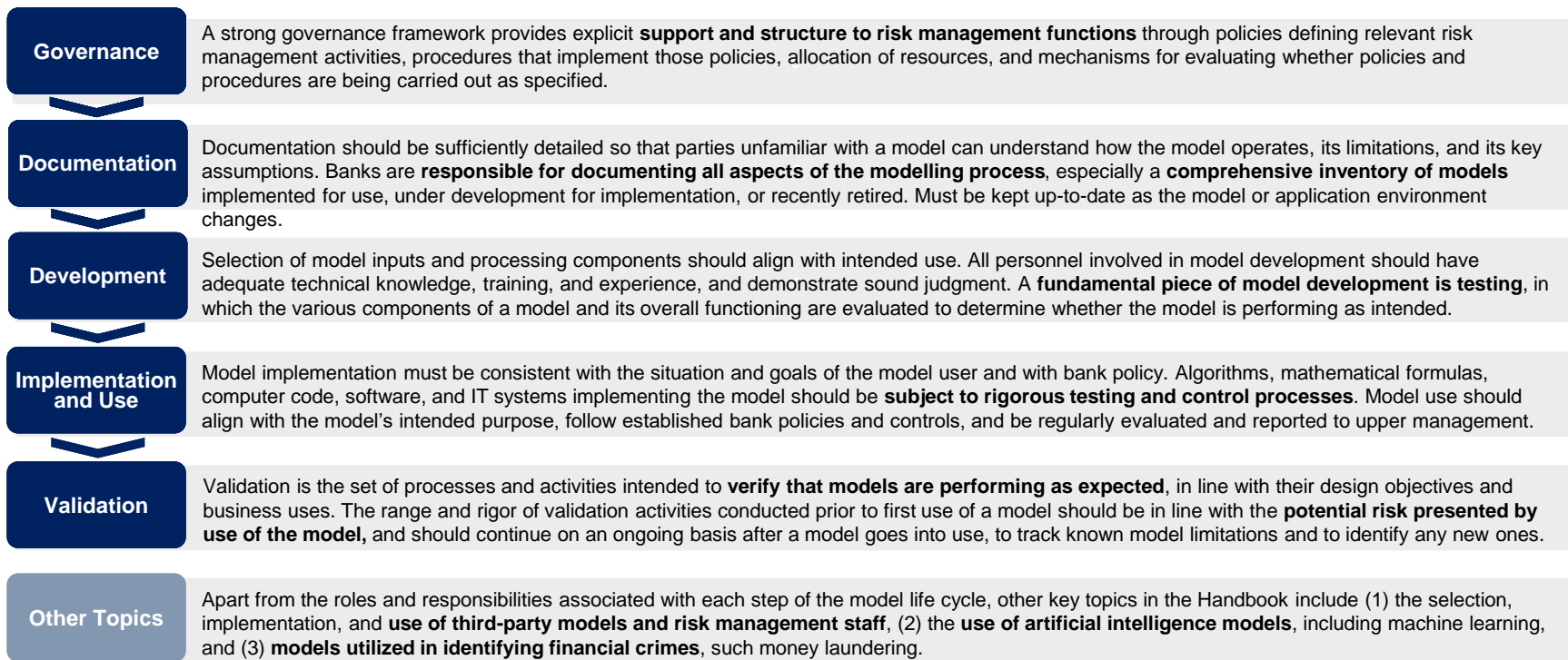


[Access the entire Document](#)

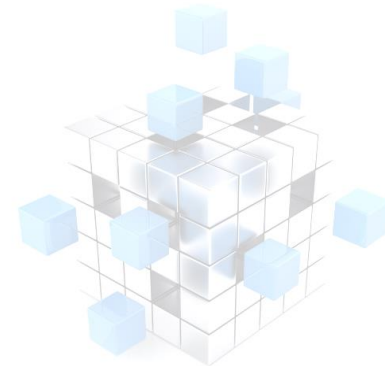
1 Executive summary

Risk management overview

The Risk Management section of the Handbook outlines key roles and responsibilities within the model life cycle, which can be broken down into the following key processes



- 1| Executive summary
- 2| Introduction**
- 3| Key take aways for model risk
- 4| Why Management Solutions
- 5| Risk Management
- 6|Annex



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 because they are based on computational rules and algorithms for which result is certain

The term **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.

- **Quantitative tools that may not meet the definition proposed in the MRM Supervision Guide apply certain rules or algorithms to process information and produce results.**
 - *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.*
 - A tool using a spreadsheet that uses algebraic formulas, such as addition, or values for which the result is certain.
- Such **tools do not rely on sensitivity analysis** or other methods to develop quantitative estimates or predictions.
- A bank's categorization of whether a tool is considered a model should **be based on all relevant information**. Risk management should be based on being commensurate with the scope and complexity of the quantitative tool used.



- On the other hand, the increasing use of the models for banks improves their business decisions, however, they have their costs aligned, not only in terms of resource implementation and model development, but also in terms of confidence in the models, which can lead to incorrect decisions.



- Models can contribute to automation, and therefore their scope and competitiveness continues to increase, highlighting the need for sound model risk management.

2 | Introduction

Model identification (2/2) – The case of AI/ML

Artificial Intelligence (AI) and Machine Learning (ML) may fit the “model” definition outlined in the Federal Reserve’s “Supervisory Guidance on Model Risk Management” (SR 11-7). Regardless their classification, the associated risk management should be commensurate to the risk of the function the AI/ML supports

- **Artificial Intelligence and machine learning.** Artificial Intelligence (AI) is defined in general terms as the application of computer tools to perform tasks that require human analysis through natural language processing, predictive analytics, recommendation engines or image, pattern or voice recognition; while machine learning is a subcategory of AI. These techniques show how new technological and analytical approaches increase the models' complexity.
- Models that use AI operate with **computational tools** to address tasks that traditionally required human analysis.
- These models are not usually quantitative in nature, however they are **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.

AI is used in some bank systems such as:

- fraud detection and prevention,
- marketing and financial marketing analytics,
- chatbots,
- credit underwriting,
- credit risk management and fair lending,
- robo-advice (i.e., an automated digital investment advisory service),
- trading algorithms and robotic process automation,
- cybersecurity,
- Bank Secrecy Act/anti-money laundering (BSA/AML)

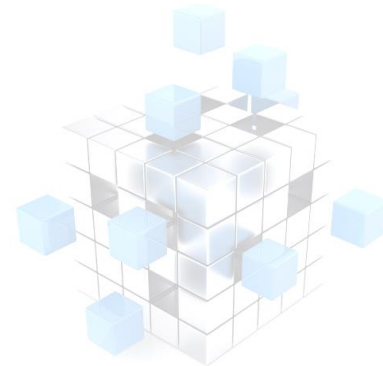
AI models are specifically **highlighted and distinguished** from regular models. Sound AI risk management typically includes:

- 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.
- establishment of clear and defined parameters governing the use of AI.
- effective processes to validate that AI use provides sound, fair, and unbiased results and effective technology controls.

Key considerations

- The rigor of an AI model's risk management should correlate with the **assessed risk** of the process being supported.
- In banks using AI models, examiners should assess if model ratings take **explainability** into account, by which AI decisioning processes and outcomes are reasonably understood by bank personnel.
- While AI models can be exceptionally accurate, the logic behind model decisions can be unclear. If such a model is being used for an important process such as determining credit worthiness, the model users must be able to understand how the model makes decisions.

- 1| Executive summary
- 2| Introduction
- 3| Key take aways for model risk**
- 4| Why Management Solutions
- 5| Risk Management
- 6|Annex



3 | Key take aways for model risk (1/2)

MRM Officers should consider the following takeaways in their strategy ...

1 Effective Challenge

Model Validation and model risk management processes must be conducted with **independence** from model development and use to ensure lack of bias. **Effective challenge** is a critical element during any MRM process.

2 Commensurate to Risk

The rigor of validation before and after implementation should be **commensurate with the potential risk** presented by use of the model, the bank's overall use of models, the complexity and materiality of its models, and the size and complexity of the bank's operations.

3 Quantitative Tools

The determination of **whether a quantitative tool is considered a model is bank-specific**. Risk management for these tools must still be **commensurate** with the associated model risk. Risk management for these tools may be less rigorous than that of models and may focus more on the **implementation and associated technological controls**.

4 Model Inventory

Banks should maintain detailed **documentation of all models in use, results of the modeling and validation processes, and model issues and their resolution**. While each line of business may maintain its own inventory, a specific party (usually, MRM) 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**.

5 Aggregate Risk

Banks should **consider model risk from individual models and in the aggregate**. Aggregate risks arise from **interactions or interdependencies** among models, data, and processes across the bank.

3 | Key take aways for model risk (2/2)

...for the improvement of model risk management

6 Targeted Testing

An effective validation framework should include three core elements with **strong testing procedures**: (1) Evaluation of **conceptual soundness**, including **developmental evidence**, (2) **Ongoing monitoring**, including **process verification** and **benchmarking**, and (3) **Outcomes analysis**, including **back-testing**.

7 Model Overlays

Model validators should have appropriate **technical knowledge** to perform adjustments to model outcome, but model overlays and adjustments **should not be viewed as a solution** that dissuades the bank from making improvements to the model.

8 AI/ML Models

MRM for AI/ML models must also be **commensurate** with the associated model risk, which will be heightened due to model complexity. Banks must maintain effective **technological controls**, documented **use cases**, and focus on **explainability** during model evaluation.

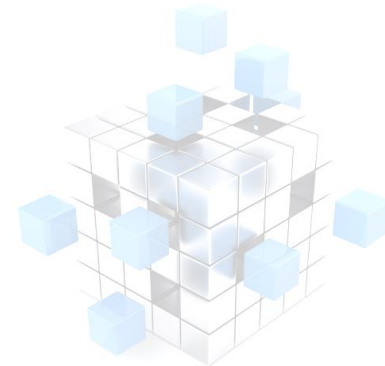
9 Third Party/ Vendor Models

A bank's use of **third parties models** does not diminish the **responsibility of the bank** to ensure that the bank operates in a safe and sound manner and in compliance with applicable laws and regulations. Alternatively, **vendors** are responsible for **providing developmental and testing evidence, instructions for implementation, and ongoing monitoring procedures and analysis**.

10 BSA/AML Models

“**Traditional**” **back-testing is not as effective** in BSA/AML models, but rather ATL/BTL analysis and **alert productivity metrics** such as false positive rate or frequency of alerts escalated. While the OCC seems to suggest treating all BSA/AML models as such, the **SR21-8** letter from the Federal Reserve states that banks may choose to classify BSA/AML models as non-models. Regardless, rigor of MRM must still be **commensurate with associated model risk**.

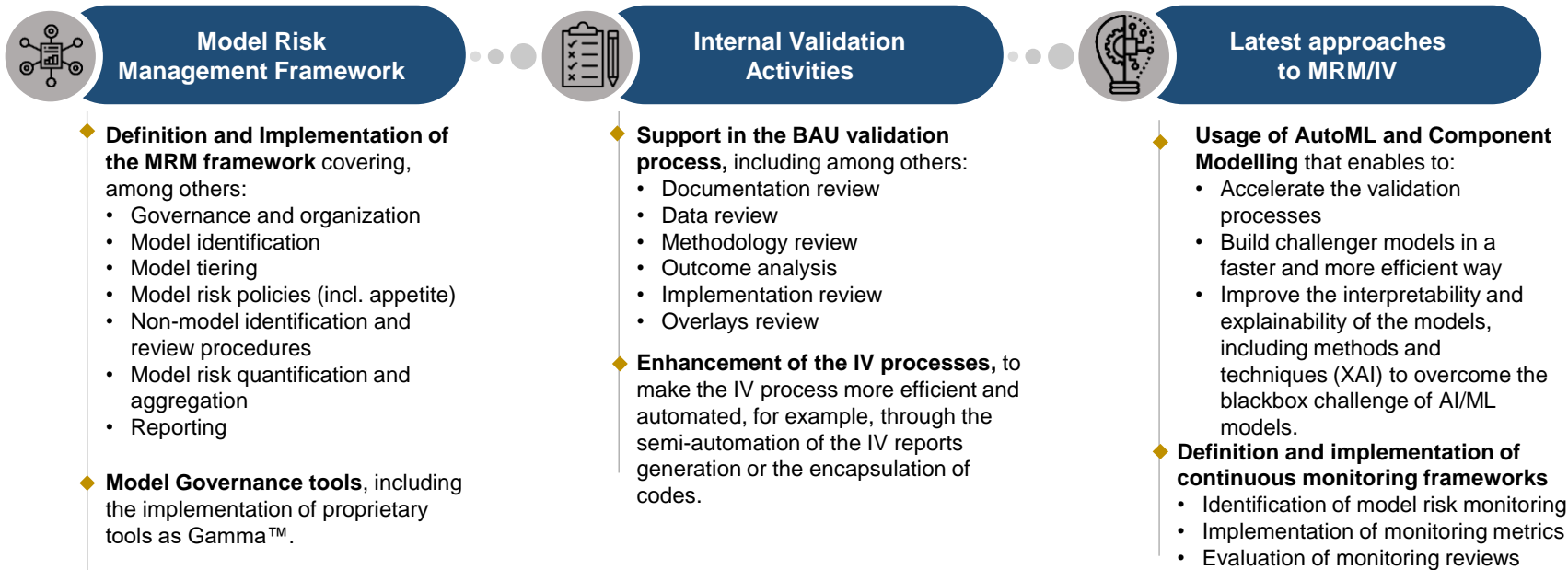
- 1| Executive summary
- 2| Introduction
- 3| Key take aways for model risk
- 4| Why Management Solutions**
- 5| Risk Management
- 6|Annex



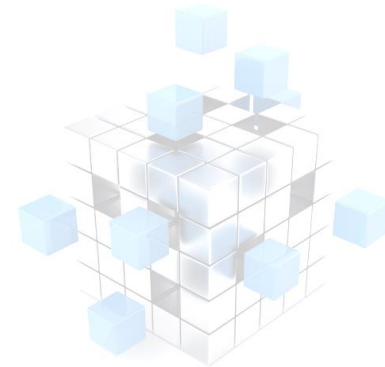
4 | Why Management Solutions

Management Solutions successfully helps strengthen the internal validation and model risk related activities in alignment with the FRB and OCC requirements on model risk management (FRB SR11-7, SR21-8, OCC Handbook)

Management Solutions has ample experience in the implementation of MRM frameworks and the execution of model validation or review activities for all model typologies and non-models (or user tools), including the latest approaches to AI/ML frameworks, third-party models and BSA/AML models. Management Solutions develops and applies specific solutions (policies, procedure, validation frameworks) commensurate to the nature and use of the models by the entity, and the risk associated to them.



- 1| Executive summary
- 2| Introduction
- 3| Key take aways for model risk
- 4| Why Management Solutions
- 5| Risk Management**
- 6|Annex



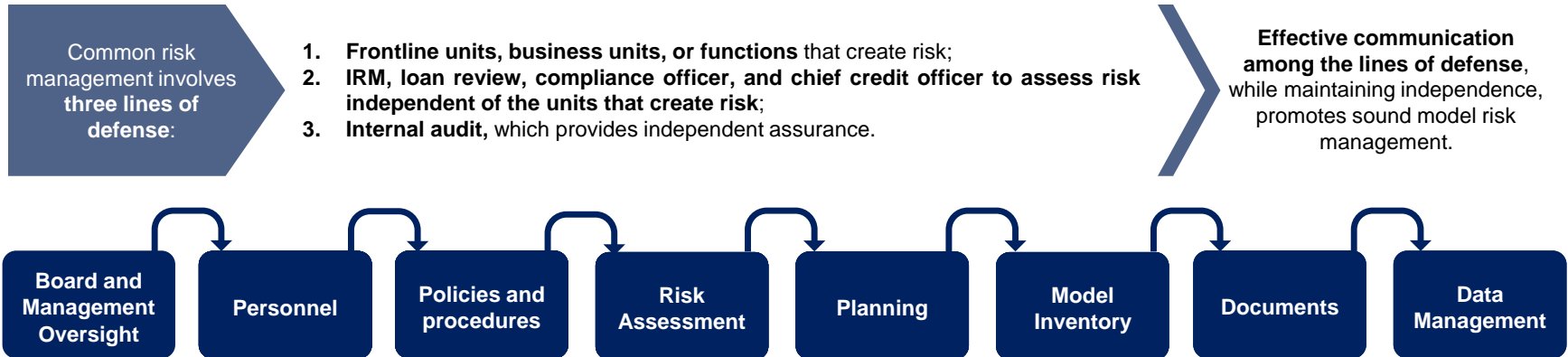
5 Risk Management

Governance (1/4)



Sound model governance includes board and management oversight, policies and procedures, a system of internal controls, internal audit, a model inventory, and documentation.

- A strong governance framework defines risk management functions, resource allocation, and management policy implementation procedures, in particular, **the scope and sophistication of a bank's governance function is expected to be commensurate with the scope and sophistication of the use of models.**
- When models and model outputs have a **material impact on business decisions, a bank's model risk management framework should be more comprehensive and rigorous.**
- For example, decisions related to risk management and capital and liquidity planning, a model failure would have a particularly detrimental impact on a bank's financial condition.



5 Risk Management

Governance (2/4)



Sound model governance includes board and management oversight, policies and procedures, a system of internal controls, internal audit, a model inventory, and documentation

Policies and procedures

Consistent with good business practices and existing supervisory expectations, banks should formalize MRM activities with policies and the procedures to implement them. MRM 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**. Policies and procedures regarding model risk management, which may vary based on the type and objectives of the bank's models, may, **among others**:

- Describe governance and establish internal controls over the MRM process.
- Describe the MRM framework.
- Require detailed documentation of it.
- Include definitions of a model and criteria for when policies should be applied.
- Define acceptable practices for model development.
- Identify roles and responsibilities of stakeholders.
- Describe standards for timely resolution of model issues.
- Establish communication standards for the communication of risk culture, appetite, controls.
- Define expectations for ongoing monitoring of third parties.
- Include standards for data management, such as standards for data proxies.

Risk Assessment

A sound model risk assessment process generally identifies risk both from **individual** models and models in the **aggregate**, and the model's **capabilities and limitations**. Furthermore, it measures the risks **associated** with model activities accurately and in a **timely manner**. 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.

• ***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.***



Sound model governance includes board and management oversight, policies and procedures, a system of internal controls, internal audit, a model inventory, and documentation

Planning

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**. Some key planning considerations include among others:

- 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?

Model Inventory

It is required that 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. 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.
- Model owner and user(s) by title or group.
- Status of model (e.g., in development, production, decommissioned).
- 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.
- Type and source of inputs used by each model and underlying components of each model.

5 Risk Management

Governance (4/4)



Sound model governance includes board and management oversight, policies and procedures, a system of internal controls, internal audit, a model inventory, and documentation

Documentation

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**. 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, etc.

When a bank uses models that have been done by third parties, the problem arises as to the scope of the model, which is usually narrower than those done internally, so examiners must **determine whether the documentation is sufficient for bank management to properly use and validate the model**.

Data Management

- The data and other information used to develop a model are of critical importance; there should be: i) rigorous assessment of **data quality**, ii) relevance appropriate documentation, iii) it must be **suitable for the model** and that they are consistent with the theory.
- **If data substitutes are used**, they must be carefully identified. Also, if the information is not representative of the bank's portfolio or other characteristics, these factors should be properly tracked and analyzed so that users are aware of the **potential limitations** to the model.
- Analysis of the completeness and applicability of internal and external information **should be performed periodically** to determine if revisions or updates are necessary.



5 Risk Management

Model Development and implementation

MRM 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. The two integral parts of model development are testing and ongoing development

Testing

Testing analyzes **particular components** to check if the model is **performing as intended**.

- **Model accuracy** is studied to determine if the model is robust and stable, which potential limitations could exist and the model's behavior over a range of input values.
- The model should 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**. These include scenarios outside the ordinary expectations and should encompass the range of products and applications for which the model is intended.
- **Extreme values** should be considered to **limit test** the model and determine the boundaries of its effectiveness.
- **The impact** of model results **on other models** should be tested.

Ongoing development

- **Regularly adjustments to account for new data and techniques** or because there has been a deterioration in performance that should be fixed.
- **Parallel outcomes analysis**. Make comparisons between original and adjusted models through a forecast test against realized outcomes. If the adjusted model does not outperform the original, developers should introduce changes or redesign the entire model.



5 Risk Management

Model Use (1/2)



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. Model users can provide valuable business insight during the development process

Opportunities

- Additional opportunity to test whether a model is functioning effectively and to assess its performance over time as conditions and model applications change.
- **Assess if the model is performing effectively** 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 and business managers affected by model outcomes **may question methods or assumptions** underlying models.

Threats

- 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.
- **These challenges may be asymmetric**, users are less likely to challenge an outcome if the results are advantageous to them. Users may incorrectly believe that model risk is low simply because outcomes from model-based decisions appear favorable to the institution.



5 Risk Management

Model Use (2/2)



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. Model users can provide valuable business insight during the development process

Model overlays and adjustments

- **Overlays** 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
- **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 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. Any model overlays or adjustments conducted by the model users must be **well-documented and supported** by sufficient evidence.
- 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.

Reporting

- 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
 - status of model issues.
- Model risk management reports may include measures on:
 - underperforming models.
 - the volume of models considered high risk.
 - models with past-due validations.
 - models with temporary exemptions or provisional approvals.
 - models in use without validation and model development.



5 Risk Management

Model Validation (1/2)



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. It should include three core elements: i) evaluation of conceptual soundness, ii) ongoing monitoring and iii) outcomes analysis

- Model validation is the set of processes and activities intended to **ensure that models are sound, in line with their design objectives** and business uses.
- It also identifies potential **limitations and assumptions** and assesses their possible impact.
- 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.
- 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.



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.



Independence: 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.

- Independent validation may be performed in-house, by a third party, or a combination thereof (Third-Party Risk Management).
- 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.
- Staff doing validation should have high level of technical expertise because of the complexity of many models, both in structure and in application.



5 Risk Management

Model Validation (2/2)

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. It should include three core elements: i) evaluation of conceptual soundness, ii) ongoing monitoring and iii) outcomes analysis

Evaluation on Conceptual Soundness

- 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.
- **Transparency and explainability** are key considerations that are typically evaluated as part of effective risk management regarding the use of complex models.
- By **changing the input data**, the user can test the results of these on the output results to assess a model's limitations.

Ongoing Monitoring

Process Verification:

All model components must be checked to be functioning as intended. All data inputs are verified, and the model behaves as expected. Examiners should determine if bank management has conducted process verification

Benchmarking:

Model output must be compared against estimates from an alternative internal or external source, and all discrepancies should trigger an investigation.

Outcome analysis

- 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.
- Outcome analysis should involve a **range of tests** because any individual test will have weaknesses, and attention should be paid to choosing the appropriate type of outcomes analysis for a particular model.
- The nature of outcome analysis requires **expert judgment** and will depend on the model's methodology, its complexity, data availability, and the magnitude of potential model risk to the bank.



Back-testing is a recommended approach, where model performance over a period is compared against the model performance observed over the same time horizon on an earlier sample of data. However, back-testing is **not always the most effective** choice for all model types. It may not be possible for many **BSA/AML models**. Evaluation on how bank management incorporates back-testing results into the modeling process is necessary.

5 Risk Management

Third-party risk management

Banks may benefit from third-party relationships by gaining operational efficiencies or improving the banks' competitive edge. 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 and Data

If a bank is utilizing third-party models and data, the **following information must be ascertained prior to use**:

- Information on the **model's development, assumptions, limitations, and intended use**.
- Intended **data inputs**, parameters, and implementation instructions.
- **Detailed testing results** and procedures for conducting validation.

Bank management should understand and evaluate the **results of validation and risk control activities** that are conducted by third parties:

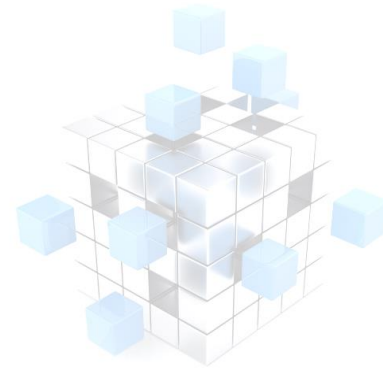
- The banks should have a **complete knowledge** of how the model works and its applications, to conduct a proper evaluation.
- **Risk-based review**. Internal report that assesses if the model works correctly and if the existing validation activities are sufficient.
- Banks should expect **the third party to conduct ongoing** performance monitoring and outcomes analysis of the model, disclose results to the bank.

Engaging Third Parties for Model Risk Management Activities

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**.



- 1| Executive summary
- 2| Introduction
- 3| Key take aways for model risk
- 4| Why Management Solutions
- 5| Risk Management
- 6|Annex



6 Annex I

Risk types (1/3)

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**. Conceptually, model risk is a distinct risk that can **influence aggregate risk** across all risk categories and 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. 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**. 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. 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 and assumptions underlying a model.



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.
- ✓ **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.



6 Annex I

Risk types (2/3)

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.

| | |
|-------------------------|---|
| Strategic risk | <p>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.</p> <ul style="list-style-type: none">➤ 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. |
| Operational risk | <p>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.</p> <ul style="list-style-type: none">➤ 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 and adjustments when model limitations become apparent.➤ 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. |
| Reputation risk | <p>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.</p> <ul style="list-style-type: none">➤ 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. |
| Compliance risk | <p>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.</p> <ul style="list-style-type: none">➤ A bank's compliance risk can increase when models used in the bank's BSA/AML and OFAC programs, inaccurately reflect the risk of a bank's business model, products, services, customer base, and geographic footprint |



6 | Annex I

Risk types (3/3)

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.

| | |
|---------------------------|--|
| Credit risk | <p>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. It exists any time bank funds are extended, committed, invested, or exposed through actual or implied contractual agreements, reflected or not in the balance sheet.</p> <ul style="list-style-type: none">➤ 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. |
| Liquidity risk | <p>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.</p> <ul style="list-style-type: none">➤ Management's failure to adjust model inputs based on changes in market conditions can increase liquidity risk. |
| Interest rate risk | <p>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:</p> <ol style="list-style-type: none">1) the sensitivity of an instrument's expected income/expense and economic value to a given change in market rates, and2) 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 |
| Price risk | <p>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.</p> |



6 | Annex II

Examination Procedures - Scope

This booklet contains expanded procedures for examining specialized activities or specific products or services that warrant extra attention. These procedures are designed to help examiners tailor the examination to each bank and determine the scope of the model risk management examination

- These procedures are designed to help examiners **tailor the examination to each bank** and determine the **scope of the model risk management examination**. The 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.

Objective

- **Review of** the supervisory strategy; the examination scope memorandum, previous 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 issues related to MRM.
- **Obtain and review** policies, procedures, board and committee meeting minutes, and reports bank management uses to supervise the use of models.
- **Consideration of 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.
- Determine the scope and objectives of the MRM examination. Through discussion with the supervisory office and Economics Department, determine if coordination with RAD is warranted.
- Selection of the necessary steps to meet examination objectives and the supervisory strategy from the examination procedures.



6 Annex II

Examination Procedures - Quantity of risk (1/4)

This booklet contains expanded procedures for examining specialized activities or specific products or services that warrant extra attention. These procedures are designed to help examiners tailor the examination to each bank and determine the scope of the model risk management examination

| | |
|------------------|---|
| Objective | <ul style="list-style-type: none"> • 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 MRM. • 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. |
|------------------|---|

| Strategic risk | Operational risk | Compliance risk | Credit risk |
|---|---|--|--|
| <ul style="list-style-type: none"> • The nature, extent, and complexity of models the bank uses and contribution to strategic decision making. • Strategic objectives that depend on the use of models. • Governance framework for developing, implementing, using, and validating models. • Models evolution to keep pace with changes in strategy. • Adjustment of model inputs and assumptions. • Accuracy of model outputs and the adjustments applied to them. | <ul style="list-style-type: none"> • The nature, extent, and complexity of models the bank uses and the bank’s reliance on third parties. • Operational losses resulting from modeling weaknesses. • Level of uncertainty or inaccuracy of model inputs and assumptions. • Frequency of ongoing monitoring. • Models contribution to decision making. • The nature and extent of operational breakdowns related to model use. | <ul style="list-style-type: none"> • The nature, extent, and complexity of models used in the bank’s CMS. • Consumer protection-related issues raised from models. • Level of uncertainty or inaccuracy of model inputs and assumptions. • Frequency of the ongoing monitoring of the bank’s models. • Models contribution to compliance-related decision making. • Models contribution to regulatory reporting. | <ul style="list-style-type: none"> • The nature, extent, and complexity of models used for lending, credit administration, risk management, or estimating credit losses or regulatory capital. • Level of uncertainty or inaccuracy of model inputs and assumptions. • Accuracy of model assumptions and the relevance of data used. • Level of uncertainty of model outputs and the significance of overlays and adjustments. • Models contribution to credit-related decision making. |



6 Annex II

Examination Procedures - Quantity of risk (2/4)

This booklet contains expanded procedures for examining specialized activities or specific products or services that warrant extra attention. These procedures are designed to help examiners tailor the examination to each bank and determine the scope of the model risk management examination

| | |
|------------------|---|
| Objective | <ul style="list-style-type: none"> • 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 MRM. • 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. |
|------------------|---|

| Liquidity risk | Interest rate risk | Price risk | Reputation risk |
|--|--|--|--|
| <ul style="list-style-type: none"> • The nature, extent, and complexity of models used for liquidity risk management. • Level of uncertainty or inaccuracy of model inputs and assumptions, including behavioral and contingent funding assumptions. • Reasonableness of the magnitude of liquidity stress scenarios and their impact on outputs. • If stress scenarios consider all relevant legal constraints. • Models contribution to liquidity risk-related decision making. | <ul style="list-style-type: none"> • The nature, extent, complexity, and technologies of models the bank uses for interest rate risk management. • Level of uncertainty or inaccuracy of interest rate measurement model inputs and assumptions. • Reasonableness of the magnitude of stress scenarios and their impact on outputs. • Models contribution to interest rate risk-related decision making. | <ul style="list-style-type: none"> • The nature, extent, and complexity of models the bank uses. • Accuracy of the model’s estimate of financial instruments’ prices. • Volume of trading instruments with prices hard to model. • Level of uncertainty or inaccuracy of model inputs and assumptions. • Models contribution to price risk-related decision making. | <ul style="list-style-type: none"> • The nature, extent, and complexity of models the bank uses. • Level of uncertainty or inaccuracy of model inputs and assumptions. • Models contribution to reputation risk-related decision making. • The extent of compliance issues related to model use. • The adequacy of policies and processes. • Adequacy of internal controls over data, including internal controls in place to prevent biased outcomes. |



6

Annex II

Examination Procedures - Quality of Model Risk Management (3/4)

The conclusion on risk management considers all risks associated with a bank's model use. The conclusion on risk management takes into account all risks associated with the bank's use of models. It is structured in policies, processes, personnel and control systems that impose order on a bank's pursuit of its objectives

| Policies | Processes | Personnel | Control Systems |
|---|---|--|---|
| <p>Objective 1: to determine whether the board has adopted consistent policies for model risk management.</p> <ul style="list-style-type: none"> Nine-step procedure for assessing if appropriate MRM policies are established . Necessary areas of policy, topics that must be addressed, appropriate guidance and governance. | <p>Objective 1: to determine the adequacy of management's planning over use of models.</p> <p>Objective 2: Determine the adequacy of the bank's model risk assessment processes</p> <p>Objective 3: Determine the adequacy of management's maintenance of comprehensive set of information.</p> <p>Objective 4: Various procedures for assessing model development.</p> <p>Objective 5: Determine the adequacy of model risk management reports.</p> <p>Objective 6: Various procedures for assessing the validation process.</p> | <p>Objective 1: to determine the adequacy of board oversight and senior management's implementation of model risk management.</p> <ul style="list-style-type: none"> Board and Management oversight MRM personnel <p>Objective 2: determine the adequacy of model risk management personnel in executing their responsibilities.</p> | <p>Objective 1: to determine whether control systems support effective model risk management.</p> <p>Objective 2: To determine the adequacy of IRM's (i.e., control staff) oversight of model risk management.</p> <p>Objective 3: To determine the adequacy of internal audit of model risk management.</p> <p>Objective 4: To determine the adequacy of management's actions in response to findings identified by IRM, validation activities, and audit reviews.</p> |

6

Annex II

Examination Procedures - Quality of Model Risk Management (4/4)

To determine, document, and communicate overall findings and conclusions regarding the examination of model risk management, it is necessary to:

- 1 Determine preliminary examination findings and conclusions** and discuss with the EIC, including: i) Quantity of associated risks (as noted in the “Introduction” section); ii) Quality of risk management; iii) Violations and deficient practices.
- 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.**
- 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.
- Compose conclusion comments**, highlighting any issues that should be included in the report of examination or supervisory letter. If necessary, compose MRA and violation write-ups.
- Update the OCC’s supervisory information systems** and any applicable report of examination schedules or tables.
- 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).
- Update, organize, and reference work papers** in accordance with OCC policy.
- Appropriately **dispose of or secure any paper or electronic media** that contain **sensitive bank** or **customer information**.

