IPPF

International Professional Practices Framework

Supplemental Guidance

Practice Guide

FINANCIAL SERVICES

Auditing Model Risk Management

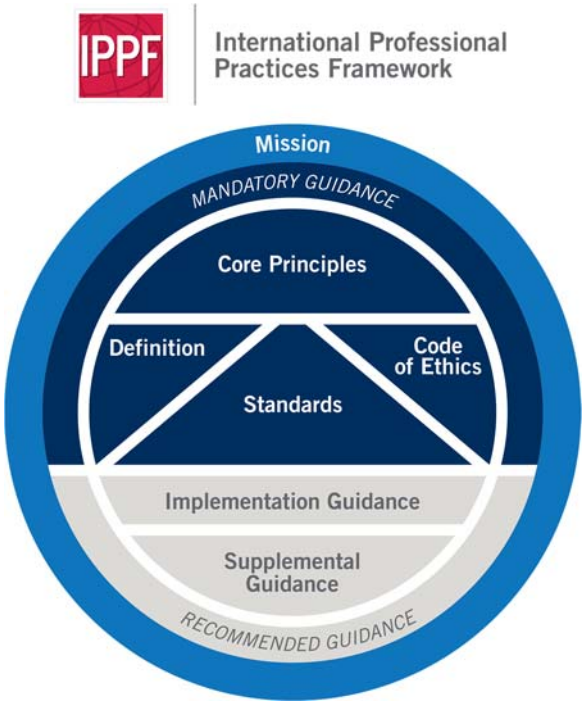
The Institute of Internal Auditors | Global

About the IPPF

The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA. A trustworthy, global, guidance-setting body, The IIA provides internal audit professionals worldwide with authoritative guidance organized in the IPPF as Mandatory Guidance and Recommended Guidance.

Mandatory Guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are:

- Core Principles for the Professional Practice of Internal Auditing.
- Definition of Internal Auditing.
- Code of Ethics.
- *International Standards for the Professional Practice of Internal Auditing*.



About Supplemental Guidance

Supplemental Guidance is part of the IPPF and provides additional recommended, nonmandatory guidance for conducting internal audit activities. While supporting the *Standards*, Supplemental Guidance is intended to address topical areas, as well as sector-specific issues, in greater procedural detail than the *Standards* or Implementation Guides. Supplemental Guidance is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides are a type of Supplemental Guidance that provide detailed step-by-step approaches, featuring processes, procedures, tools, and programs, as well as examples of deliverables.

Practice Guides are intended to support internal auditors. Practice Guides are also available to support:

- Financial Services.
- Public Sector.
- Information Technology (GTAG®).

For an overview of authoritative guidance materials provided by The IIA, please visit www.globaliia.org/standards-guidance.

Table of Contents

Executive Summary

Banks[1] and other large financial services organizations rely extensively on mathematical models to make business decisions and meet regulatory requirements. Models are inherently risky because they apply statistical, economic, financial, or mathematical theories, which require the use of assumptions based on judgment, to yield estimates of real-world financial events. This process can lead to imprecise or inaccurate results. Additionally, errors can be introduced throughout the life cycle of the **model** from errors in input data to incorrect calculations and inappropriate application of the model and its results.

The growing dependence of organizations on quantitative analytical models has brought increased regulatory attention to effective **model risk management** (MRM). As regulatory scrutiny around model risk management increases, the internal audit activity plays a key role in assessing an organization's MRM framework.

This guidance provides an overview of the internal audit activity's responsibilities related to MRM and describes methods and processes internal auditors can use to review the design, implementation, and operation of their organization's MRM framework.

[1] For the purpose of this Practice Guide, the term "bank" refers to banks, bank holding companies, or other companies considered by banking supervisors to be the parent of a banking group under applicable national law as determined to be appropriate by the entity's national supervisor. The term "organizations" is used throughout the guide to refer to banks and other large financial services organizations, such as insurance companies.

Introduction

Model risk management has been incorporated into financial services regulations promulgated by supervisory bodies throughout the world. Enhanced capital, liquidity, and leverage rules aim to mitigate the negative effects that inadequately capitalized organizations may have on the economy. In response, organizations across the financial services industry have adjusted and continue to adjust their operations to conform to such regulations.

Note: Terms in bold are defined in the glossary in Appendix B. This guidance contains a variety of technical terms common in the financial services industry. If a definition does not appear in the glossary, please consult the references and additional reading sources appearing in Appendix F.

Because model output affects, and sometimes even determines, certain decisions of senior management, model errors may expose an organization to significant risk. Additionally, models are growing in importance, complexity, and variety. As a result, organizations depend on systems of internal control to prevent, detect, and correct model errors. The internal audit activity plays a key role in assuring senior management and the board that the internal control system contained within the MRM framework is operating at optimal levels throughout the risk modeling processes and that the results are interpreted accurately throughout the organization.

Business Significance: Key Risks

Model risk is defined as "the potential for adverse consequences from decisions based on incorrect or misused model outputs or reports."[2] Model risk occurs for two primary reasons: (1) fundamental errors in model data, rationale, hypothesis, and methodologies may produce inaccurate outputs when viewed against the design objective and intended business uses, and/or (2) the model or its results may be used incorrectly or inappropriately. Further, **aggregate model risk** refers to interrelated risk among models caused by shared inputs and/or assumptions or one model's output being another model's input.[3]

The Internal Audit Activity's Role in Model Risk Management

To assess an organization's compliance, internal auditors must have a sound understanding of the legislation relevant to their organization and jurisdictions within which it operates. Internal auditors

[2] Board of Governors of the Federal Reserve System (FRS), *Supervisory Guidance on Model Risk Management*. SR 11-7, (Washington, D.C.: FRS, 2011), 4, https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm.

[3] Ibid.

are also responsible for understanding the organization's model methodologies well enough to assess model design and operation.

Internal audit's role in the MRM process is to assess the effectiveness of the MRM framework, including the governance, policies, procedures, and activities conducted to address the risk of model error. Internal auditors are also responsible for understanding how the model output is used and if it is appropriate to the model's stated purpose. In addition, internal auditors should provide insight on the design and operating effectiveness of MRM activities to aid management, the board, and other key stakeholders in the commission of their duties, and to confirm that the organization is abiding by direction from regulators.

Internal auditors are not accountable for performing or repeating any model risk activities. To fulfill their responsibilities, internal auditors should be independent, possess relevant skills, report their findings directly to the board, and appropriately consider MRM when developing and executing the engagement plan.

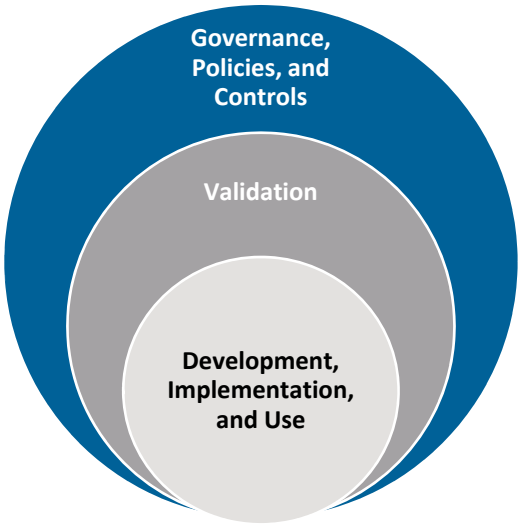
Model Risk Management Process

The MRM process may be divided into three areas of activity:

- Governance, policies, and controls.
- Development, implementation, and use.
- Initial and ongoing validation.[4]

The areas of activity are fluid and should not be viewed as having defined starting and ending points. Figure 1 depicts the relationship of each area.

Figure 1: Model Risk Management Process



[4] Board of Governors of the Federal Reserve System, *Supervisory Guidance on Model Risk Management*, 3-9.

Model Governance, Policies, and Controls

Effective governance, policies, procedures, and controls are essential components of a successful MRM framework. Without proper oversight and guidelines, it is difficult to ensure that the model development, implementation, validation, and use processes are operating as intended. Ultimately, the board is responsible for oversight of the MRM framework. However, the development and detailed execution is delegated to senior management.

Organizations should formally document policies and procedures related to the MRM process. These policies and procedures are typically drafted by senior management and approved by the board and should meet the following criteria:

- Cover the entire MRM process.
- Be written in a detailed manner to reduce the need for interpretation and increase uniform execution throughout the organization.
- Establish documentation standards for all key activities in the three model risk management areas of activity.
- Define MRM roles and responsibilities across the organization.
- Define the model risk assessment framework and process.
- Establish control standards for models.
- Require the creation and maintenance of an organizationwide model inventory.

For certain models, an organization may choose to outsource these activities; for example, when the internal resources required to support development and/or validation are not available. In these cases, management should establish guidelines for incorporating external resources and purchased products (e.g., models, data, parameters, values) into the overall MRM framework.

Management should establish the roles and responsibilities of each party involved with the MRM process. Management may document these roles and responsibilities by creating a chart for insertion into the MRM policies and procedures document. At a minimum, it should include each level of employee involved with the process, their assigned deliverables, and any required reviews or approvals. As a best practice, organizations can use the Three Lines of Defense[5] model to build out the roles and responsibilities. Internal auditors may assist management in this task by sharing the related areas documented in their assurance map if one exists.

For more information on developing an assurance map please see IIA Practice Guide "Coordination and Reliance: Developing an Assurance Map."

[5] The Institute of Internal Auditors. IIA Position Paper: *The Three Lines of Defense in Effective Risk Management and Control* (Altamonte Springs: The Institute of Internal Auditors, 2013).

The Three Lines of Defense model is a best-practice framework organizations may use to structure business processes. The model helps management establish clear roles and responsibilities and internal auditors can use the model to identify gaps or duplication in risk coverage, to identify sources of information needed to plan engagements, and to help develop or enhance an organization's current MRM framework.

The first line of defense is operational management. In the context of MRM, it includes heads of business or functional area and model users, owners, and developers. These roles are primarily accountable for ensuring organizations identify, rate, and mitigate model risks. In addition, the first line is responsible for the foundation of the MRM process; the development of models; the implementation, execution, and oversight of model controls; and maintenance of model documentation.

The second line of defense comprises other business oversight functions such as risk management and compliance. Large organizations typically have designated model risk units within their risk management or compliance departments. This line of defense may also include various board and management risk committees. The second line of defense is responsible for:

- Overseeing, advising, and assisting the first line of defense.
- Supporting the mitigation of overall model risk through aggregation and analysis of model information across business areas.
- Performing the initial validation as well as ongoing monitoring and validation and ensuring any identified issues are addressed.
- Reporting model risk information to senior management, the board, and appropriate oversight groups.

The internal audit activity is the third line of defense, providing the board and senior management with comprehensive assurance based on the highest level of independence and objectivity within the organization. In the context of MRM, internal auditors review the sufficiency of the MRM framework (governance, policies, procedures, and controls) and provide an opinion on the overall process. The internal audit activity is independent from the other lines of defense and reports its results directly to the board or its delegates.

Model Development, Implementation, and Use

When a gap or deficiency in an organization's model portfolio is identified, management must decide to either build or purchase a new model. Management should formally document the intended purpose of the new model and its decision to build or buy. If management decides to build the model, it should assign knowledgeable and experienced developers to the project. In

addition to building the model, developers must select appropriate data inputs to ensure that the quality of the resultant data is high.[6]

There are numerous types of data developers may use:

- The most basic type is raw data derived directly from the source and not manipulated in any way.
- If there are breaks in the raw data, developers may fill them with artificial data sets called expansion data. This data is created by duplicating or applying simple rules to existing data sets in an effort to approximate the missing data.
- In the event no data is available, the developer must use proxy data, which is a highly correlated data set used to approximate unobservable or immeasurable data. For example, the gross national product commonly serves as proxy data for a country's economic condition.
- Finally, developers may obtain data from other models. This is called sub-model data and refers to the output of a model being used as the input for another model.

Once the developers have built the model and determined the data sets, they must test the model's functionality to ensure it is performing as expected. Thorough testing will cover a variety of scenarios, including extreme situations also referred to as stress testing. If the model does not function as intended under these extreme situations, it may be necessary to place limitations on the model and restrict its use. Organizations should formally document all limitations. After the model has been tested by developers, business users should have an opportunity to sample or test the model and provide feedback.

For more information on stress testing in organizations, please see IIA Practice Guide "Auditing Capital Adequacy and Stress Testing in Organizations."

Once the developers and the business users are satisfied with the model's functionality, it can be moved into the initial validation phase, which involves testing by independent parties from inside or outside the organization. If the model fails initial validation testing, it must go back through the development process. If the model passes validation, it should enter the implementation phase for production according to the organization's information technology guidelines. Once this has been completed, the model is available for the organization to use.

Throughout the model's life, the business is responsible for maintaining appropriate processes and controls to limit model risk and support accurate results aligned with the model's intended use. These include, for example, sufficiently documenting the model's purpose, methodology, assumptions, and limitations. Depending on the nature of the business and **materiality** of the model

[6] Board of Governors of the FRS, *Supervisory Guidance on Model Risk Management*, 5-6.

to business operations, it may also be helpful to document deviations from industry standards and the reason behind the differences.

The business is also responsible for promptly reporting any issues with model performance to the appropriate level of management. Further, given the importance of the models' outputs that management will use in their decision-making processes and in carrying out their other responsibilities, models with material significance should be subject to ongoing validation.

Validation

Validation is the process of verifying whether a model is functioning as intended. Typically performed by an independent party, validation is separate from the testing performed by the developers and business users. However, there may be instances where it is impractical to use a third party to validate (i.e., due to the size and/or nature of the business) and the developers or business users must execute the validation testing. In this situation, an independent party, such as the internal audit activity, should review the testing results to support the accuracy of the validation.

The parties involved in the validation process should be able to effectively challenge the model. The exact definition of effective challenge may vary depending on the expectations of an organization's regulators and other stakeholders. The Federal Reserve Board (FRB) and Office of the Comptroller of the Currency (OCC) provide a general definition of effective challenge as "critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate changes."[7] To effectively challenge a model, a person should be competent and influential, and free from incentives. Specifically, a validator should satisfy the following qualifications:

- Have no involvement in the development process nor any financial considerations tied to the model (e.g., raises, bonuses, promotions, performance evaluations).
- Possess in-depth knowledge about the model itself and about the line(s) of business using it.
- Hold an appropriate level of authority to ensure corrective actions are taken to address any model errors identified during the validation process.

According to the International Association of Insurance Supervisors' Standard No. 2.2.7, before models purposed for regulatory capital are placed in use, three tests must be performed. These three tests are a good starting point for any model validation program:

1. A statistical quality test assesses the base quantitative methodology of the internal model. As part of this test process, the model user should be able to demonstrate the

[7] Board of Governors of the Federal Reserve System, *Supervisory Guidance on Model Risk Management*, 4.

appropriateness of the methodology, including the choice of model inputs and parameters, and should be able to justify the assumptions underlying the model.

2. A calibration test demonstrates that the regulatory capital requirement determined by the internal model satisfies the modeling criteria specified by the supervisor.
3. A use test confirms that the internal model and its methodologies and results are fully embedded into the risk strategy and operational processes of the model user. The standard also iterates that the board and senior management should have the overall responsibility to ensure that adequate governance and controls are in place related to the construction and use of internal models.[8]

Monitoring and Revalidation

Initial model validation normally occurs before a model is made available for use, and ongoing monitoring and validation continue throughout the life of the model. Where an organization relies on numerous models, management may use a model risk assessment to determine the frequency with which monitoring and revalidation should be performed.

A model risk assessment involves:

- Identifying key risk factors associated with each model. Risk factors include the level of model complexity, the criticality of model output, the nature of model calculations (manual versus automated), etc.
- Assessing the **inherent risk** of each model based on the identified factors.
- Determining whether the model monitoring and ongoing validation activities align in frequency (schedule) and nature with the inherent risk of each model.
- Assessing whether the frequency of model monitoring and ongoing validation aligns with the overall **risk appetite** of the organization.

Model validators should monitor models of material significance regularly to assess high-level functionality and determine whether the historic validation activities remain sufficient. If the model is not functioning properly, it should be adjusted and revalidated. If the model is functioning properly but the historic validation activities are deemed insufficient by regulators or some other relevant party, validators should perform a full or partial revalidation as appropriate.

Organizations should avoid long periods of time without revalidating models of material significance. Some regulatory bodies and other key stakeholders may expect ongoing validation to occur at certain

[8] Solvency and Actuarial Issues Subcommittee, "Standard No. 2.2.7: IAIS Standard on the Use of Internal Models for Regulatory Purposes," (Basel: International Association of Insurance Supervisors, 2008), 5, https://www.iaisweb.org/file/34143/16-standard-no-227-on-the-use-of-internal-models-for-regulatory-capital-purposes.

intervals. For example, the FRB and OCC recommend that models of material significance be fully revalidated on a routine basis, regardless of the results of regular monitoring activities.[9]

Auditing Model Risk Management

Planning the Engagement

IIA Standard 2200 – Engagement Planning
IIA Standard 2201 – Planning Considerations

In planning an assessment of an organization's MRM framework, internal auditors must identify the policies, processes, and tools used to control the risks and manage the environment related to models. Then, internal auditors must determine if the MRM framework is included as part of a unified and cohesive, organizationwide governance structure.

For more information please see IIA Practice Guide "Engagement Planning: Establishing Objectives and Scope."

Engagement planning generally includes these steps:

- Understand the context and purpose of the engagement.
- Gather information to understand the area or process under review.
- Conduct a preliminary risk assessment.
- Form engagement objectives.
- Establish engagement scope.
- Allocate resources.
- Document the plan.

The following sections of this guide will help the internal auditor through the process of planning and executing an assessment of the organization's MRM framework.

Understand the context and purpose of the engagement

IIA Standard 2201 – Planning Considerations

In planning the audit engagement, internal auditors should consider the following elements:

- Models used by the organization.
- Size and sophistication of the organization and its MRM framework.
- MRM regulatory requirements/expectations relevant to the organization and the jurisdictions within which it operates.
- Robustness of MRM roles, responsibilities, and activities across the organization.

[9] Ibid.

- Results of model monitoring and validation activities and any other model oversight activities undertaken across the organization.

While developing the individual engagement plan, internal auditors gather information through procedures such as reviewing prior assessments (e.g., risk assessments, reports by assurance and consulting service providers), understanding and mapping of process flows and controls, and interviewing relevant stakeholders. Because MRM is an organizationwide activity, newly acquired information may affect the engagement objectives, scope, work program, and methods of analysis. Thus, the information acquired throughout planning should be well documented, promptly updated, and taken into account throughout the engagement. The information may also be useful in the CAE's long-range planning for future engagements.

Gather information to understand the area or process under review

IIA Standard 2201 – Planning Considerations

Once internal auditors have identified the departments, functions, and roles in the organization that are relevant to MRM, they should gather relevant documentation to support the preliminary risk assessment. The following elements can help identify the risks facing the organization and the strategies used to manage those risks in terms of the MRM framework:

- Charters, policies, and other mandate information for the governance entities responsible for establishing the MRM framework.
- MRM policies, guidelines, and standards.
- Management's model risk and control assessment.
- The organization's model inventory and model risk assessment process and results.
- Any documents or personnel that can assist in understanding the types of models used.
- Documentation of all phases of the model development and validation processes.
- Model validation reports.
- Results of modeling for credit, market, liquidity, capital, financial reporting, and operational purposes.
- Documentation of the process for designing and running normal and stress scenarios.
- Reports containing the results of stress testing.
- Results of prior regulatory examinations of the MRM framework and the individual models used in the organization.

Conduct a preliminary risk assessment

IIA Standard 2210.A1 – Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review.

Because any single internal audit engagement cannot cover every risk, internal auditors assess the significance of the risks identified by management, validators, regulators, and during previous internal audit engagements. Three primary sources contribute to model risk:

1. Fundamental errors may produce inaccurate outputs when viewed against the design objective and intended business uses.
2. Incorrect or inappropriate use.
3. Inaccurate or corrupted input data.

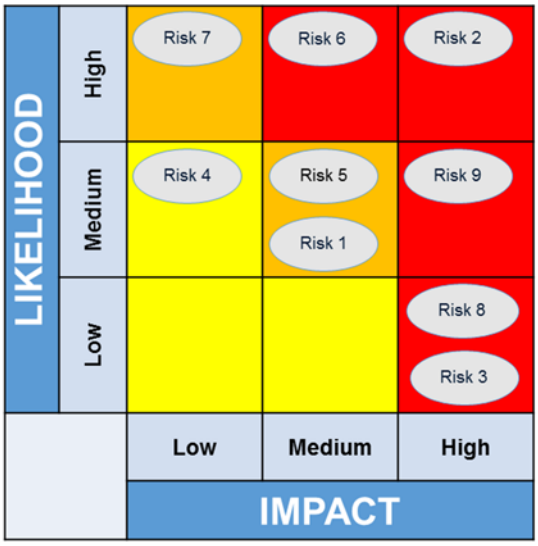
Internal auditors should examine all of the organization's significant models for these sources of risk and determine which specific risks are relevant to the models included in the engagement. Internal auditors may want to interview model developers, validators, risk managers, and other relevant personnel who may have technical knowledge that can assist in identifying risks customized to a specific model or group of models. As previously mentioned, internal auditors may obtain management's assessments of the inherent risks of the models and incorporate that information into their engagement-level risk assessment as well.

An effective way to perform and document an engagement-level risk assessment is to create a risk matrix listing the relevant risks and then expand the matrix to include measures of significance. An MRM risk matrix may be created using a spreadsheet or similar document, with or without an audit software program. The format of the matrix may vary but typically includes a row for each risk and a column for each risk measure, such as impact and likelihood.

Assessing likelihood is relatively straightforward; factors to consider include past risk occurrences, risk occurrence data from proxy sources, the complexity of the model, and the number of people involved in the process. Assessing impact is often more complicated because it involves both quantitative and qualitative factors. Internal auditors should account for not only the financial, operational, and regulatory impact of the MRM risks, but also the nonfinancial impacts, such as damage to the organization's reputation or relationships with customers or vendors. For example, an error in a data stream for an upstream model may have material impacts on downstream models depending on how the outputs from the upstream model are used. Some risks may seem insignificant on their own but should be considered in the context of the organization's MRM program.

The risk ratings from the MRM risk matrix can then be represented on a basic graph, such as a heat map. By plotting each risk's impact along one axis and its likelihood along the other axis, internal auditors clearly depict the risk's overall significance, or priority. Typically, the combined significance of impact and likelihood is indicated using a color system: red denotes the highest priorities, orange denotes risks that are significant enough to warrant consideration, and yellow denotes risks that are not significant, as shown in Figure 2. The heat map should be included in the engagement workpapers because it supports internal auditors' decisions about risk significance.

Figure 2: Heat Map



One limitation of heat maps is that impact and likelihood appear to be equally important. While such equivalence might be true at times, impact usually takes priority over likelihood. For example, in most cases, a risk rated high impact and low likelihood (H, L) should be prioritized over a risk considered low impact, even if the likelihood of its occurrence is high (L, H).

An additional limitation of heat maps is that only two measures can be considered at a time (in this case, impact and likelihood). It may be desirable or necessary to also consider such measures as velocity, vulnerability, volatility, interdependency, and/or correlation when determining the significance of risk.

Based on the completed heat map, internal auditors can easily visualize the risks that are significant when no controls are in place. After internal auditors have identified the significant inherent risks, they should determine which controls, if any, are in place to mitigate those risks. This allows internal auditors to consider the residual risk levels and choose the risks to include in the engagement for further testing.

Like the heat map, the risk and control matrix should be included in the engagement workpapers. The information from the matrix is then incorporated into the preliminary risk assessment used to establish the engagement objectives and scope. The IIA Practice Guide "Engagement Planning: Establishing Objectives and Scope" provides detailed information about building upon the risk assessment to develop the engagement objectives and scope. In addition, the heat map and risk and control matrix will lend support to the engagement results and conclusions, in conformance with Standard 2330 – Documenting Information.

Form engagement objectives

IIA Standard 2210 – Engagement Objectives

The objective of an MRM assurance engagement is typically to provide independent assurance over the governance, policies, processes, and key controls that support the implementation, execution, and oversight of an organization's MRM framework.

When forming the engagement objectives, internal auditors must identify the criteria that will be used to evaluate whether MRM-related objectives and goals have been accomplished. According to Standard 2210.A3, internal auditors may use any of the following sources of criteria:

- Internal (e.g., policies and procedures of the organization).
- External (e.g., laws and regulations imposed by statutory bodies).
- Leading practices (e.g., industry and professional guidance).

Objectives of Assurance Engagements

- Reflect risks to the business objectives of the area or process that were assessed as significant during the preliminary risk assessment (Standard 2210.A1).
- Consider the probability of significant errors, fraud, noncompliance, and other exposures (Standard 2210.A2).
- Identify appropriate evaluation criteria (Standard 2210.A3).

In the end, the assessment should determine whether the MRM framework is functioning in accordance with the expectations of supervisors and the board and as described in approved policies and procedures.

Establish engagement scope

IIA Standard 2220 – Engagement Scope

Internal auditors should consider including the following in determining the scope of an engagement to assess model risk management:

1. Sufficiency of the policies, procedures, and activities that support the models and MRM framework, including alignment with the organization's risk appetite, stakeholder expectations, and industry standards.
2. Governance conducted over the policies, procedures, and activities that support the models and MRM framework.
3. Inclusion of the following in the MRM framework:
    - Defined roles and responsibilities for each of the three lines of defense and governing bodies.
    - Definitions of a model, model risk appetite, and materiality.
    - A model inventory, risk rating criteria, and risk assessment process.
    - Expectations related to model controls, including input and result review, data accuracy, balancing controls, security, and change controls.

- Reporting requirements for model risk exposures.
- A risk-based model review plan that includes independent review and testing, including standards for definition and approval of the plan.
- Model validation standards including coverage of: conceptual soundness, data, IT infrastructure, documentation, processes and controls, and model limitations.
- Processes for the classification, escalation, and tracking of findings that result from model validation activities.

4. Operating effectiveness of model risk management activities.

Internal auditors should customize these elements to their unique organization; however, all of these things should be present in some form.

Allocate resources

IIA Standard 2230 – Engagement Resource Allocation

IIA Standard 2230 – Engagement Resource Allocation states: "Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources." Further, according to IIA Standard 1100 – Independence and Objectivity, internal auditors must be objective in performing their work, and the internal audit activity must be independent, that is, "free from conditions that threaten the internal audit activity's ability to execute internal audit responsibilities." Standard 1130.A1 requires internal auditors to "refrain from assessing operations for which they were previously responsible." To be independent, internal auditors should not be involved with the development, implementation, or use of the models (or MRM framework) under review. However, internal auditors may be involved with the validation process. If this situation occurs, the internal auditors who performed the validation work should not be part of the MRM audit team.

Internal auditors leading an assessment of an MRM framework need skills and specialized knowledge in addition to having a clear understanding of the regulatory requirements to which the organization is subject. This should include both modeling concepts and their use in the relevant lines of business. All internal auditors on the model risk team should possess general competencies for auditing model risk, but they are not required to be model risk experts.

The engagement supervisor should ensure appropriate staff is assigned to each area of the engagement. IIA Standard 1210 – Proficiency states: "Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities." To uphold these standards, more experienced internal auditors with in-depth business and modeling knowledge should be assigned to the validation area. In addition, internal auditors who have proficiencies in the business, modeling, and information technology should test the development, implementation, and use

area. The remaining areas of the audit plan can be tested by less experienced staff with a strong understanding of basic audit concepts and a working knowledge of the business.

On a routine basis, the **chief audit executive** (CAE) may perform a gap analysis to review the qualifications and competencies of internal auditors on staff and to determine whether the internal audit activity collectively possesses the appropriate qualifications and competencies. If the internal audit activity lacks sufficient and appropriate competencies, Standard 1210.A1 requires that the CAE obtain competent advice and assistance to perform all or part of the audit engagement. Options include oversight, training, and outsourcing.

If the CAE finds gaps in the internal audit activity's knowledge of MRM, it may be cost effective to provide model risk training. This can be achieved by having in-house experts develop training or by hiring external trainers. If knowledge gaps are too great, time to provide training is insufficient, or training is too expensive, then the audit engagement should be cosourced. Implementation Guide 2230 – Engagement Resource Allocation provides additional guidance on utilizing third parties.

When choosing an outside partner with whom to work on model risk assessments, the CAE must ensure a qualified, competent, capable, and objective audit expert is hired. Once selected, all agreed upon services should be formally documented. Standard 2050 – Coordination and Reliance notes: "Where reliance is placed on the work of others, the chief audit executive is still accountable and responsible for ensuring adequate support for conclusions and opinions reached by the internal audit activity." Therefore, even if testing is cosourced with an external third party, the expert's work product should be evaluated through corroborative procedures upon completion of the engagement. Thus, the CAE and internal auditors who might evaluate the expert's work must understand MRM concepts and auditor responsibilities. When hiring an expert, the CAE or delegated engagement supervisor may use the "Evaluating an Expert" diagram in Appendix C.

Document the plan

IIA Standard 2240 – Engagement Work Program

During planning, internal auditors document information in engagement workpapers. This information becomes part of the engagement work program that must be established to achieve the engagement objectives, as required by Standard 2240 – Engagement Work Program.

The process of establishing the engagement objectives and scope may produce any or all of the following workpapers:

- Process maps.
- Model inventories.
- Summary of interviews.
- Preliminary risk assessment (e.g., risk and control matrix and heat map).
- Rationale for decisions regarding which risks to include in the engagement.
- Criteria that will be used to evaluate the area or process under review.

For more details on how to plan and scope an engagement, see The IIA Practice Guide "Engagement Planning: Establishing Objectives and Scope."

Testing and Evaluating Model Risk Management

IIA Standard 2300 – Performing the Engagement
IIA Standard 2320 – Analysis and Evaluation

Testing governance and oversight

Internal auditors should design tests to confirm that senior management and the board have primary responsibility for establishing and enforcing the MRM framework. Board minutes should be reviewed to confirm the board is actively engaged in the MRM process. In addition, internal auditors should obtain evidence that all aspects of the MRM process have been assigned to appropriate parties and are being properly performed. When assessing the appropriateness of assigned responsibilities, internal auditors may refer to The IIA's Three Lines of Defense model.[10] Appendix D offers more information.

Evaluating documented MRM procedures

Internal auditors should confirm that the organization's MRM procedures promote good business practices and are consistent with regulatory requirements. For example, internal auditors should obtain evidence that the board or its delegates review and approve the procedures annually. In addition, internal auditors should seek evidence that protocols are in place to trigger timely procedural updates related to changes in products, regulations, organizational structure (acquisitions), and similar events. Finally, internal auditors should verify that the procedures cover the entire MRM process in detail and include the roles and responsibilities of all parties involved.

Maintaining a model inventory

Management is responsible for compiling a complete and accurate inventory of models that includes all models in development, in use, and recently retired. Internal auditors should confirm the existence of the inventory and validate that adequate controls are in place to confirm its completeness and accuracy. In addition, internal auditors should assess whether the level of detail in the inventory is reasonable given the complexity of the organization's models and their level of usage. Finally, internal auditors may use information from the model inventory to help determine the level of employee adherence to the organization's MRM policies and procedures. Appendix D provides more information.

[10] The Institute of Internal Auditors. The IIA's Position Paper*: The Three Lines of Defense in Effective Risk Management and Control*, 2-6.

Testing the validation process

To begin building an opinion on the validation process, internal auditors should evaluate the adequacy and comprehensiveness of the risk assessment methodology used by validators. The following questions should be asked regarding the risk assessment methodology:

- Is it clearly defined?
- Is it documented?
- Is it followed?
- Does it consider all relevant characteristics that impact the level of risk?
- How often is the risk assessment performed?
- What trigger events would prompt a change in a model's risk level?

Once the methodology has been assessed, internal auditors should evaluate the appropriateness of the individual model risk ratings produced by the risk assessment. For large model inventories, a sample may be used. Internal auditors should determine whether the control activities for each level of risk (frequency of validation, etc.) are appropriate and should assure that models are not intentionally "underrated" to escape additional scrutiny.

Internal auditors should perform high-level testing to confirm that the validation process is comprehensive and that the validators are reviewing all key risk areas. Substantive testing should be performed on validation programs that involve a sample of models. Such testing should confirm that the validators have reviewed the conceptual soundness of the models, including their inputs, processing, and reporting components. Internal auditors should also confirm the validators met the criteria for effective challenge, which may be defined as "critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate change."[11]

Internal auditors should verify that the level of validation activities performed was commensurate with the model's risk. For example, the validator should have reviewed the model's ongoing monitoring activities and analyzed the outcomes to ensure that the model's output is representative of actual results. Internal auditors should confirm that any deficiencies or limitations noted during the validation process were logged, monitored, and addressed. As a last step, internal auditors should verify that the data quality of the model was validated. This supports the internal audit activity's conformance with IIA Standard 2120.A1 – "The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the… reliability and integrity of financial and operational information." Appendix D provides additional information.

[11] Board of Governors of the Federal Reserve System, *Supervisory Guidance on Model Risk Management*, 4.

Testing model development, implementation, and use

Internal auditors should apply analytical procedures to a sample of models to substantively test model development, implementation, and use. According to the Public Company Accounting Oversight Board's 2002 release AS 2305: *Substantive Analytical Procedures*, "Analytical procedures are an important part of the audit process and consist of evaluations of financial information made by a study of plausible relationships among both financial and nonfinancial data. Analytical procedures range from simple comparisons to the use of complex models involving many relationships and elements of data." The IIA's Implementation Guide 2320 – Analysis and Evaluation provides more information on internal audit methods of analyses.

Internal auditors should obtain confirmation that the developers who created the models and performed testing possessed sufficient, relevant skills and that all final modeling decisions were properly supported. Detailed documentation of the entire process should be readily available for internal audit's review. Internal auditors should seek evidence to confirm that developers obtained required approvals prior to implementation. Appendix D offers more information.

Model data

An organization's MRM framework should establish control standards for models, including controls over data inputs. Internal auditors should perform testing to confirm that data input controls are assessed during model validations and could also check the quality of data inputs. Controls should be in place to help ensure the data is complete, accurate, timely, and correctly interpreted. When proxy data is used, internal auditors should assess the appropriateness of the method used to develop the data. If the model uses data from another model, internal auditors should assess the controls that are in place to ensure the accuracy of the sub-model calculations and output.

Use of third parties in development and/or validation

To support the effective ongoing use and viability of third-party tools, the organization should obtain results of each vendor's ongoing monitoring and details of any modifications to models, as well as performing its own ongoing monitoring using organizational inputs. Additionally, the organization must have a contingency plan in place to prevent interruption of its activity if the vendor becomes unable to support the model, perform ongoing monitoring, or make modifications.

Internal auditors should confirm that the vendor is performing according to any service level agreements in place. If a vendor becomes unable to fulfill its obligations, internal auditors should verify that management has executed the contingency plan timely and completely according to the documented procedures. If an external party is hired to perform a validation, internal auditors should confirm that the party meets the effective challenge criteria. Appendix D provides more information.

Reporting the Engagement Results

IIA Standard 2330 – Documenting Information
IIA Standard 2410 – Criteria for Communicating
IIA Standard 2440 – Disseminating Results

Upon completion of thorough testing, analysis, and evaluation, internal auditors will have documented "sufficient, reliable, relevant, and useful information to support the engagement results and conclusions," in conformance with Standard 2330 – Documenting Information. Internal auditors should follow their standard reporting procedures for all MRM engagements. However, when disseminating results, a written report should be issued and the board should receive a copy. If no material weaknesses were identified during an engagement and a satisfactory rating was determined, providing a summary report to the board or its delegates is typically acceptable. However, internal auditors should note that to conform with IIA Standard 2410 – Criteria for Communicating and Standard 2410.A1, the final communication of engagement results must include the engagement's objectives, scope, results, applicable conclusions, recommendations, and/or action plans. More information may be found in The IIA's Practice Guide "Audit Reports: Communicating Assurance Engagement Results."

Appendix A. Related IIA Standards and Guidance

Please refer to the *Standards* for the complete pronouncement. To assist with the implementation of the *Standards*, The IIA recommends that internal auditors refer to each standard's respective Implementation Guide.

Related IIA Standards
Standard 1100 – Independence and Objectivity
Standard 1210 – Proficiency
Standard 2060 – Reporting to Senior Management and the Board
Standard 2200 – Engagement Planning
Standard 2201 – Planning Considerations
Standard 2210 – Engagement Objectives
Standard 2220 – Engagement Scope
Standard 2230 – Engagement Resource Allocation
Standard 2240 – Engagement Work Program
Standard 2300 – Performing the Engagement
Standard 2320 – Analysis and Evaluation
Standard 2330 – Documenting Information
Standard 2410 – Criteria for Communicating
Standard 2440 – Disseminating Results
Related IIA Guidance
Practice Guide "Audit Reports: Communicating Assurance Engagement Results," 2016.
Practice Guide "Auditing Capital Adequacy and Stress Testing for Banking Institutions," 2018.
Practice Guide "Auditing Liquidity Risk: An Overview," 2018.
Practice Guide "Engagement Planning: Establishing Objectives and Scope," 2017.
Practice Guide "Internal Audit and the Second Line of Defense," 2016.
IIA Position Paper: *The Three Lines of Defense in Effective Risk Management and Control*, 2013.

Appendix B. Glossary

Terms identified with an asterisk (*) are taken from the "Glossary" of The IIA's *International Professional Practices Framework®* (*IPPF®*), 2017 edition. Unless otherwise noted, the remaining definitions are taken from Federal Reserve, SR 11-7: Guidance on Model Risk Management, 2011.

Aggregate Model Risk – Interrelated model risk caused by shared inputs and assumptions or one model's output being another model's input.

Chief Audit Executive* – Describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of the International Professional Practices Framework. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title and/or responsibilities of the chief audit executive may vary across organizations.

Inherent Risk – The risk before the quality of internal controls is considered.[12]

Materiality – What would be material to the reasonable investor when making an investment decision in the company's securities. Usually, this is 5 percent of the company's pre-tax net income, but may be different when the company has losses or low profit levels; both quantitative and qualitative aspects must be considered[13].

Model – 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 date to the model; a processing component, which transforms inputs into estimates; and a reporting component, which translates the estimates into useful business information.

Model Criteria – Set of definitions used to assist management in determining which tools or processes are considered models.

Model Risk – The potential for adverse consequences from decisions based on incorrect or misused model outputs or reports. Model risk occurs primarily for three reasons:

1. Fundamental errors may produce inaccurate outputs when viewed against the design objective and intended business uses.
2. Incorrect or inappropriate use.
3. Inaccurate or corrupted input data.

---

[12] Norman Marks, *Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioners*, (Altamonte Springs: The Institute of Internal Auditors, 2008), https://na.theiia.org/standards-guidance/Public%20Documents/Sarbanes-Oxley_Section_404_--_A_Guide_for_Management_2nd_edition_1_08.pdf

[13] Ibid.

Model Risk Management (MRM) – The process of building models, rating their risks, and managing those risks.

Risk Appetite* – The level of risk that an organization is willing to accept.

Appendix C. Diagram: Evaluating an Expert

Appendix D. Testing and Evaluating Model Risk Management

Given the internal audit activity's role in providing independent assurance that the organization is managing risk in a way that is consistent with regulatory requirements and the achievement of their objectives, the tables below comprise a framework for conducting an assessment of the MRM framework. The internal auditor may need to tailor or create test steps for unique areas of an organization's specific framework, policies, and procedures. The internal auditor may also need to refer to work programs for related areas (i.e., stress testing, liquidity risk management, credit/market/operational risk management) to design a fully developed MRM engagement, especially if the engagement is broken down into segments as mentioned in this guide.

Governance and Oversight	Initials/ Date	WP Ref
Communications		
■ MRM roles and responsibilities have been communicated. ■ MRM organizational communications are accurate.		
Training		
■ Employees trained on the MRM process. ■ Training documents are accurate. ■ All required employees have completed the training.		
Roles and Responsibilities		
■ Roles and responsibilities for compliance align with the Three Lines of Defense model. ■ Roles and responsibilities include a detailed description of who performs each process, the expected deliverables, and timing of required approvals.		
Board of Directors and Senior Management		
■ Review of board minutes evidences board's active involvement with the MRM process, including consideration of the organization's risk tolerance. ■ The board assesses model risk for the organization individually and in the aggregate. ■ The board received all required MRM reporting during the year. ■ The board is required to review and approve the policies and procedures on an annual basis. A copy of the most recent approval has been obtained.		

Policies and Procedures	Initials/ Date	WP Ref
Completeness and Accuracy		
■ The policies and procedures are current and updated timely for any procedural changes. Updates requested by the board during the most recent review were made properly. ■ The policies and procedures cover the entire MRM process in detail. Specific areas of importance are included: - Documentation standards. - Criteria for defining a model. - Model and model risk definitions. - Risk appetite statement. - Materiality statement. - Governance overview. - Controls. - Development standards. - Implementation and use guidelines. - Validation and ongoing monitoring. - Risk assessment methodology. - Data considerations. - Change management. - Processes/criteria for classification, escalation, and tracking model issues. ■ All pertinent regulations have been incorporated into the policies and procedures (e.g., SR 11-07/OCC 2011-12, Basel III, Solvency II, SR 15-18).		

Development, Implementation, and Use	Initials/ Date	WP Ref
Assignment of Developers		
■ On a collective basis, the skills of the developers assigned to build the model appear appropriate in terms of educational background, experience, and/or technical knowledge.		
General Documentation		
■ The decision to build or purchase the model was clearly documented. ■ The model's purpose was documented. ■ All required reviews and approvals were performed.		
Appropriateness of Model		
■ The technical development documentation is detailed enough for a third party to understand how the model was built. ■ Alternate theories were explored before deciding on the final version of the model. ■ The rationale supporting all assumptions and estimates was documented and appears reasonable. ■ The treatment and controls regarding data used to develop the model are documented. ■ For model(s) purchased from a vendor, detailed specifications were obtained and reviewed and support for modifications to the model is available.		

Development, Implementation, and Use	Initials/ Date	WP Ref
Developer and End-user Testing		
■ The developers performed detailed testing on the model to ensure it was functioning properly. ■ The developers tested the model input data for accuracy and completeness. ■ Any limitations noted during testing were documented. ■ Any errors noted during testing were logged and corrected. ■ If the end users were given the opportunity to test the model, all relevant comments were reviewed and addressed, as appropriate. ■ If the model was implemented before testing was completed, the appropriate level of authority was involved in the decision.		
Model Changes		
■ Changes to the model were logged and documented according to the policies and procedures. ■ All changes were reviewed and approved.		
Implementation		
■ The model code deployed was the same as the code that was tested and subject to validation. ■ The implemented version of the model contains the approved assumptions. ■ The model and its inputs and outputs were implemented in an access-controlled, corporate IT infrastructure.		
Access Controls		
■ The working version of the model is not stored locally on individual computers. ■ Internal auditors have obtained a list of users with model access and have inquired about those who have/do not have an obvious business need to access the model. ■ Internal auditors have cross-referenced an employee listing to a list of users with model access and have inquired about nonemployees or terminated employees.		
Input Controls		
■ Internal auditors have observed an end user import of data into the model and have reviewed applicable controls for accuracy. ■ All date fields have a consistent format (mm/dd/yy, yyyy/mm/dd, dd/mm/yyyy, etc.). ■ Data linked to upstream or downstream models was accurately transmitted. ■ If the model has indicators to notify a user when incorrect information has been entered, internal auditors have tested the functionality of the indicators by asking the end user to enter erroneous data. ■ Data coming from different sources is segregated and labeled. ■ Internal auditors have traced back one set of imported data to the source file to confirm its accuracy and completeness.		

Development, Implementation, and Use	Initials/ Date	WP Ref
Calculation Controls		
■ All cells or fields that do not require data inputs are locked and protected. ■ Cross-footing was implemented wherever possible. Internal auditors have performed recalculations to verify accuracy. ■ Internal auditors have independently performed the model's calculations to verify accuracy. ■ Values for formulas are pulled from data value entry sheets (best practice), not hard coded into formulas. ■ If pivot tables are used, the capture of all relevant data sets has been ensured.		
Output and Management Review		
■ Management performs a variance analysis of actual model output to other known values (e.g., prior periods, budgets, forecasts).		

Validation	Initials/ Date	WP Ref
Policies and Procedures		
■ Templates and guidance around the organization's standard validation procedures include requirements that the validators are required to test all key risk areas. ■ The organization has established a frequency for validation and ongoing monitoring activities. ■ Models are required to be validated prior to implementation. ■ Detailed instructions for the scope and prioritization of validation testing have been established. ■ The risk ratings of models are used to determine the scope and prioritization of validation testing. ■ Confirm that all identified model issues are required to be documented and tracked. ■ The policies and procedures require testing and analysis of models. ■ Targets and acceptable deviations for model accuracy have been established. ■ Procedures for reviewing and addressing unacceptable deviations are in place.		
General		
■ Validation schedules and timelines are presented to the appropriate parties for approval. ■ Models are subject to validation, whether built internally or purchased from a vendor. ■ Validation documentation is detailed enough for a third party to understand the work performed. ■ Validation reporting sent to management is accurate and complete. ■ Validators possess the criteria necessary for effective challenge (i.e., incentives, competence, and influence).		

Validation	Initials/ Date	WP Ref
Conceptual Soundness		
■ Validator performed independent testing to evaluate the developer's choice of theories, assumptions, inputs, data sources, etc. ■ Validation included sensitivity analyses and stress testing wherever appropriate. ■ Model breakdowns and/or limitations identified through the validation were logged, monitored, and corrected or mitigated through additional controls.		
Ongoing Monitoring		
■ Models are subject to an annual review process. ■ Full or partial revalidations were performed if indicated by the latest annual review results. ■ Models are subject to full revalidation on a routine basis, regardless of the annual review results. ■ The validator(s) reviewed all overrides, and the proper override information has been logged, approved, and supported. ■ The validator(s) compared model output to alternative data or models and researched any discrepancies (e.g., benchmarking).		
Outcomes Analysis		
■ The validator(s) performed outcomes analyses to compare model outputs to actual outcomes (e.g., parallel outcomes analysis and back-testing). ■ Discrepancies were researched and addressed, as appropriate.		
Data Quality		
■ Management documented expectations around data quality, and the validator(s) compared the data quality expectations to model data. ■ The validator(s) reviewed controls around the validity, completeness, accuracy, appropriateness, and integrity of the data. Errors identified via the controls were properly addressed. ■ The validator(s) assessed the process in place for refreshing and updating data. ■ Instructions related to data flows, aggregations, and transformations were documented and reviewed by the validator(s). ■ The results of each data aggregation and transformation step were documented. Internal auditors repeated the data aggregations and transformations and compared each step to the business's results.		

Model Inventory	Initials/ Date	WP Ref
Policies and Procedures		
■ The MRM policies and procedures require maintenance of a model inventory. ■ The model inventory is accompanied by guidelines or a template. ■ Criteria have been established to help management distinguish between models and tools or processes. ■ Criteria have been established to rate each model according to its risk and/or materiality.		

Model Inventory	Initials/ Date	WP Ref
Completeness and Accuracy		
■ The models selected for validation and development, implementation, and use testing are included in the model inventory and their information is accurately recorded. ■ If management is required to certify the completeness of the model inventory, a sample of lines of business evidences that all required parties submitted their certifications. ■ If management has a mapping process in place to ensure completeness of the inventory, internal auditors have obtained a copy and reviewed it for reasonableness (e.g., mapping of models to financial statement line items). ■ The model inventory has no blank fields. ■ The model inventory is properly secured so that only approved individuals may make updates.		
Model Classification		
■ The models selected for validation and development, implementation, and use testing meet the organization's criteria for being classified as a model. ■ Nonmodel tools or processes are *not* included in the model inventory. ■ A sample of nonmodel tools or processes appears to be classified appropriately, based on the organization's **model criteria**. ■ Expert judgment models are accurately classified and documented, according to their unique aspects regarding validation, governance, and monitoring of models that are based on expert opinions.		
Model Ratings		
■ Internal auditors have used the model ratings criteria established by management to independently assess the ratings on the model inventory. ■ Model rating overrides (if any) followed the appropriate procedures to be supported and approved. ■ If the inventory contains a large number of low-rated models, their aggregated risk is being assessed.		
Validation		
■ All models on the inventory were validated prior to implementation, unless otherwise properly approved for implementation followed timely by validation. ■ Based on a sample of models that did not pass initial validation, it appears that errors were logged and corrected. ■ Based on details in the model inventory regarding the level of validation performed, models with similar ratings appear to receive commensurate levels of validation work. ■ Changes to models were approved and validated.		
Ongoing Monitoring		
■ All models on the inventory were subject to validation or monitoring through the annual review process during the past year. ■ Each model's most recent validation date or ongoing monitoring schedule matches the timing approved by the organization.		

Appendix E. Overview of Key Regulations

European Union Regulation, Solvency II Directive

This three-pillar directive establishes solvency capital requirement (SCR) for insurers in the European Union, that is, capital levels that enable them to withstand their worst expected losses for a given year within a 99.5 percent confidence level. Under the first pillar, organizations may use a standard model, full internal model, or partial internal model to determine their SCR. The second pillar requires an organization to complete its "own risk and solvency assessment," which ensures the SCR modeled in the first pillar is reasonable. The third pillar increases reporting requirements to both supervisory agencies and the public.

If an organization wishes to use a full or partial internal model for its SCR estimation, it must submit an application to the Prudential Regulation Authority (PRA). Along with the application, the organization must submit a model change policy for review and approval. Within the change policy, the organization must establish criteria for defining major and minor model changes. If the PRA accepts the model and change policy, the organization may begin using the internal model. Going forward, the organization must obtain express approval from the PRA prior to making any policy updates or major model changes.

Capital Requirements Directive IV (Directive 2013/36/EU)

Article 3 — Definitions: 1. For the purposes of this Directive, the following definitions shall apply: […] (11) "model risk" means the potential loss an institution may incur, as a consequence of decisions that could be principally based on the output of internal models, due to errors in the development, implementation, or use of such models.

Article 85 — Operational risk: 1. competent authorities shall ensure that institutions implement policies and processes to evaluate and manage the exposure to operational risk, including model risk, and to cover low-frequency, high-severity events. Institutions shall articulate what constitutes operational risk for the purposes of those policies and procedures.

Basel Committee on Banking Supervision, Basel III

Basel III proposes to globally strengthen the banking sector through capital reforms, liquidity reforms, and general financial system improvements. There is a phase-in period, and each country wishing to adopt Basel III is responsible for implementing the reforms into its national laws and regulations.

Basel III proposes an increase in the quality and quantity of capital held by organizations. This is accomplished through more stringent capital tiering rules and increased capital level requirements. In addition, the proposal sets a maximum leverage ratio of 3 percent to prevent organizations from being over leveraged. The proposal also introduces a 30-day liquidity coverage ratio to ensure organizations maintain adequate liquidity to withstand a stressed funding scenario. Calculating this ratio requires modeling of expected cash outflows under the stressed scenario.

Another ratio proposed by Basel III is the net stable funding ratio. It drives funding toward stable sources by comparing the organization's available stable funding to its required stable funding; both must be modeled. Finally, Basel III includes guidelines for managing risk. Most notably, organizations will need to use models for estimating their counterparty risk, which is the risk that an organization will not pay its outstanding debts upon maturity.

FRB Letter SR 11-7/Bulletin OCC 2011-12

SR 11-7/OCC 2011-12 is a collaborative effort between the FRB and the Office of the Comptroller of the Currency to provide MRM guidance to organizations across the entire model lifecycle. It requires organizations to have documented policies, procedures, and controls around the MRM process. In addition, models must be developed by qualified personnel, validated by an independent third party, and continuously monitored after implementation. Finally, it places ultimate responsibility for the MRM process on the board. Specific requirements of SR 11-7/OCC 2011-12 are explored in detail throughout this guidance.

FRB Letter SR 15-18

In SR 15-18, the FRB provides guidance on the capital planning and supervisory expectations of firms subject to the Large Institution Supervision Coordinating Committee framework and to other large and complex firms. Within this guidance, the FRB requires senior management to design and manage an organization's capital planning process. In addition, senior management is expected to have a sound understanding of the institution's capital planning models, along with any related overlays (i.e., overrides), limitations, and assumptions. Furthermore, senior management should be involved with the related stress testing and sensitivity analyses. On a quarterly basis, senior management is expected to review the entire capital planning process. Results must be reported to the board of directors so they can make a final decision on the organization's capital adequacy.

To comply with SR 15-18, organizations are also required to develop and document stress scenarios that equal or exceed a severely adverse supervisory scenario established by the FRB. The effect of the stressors on the organization's capital level is projected using models or other estimation approaches. To ensure the institution is adequately capitalized, the results are compared to the post-stress capital goals established within the organization's capital policy.

Under SR 15-18, institutions are required to have a strong risk management process and an internal control framework that supports their capital planning process. The internal control framework must include a model inventory, maintenance of detailed model documentation, and an independent model validation process. Internal auditors must perform an overall evaluation of the capital planning process and report the results to the board.

IAIS Standard 2.2.7

This standard mandates three tests to validate models used in determining regulatory capital levels. Institutions are required to submit the results of these tests to the supervisor before the use of internal models would be approved. These tests are mentioned in the text of this guide and are listed here:

1. A statistical quality test assesses the base quantitative methodology of the internal model. As part of this test process, the model user should be able to demonstrate the appropriateness of the methodology, including the choice of model inputs and parameters, and should be able to justify the assumptions underlying the model.
2. A calibration test demonstrates that the regulatory capital requirement determined by the internal model satisfies the modeling criteria specified by the supervisor.
3. A use test confirms that the internal model and its methodologies and results are fully embedded into the risk strategy and operational processes of the model user. The standard also iterates that the board and senior management should have the overall responsibility to ensure that adequate governance and controls are in place related to the construction and use of internal models.

Guidance on the issues to consider in the context of an internal model used for the purposes of an insurer's own risk and solvency assessment, but not for regulatory capital purposes, are discussed in the IAIS guidance paper on enterprise risk management for capital and solvency purposes.

Appendix F. References and Additional Reading

Basel Committee on Banking Supervision. *Basel III: The liquidity coverage ratio and liquidity risk monitoring tools*. Basel, Switzerland: Bank for International Settlements, January 2013. bis.org/publ/bcbs238.pdf.

Basel Committee on Banking Supervision. *Basel III: The net stable funding ratio*. Basel, Switzerland: Bank for International Settlements, 2014. www.bis.org/bcbs/publ/d295.pdf

Board of Governors of the Federal Reserve System. SR Letter 11-7 attachment: *Supervisory Guidance on Model Risk Management*. Washington, D.C.: FRS, 2011. https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf.

Board of Governors of the Federal Reserve System. SR 15-18 attachment: *Federal Reserve Supervisory Assessment of Capital Planning and Positions for LISCC Firms and Large and Complex Firms*. Washington, D.C.: FRS, 2015. https://www.federalreserve.gov/supervisionreg/srletters/sr1518_PW.pdf.

European Parliament and the Council of the European Union. "Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013," *Office Journal of the European Union*. Document 32013L0036. Luxembourg: Publications Office of the European Union, 2013. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:176:0338:0436:En:PDF

Marks, Norman. *Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioners*. Altamonte Springs: The Institute of Internal Auditors, 2008. https://na.theiia.org/standards-guidance/Public%20Documents/Sarbanes-Oxley_Section_404_--_A_Guide_for_Management_2nd_edition_1_08.pdf.

International Auditing and Assurance Standards Board. International Standard on Auditing 620, "Using the Work of an Expert." New York: IFAC, 2008. http://www.ifac.org/system/files/downloads/2008_Auditing_Handbook_A190_ISA_620.pdf.

Office of the Comptroller of the Currency. Bulletin OCC 2011-12, "Description: Supervisory Guidance on Model Risk Management," by Mark Levonian. Washington, D.C.: OCC, 2011. https://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12.html.

Office of the Superintendent for Financial Institutions. "Enterprise-Wide Model Risk Management for Deposit-Taking Institutions." No. E-23. Ottawa: OFSI, 2017. http://www.osfi-bsif.gc.ca/Eng/Docs/e23.pdf.

Organization of England, Prudential Regulation Authority. Policy Statement 2/15: *Solvency II: a new regime for insurers*. London: PRA, 2015. https://www.bankofengland.co.uk/prudential-regulation/publication/2015/solvency-2-a-new-regime-for-insurers.

Rao, Vasant, and Swaminathan Aiyer. “Models, Model Risk and Running Effective Model Management Programs” (white paper). *Cognizant*. April 2015. Teaneck: Cognizant, 2015. https://www.cognizant.com/whitepapers/model-risk-and-running-effective.pdf.

Solvency and Actuarial Issues Subcommittee. “Standard No. 2.2.7: IAIS Standard on the Use of Internal Models for Regulatory Purposes.” Basel: International Association of Insurance Supervisors, 2008. https://www.iaisweb.org/file/34143/16-standard-no-227-on-the-use-of-internal-models-for-regulatory-capital-purposes.

Acknowledgements

Guidance Development Team

Mark Carawan, CIA, QIAL, United States (Chairman)

Stacey Schabel, United States (Project Lead)

Global Guidance Contributors

Karl Erhardt, United States

Margaret Warianka, United States

Gloria DeSantis-Stahl, United States

IIA Global Standards and Guidance

Jeanette York, CCSA, Director (Project Lead)

Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President

Debi Roth, CIA, Managing Director

Shelli Browning, Technical Writer

Lauressa Nelson, Technical Writer

The IIA would like to thank the following oversight bodies for their support: Financial Services Guidance Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and International Professional Practices Framework Oversight Council.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

Copyright

March 2018

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org