# Establishing Model Risk Management

Committee of Chief Risk Officers


First Publication March 2025

## Table of Contents

## Executive Summary

This white paper provides a framework for energy and commodity risk professionals to manage risks stemming from model usage. The Committee of Chief Risk Officers ("CCRO") believes that model risk can be a significant risk source and a necessary component of any effective risk management program. Model Risk Management ("MRM") principles were first enumerated in the banking space and have been making their way into other industries over the past decade. This white paper takes those principles, adapts them to the context of the energy and commodity markets, and recommends an MRM framework relevant to the energy companies. The target audience includes risk committee members, risk managers, modelers, and model validation specialists.

The paper begins with a brief review of model risk in its original context, including regulatory guidance for capital markets such as SR 11-7. That context allows for a robust definition of the word "model," as well as a description of the three most common sources of model risk: misspecification, misuse, and miscalibration. In addition, it allows us to consider End User Computing ("EUC") as separate from the established definition of "model."

The paper considers the major components of the model lifecycle as a starting point for risk management: identification, development, validation, implementation, usage, monitoring, and review. From there, model risk management professionals can begin to assess risk based on usage, materiality, and complexity. Those risks can be managed through the MRM framework principles noted in this paper. Notably, the key framework components include governance, independent challenge and validation, model life cycle management, inventory, and data integrity measures. The framework's goal is to ensure models are used safely, accurately, and efficiently, emphasizing effective challenge principles and tiered risk classification.

The Committee of Chief Risk Officers (CCRO) advocates for industry practitioners to establish reasonable and fit-for-purpose MRM programs based on the recommendations and examples noted in this document. In so doing, companies can benefit from MRM not only as a risk mitigation strategy but also as a driver for operational efficiency and value creation. By means of this white paper, we recommend collaboration within the energy sector to embrace sensible MRM practices, ultimately fostering trust and resilience in model-based decision-making processes across the industry.

The intention of this position paper is to promulgate MRM concepts within the energy industry and provide a recommended MRM framework which members may reference and adapt to their individual business and risk needs.

## Acknowledgements

White papers issued by the CCRO are the product of the efforts of its body of members and other registered working group participants. The views expressed in any particular CCRO paper are attributable only to the CCRO itself and do not necessarily represent the views or intentions of an individual member.

The preparation of a paper is led by a subset of CCRO members, termed a "working group" that possesses a particular interest in the subject topic. The working group then develops, researches, and prepares the paper. Certain external parties, whose functions may include providing valuable expertise, perspective, and/or coordination and facilitation, assist the working group as necessary.

The efforts of all these parties are greatly appreciated, and while this group continues with its work, all interested parties are encouraged to contact us at http://ccro.org.

*The CCRO extends special thanks* to the following organizations and individuals who continue to dedicate considerable and valuable time, resources, expertise, and/or perspective to the preparation and issuance of this paper, *Establishing Model Risk Management*.

### Working Group Leadership Team

#### Lead Authors

Brian O'Neal
Partner
at **Weaver**

Akshay Singh
Market Risk Manager
at **Golden Pass LNG**

#### Thought Leaders

Sid Jacobson
**CCRO Member Emeritus**

Alex Zhukovsky
Director Energy Portfolio Risk
at **National Grid**

Cengizhan Yenerim
Head of Risk and Strategy
at **Engie Energy Marketing, NA**

Pierre Brunelle
Manager Middle Office, Gas & Power
at **Repsol**

While these individuals provided the lead for this initiative's content and direction, many other CCRO members contributed by reviewing and commenting as the paper was developed.

## 1. Background

Post-mortem analysis of the 2008 Global Financial Crisis attributed it partly to poor Model Risk Management ("MRM"). Subsequently, with increased industry experience, the Federal Reserve and Office of the Comptroller of the Currency ("OCC") introduced the Supervisory Guidance on Model Risk Management ("SR 11-7") that provided key conceptual clarity for all phases of model life cycle management. MRM has been a key regulatory mandate in the banking sector since.

Subsequent circumstances, like the market reaction to COVID-19 and the growth of algorithmic trading, reminded banking institutions of the importance of these frameworks and the need for real-time model performance monitoring. Recently, industries outside of banking have considered adopting relevant portions of this statement to mitigate the financial, capital, operational, decision-making, regulatory, and reputational risks attributable to model usage.

# 2. Definitions

## 2.1. Model

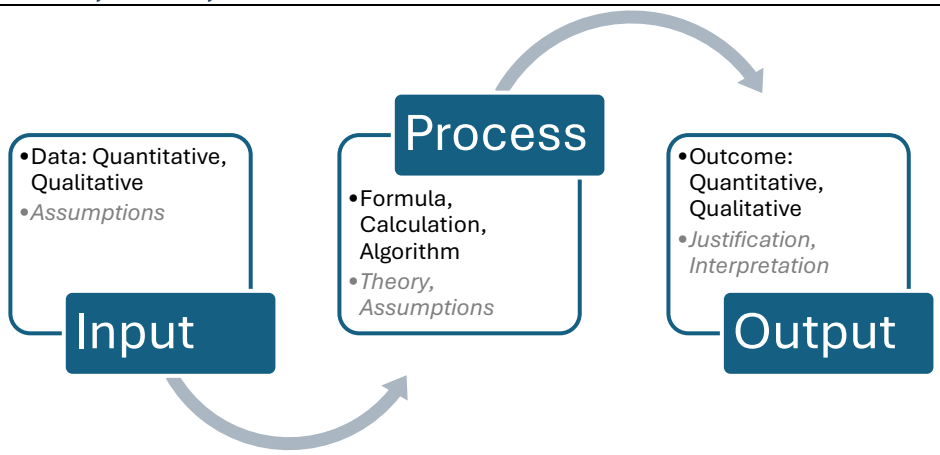
Analytical models are sophisticated computational tools that organizations depend on to inform financial decisions, optimize investments, shape operational strategies, manage risks, ensure regulatory compliance, and support various other critical business functions and reporting. They are typically imperfect approximations of reality, subject to the parameters and constraints of their inputs and quantitative approaches.

SR 11-7 defines models as follows:

> "The term *model* refers to a quantitative method, system or approach that applies statistical, economic, financial, or mathematical theories, techniques and assumptions to process input data into quantitative estimates…The definition of *model* also covers quantitative as approaches whose inputs are partially or wholly qualitative based on expert judgment, provided that the output is quantitative in nature."

The flow and transformation of data within a model can be thought of as follows:

*Figure 1: Flow and Transformation of Data*




Not all calculations or processing approaches are considered "models" for this purpose. Rather, the uncertainty attributable to assumption and theory selection, parameters and input choices, and output interpretation is an essential determinant for something to be considered a model.

## 2.2. Model Risk

Model risk arises from actions taken or decisions made based on incorrect or misapplied model outputs. The term "model risk" refers to the uncertainty that arises primarily due to:

- Misspecification: fundamental errors caused by improper development, over/underfitting, or false validation that causes incorrect results;
- Misuse: incorrect or inappropriate model usage, ignorance about limitations, and other errors stemming from using a model without full understanding; and

- Miscalibration: data errors resulting from incorrect inputs, or false parameterization.

Model risk can be categorized by inherent complexity and materiality, including the model's relevance. That categorization can be used to prioritize activities for highly complex, material models while reducing the administrative burden for low-risk, low-impact models. For example, model risk might be organized by tiers as presented below:

*Figure 2: Model Risk Tiers*

| **Model Risk Classification Tiers** | | **Materiality** | | |
|---|---|---|---|---|
| | | *High* | *Medium* | *Low* |
| **Complexity** | *High* | Tier-1 | Tier-2 | Tier-3 |
| | *Medium* | Tier-2 | Tier-3 | Tier-4 |
| | *Low* | Tier-3 | Tier-3 | Tier-4 |

In this example, Tier-1 models carry the highest model risk and should be subject to the most stringent controls. Tier-4 models, on the other hand, are comparatively lower risk and may be subject to less rigor.

### 2.3. Model Risk Management

The term "Model Risk Management" ("MRM") refers to the system of organization, controls, procedures, and supporting capabilities that allow a company to manage risk throughout the model life cycle. The foundation of any MRM program should mandate that the business is only allowed to use validated models with current approvals. Companies should aim for a fit-for-purpose framework that aligns with their organization, models, and risk profile, in addition to meeting regulatory requirements and considering other human factors such as health and safety concerns. MRM programs generally incorporate policies and procedures, committee participation, and independent model development and validation teams (see Section 4 for more details).

### 2.4. Tools and End User Computing

The terms "End User Computing" (EUC) and "Tool" refer to Information Technology (IT) applications, databases, spreadsheets, macros, database queries, batch processing programs, scripts, and vendor-based software products that might not meet a strict definition of "model" but should still be subject to reasonable oversight and controls. Since these EUC tools can pose significant risks, organizations should have a fit-for-purpose EUC governance framework alongside their MRM framework.

### 2.5. Vendor Models

The term "vendor models" has two meanings in this paper. The first includes stand-alone models provided by a third party. The second includes models and functions embedded in software systems (e.g., the Black-Scholes engine in a trade capture system) or analytics

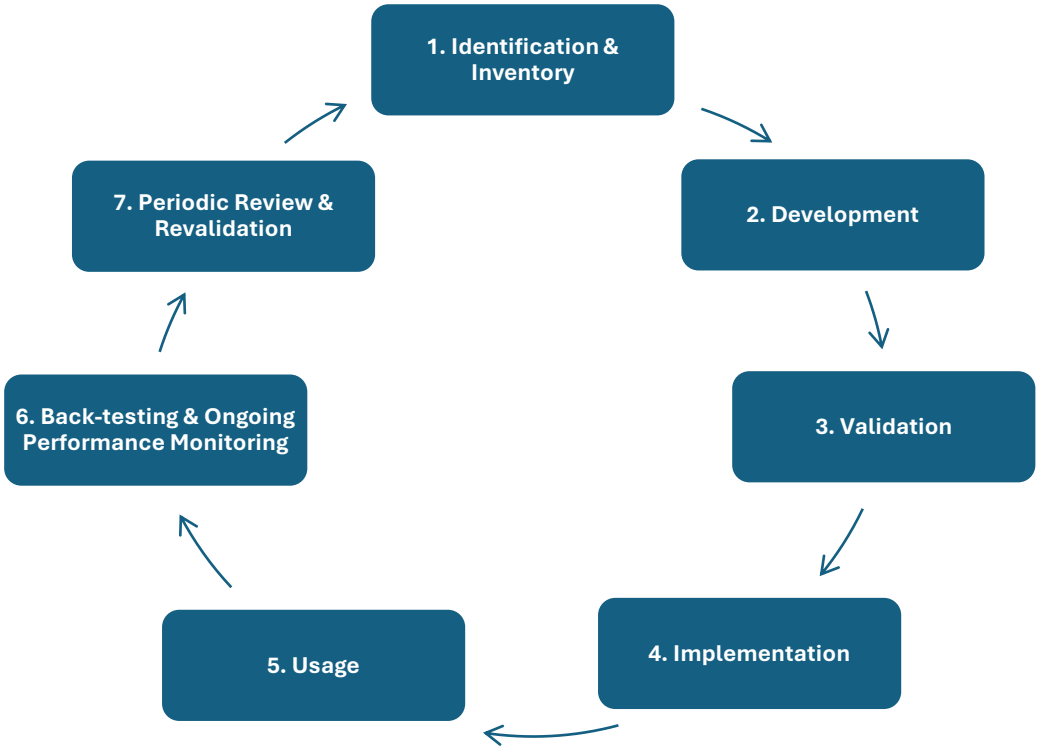
platforms (e.g., the Expected Shortfall function in pyRisk). Vendor models create unique risks and should be subject to reasonable oversight and control.

### 2.6. Model Life Cycle

The term "model life cycle" refers to the various stages of activities that a model goes through as it progresses from conception and development to validation and deployment and eventually to deprecation. The model life cycle includes more than the traditional development, testing, validation, and deployment phases common for IT applications and systems. Rather, it considers broader model governance expectations through all stages in the life of a model. It starts with the need or intent to have a model and involves documenting the rationale behind selected data, processing techniques, and output components. A model requires thorough testing, verification, and challenge during the model validation phase. It also includes model change controls, upgrades, and end-of-life processes.

Proper model life cycle management is an iterative process, as summarized below:

*Figure 3: Model Life Cycle Management*



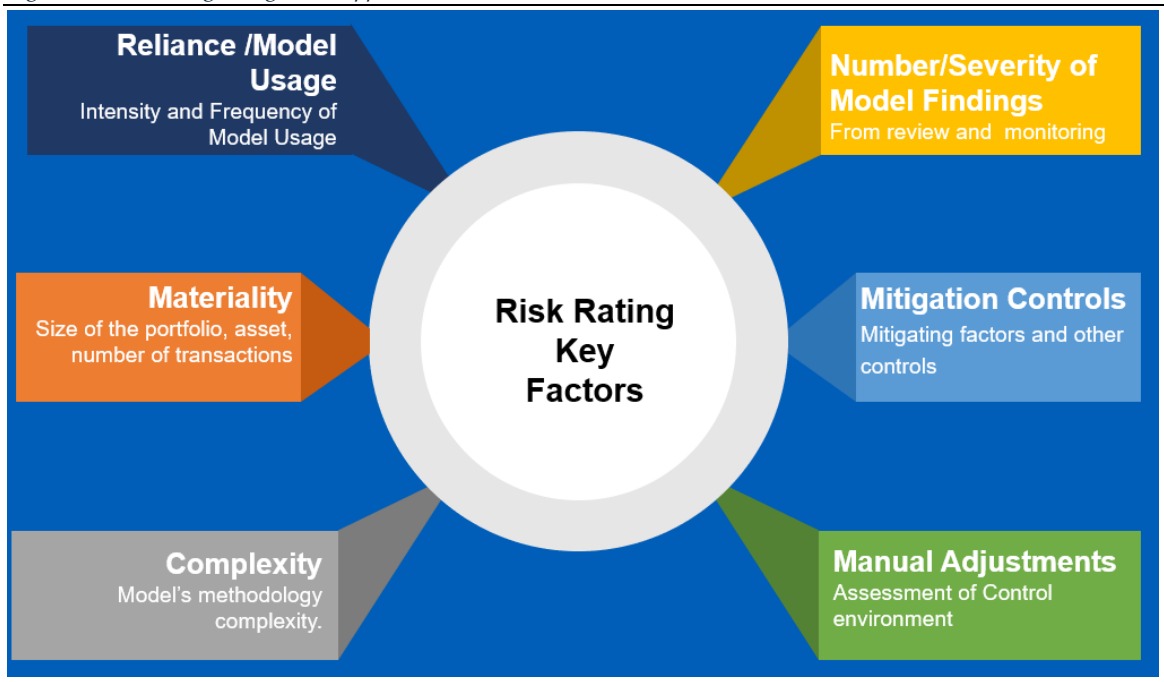

1. Identification & Inventory: The processes and platforms by which all model-like tools are identified and inventoried before use, classified as models or EUC, and reported to management.

2. Development: The model request and development processes, including selection and design development implementation, testing, performance monitoring planning, and documentation.
3. Validation: The independent verification of assumptions, choices, operability, and results from the model development process. Validation incorporates effective challenge principles and typically includes analysis, testing and challenger models, documentation, risk tiering, and approval processes to move the model from development to implementation.
4. Implementation: The implementation and deployment of models following proper validation and approval. Implementation processes often include change management procedures, upstream and downstream data dependency identification, communication and training plan rollout, and prior-model restoration plans if the implementation fails.
5. Usage: The use of models for their intended purposes. Usage processes include receiving training, supervision of access rights and other controls, running the model and accessing its outputs.
6. Ongoing Performance Monitoring: Statistical performance reviews are carried out on a regular basis. Monitoring processes often include escalations when results deviate from stated use cases or predefined tolerance parameters. Back-testing processes often include parameterization reviews and recalibration as necessary to maintain model accuracy and usefulness.
7. Periodic Review & Revalidation: The post-validation review and revalidation are carried out by the validation team on a regular basis.

## 3. Model Risk Management Goals

There are numerous factors that can contribute to increased model risk. These factors include governance program dysfunction (e.g., process, control, reporting deficiencies), staff turnover, regulatory pressure, market changes, and other external macro events. A strong MRM program should support the company's understanding of its model risk by defining key risk factors and standardizing risk ratings. For example, a company might combine qualitative and judgmental approaches to determine risk rating via a categorical approach, as noted below:

*Figure 4: Risk Rating Categorical Approach*




In practice, a risk-based assessment within the model inventory should align model development and usage with risk management principles. By considering the model's purpose and usage and the consequence of misspecification or misuse, the company should improve its understanding of model risk and be able to take the steps necessary to manage that risk to tolerable levels. Even the simplest calculations have the potential to expose an organization to significant risk. Thus, a well-defined MRM program should be applicable in most instances.

## 4. Model Usage

Energy markets are highly volatile, subject to complex valuation drivers, and can often lack transparent observable data. Input data can often be dependent on relationships with other data, tenors, locations, and data sources. Beyond those factors, the energy sector faces ongoing complexity due to the influences of weather, logistics, geopolitics, environmental changes, social and governance factors, consumer preferences, and physical market structure changes. For example, power markets are subject to real-time hourly spot electricity prices, non-standard price determination processes for renewables, grid/transmission reliability, zonal or nodal price spreads, and a complex interplay between environmental events, generation performance, available capacity, and variable load demand. As such, our members have observed an organizational need and focus on a wide variety of financial and operational models to manage both their business and system reliability.

Energy also has diverse use cases for models beyond traditional financial and credit risk management activities. For example, operational safety and reliability are highly valued in the energy sector, as are supply security, optimal asset utilization, portfolio valuation, financial planning and analysis, and long-term forecasting. The advent of Big Data, Artificial Intelligence ("AI") and Machine Learning ("ML") has further fueled the use of complex models and a need for traceability.

With increased usage comes increased responsibility. The Committee of Chief Risk Officers ("CCRO") recommends its members develop MRM framework suitable to their specific lines of business and risk profiles. Recognizing an opportunity to efficiently convey an industry perspective, the CCRO formed a dedicated MRM Working Group (the "Working Group") to consider the issue and publish this position paper.

# 5. Model Risk Management Framework

## 5.1. Introduction

### *Basic Framework*

An effective MRM program should enable a company to manage model-related risks and drive value across the organization. This starts with a framework that includes provisions for people, processes, technology, and data embedded in its core components. In addition, the framework should have a strong organizational structure, a clear plan for delivery, a transparent model inventory, and effective model data and security management.

It is the Working Group's assertion that the MRM framework should be thoughtfully considered to each company's activities, exposure, and stakeholder expectations.

### *Principles of Effective Challenge*

Organizations should address model risk at both the individual model and the aggregate level using the guiding principle of "effective challenge." Although it is not a regulatory requirement for most energy market participants, SR 11-7 provides a useful definition of effective challenge: "critical analysis by objective, informed parties that can identify model limitations and produce appropriate changes." Effective challenge should involve a combination of incentives, competence, and influence across the model life cycle.

## 5.2. Framework Components

When designing an MRM framework, the company should consider organizational capabilities, model prevalence and complexity, and enterprise risk tolerance. The MRM framework typically should include the following.

- **Governing Documents**: An MRM Policy, controls, procedures, and other documents as needed to ensure effective model risk governance.
- **Committee Oversight**: Either a Model Risk Oversight Committee or a standing agenda item in Risk or Audit Committee meetings.
- **Dedicated Modelers**: A model development team or Subject Matter Expert ("SME") roles with specific modeling competencies.
- **Independent Challenge**: A model validation function or SME roles that report independently of the model developers.
- **Model Documentation**: Requirements and document templates for models, model testing, validations, and ongoing monitoring.
- **Inventory**: Model inventories with model owners, risk tiering, approved uses and users, testing results, validation status, and supporting technologies.
- **Reporting**: Regular reporting for model development and validation status, policy violations, and model risk estimates.

**Recommendations:**

1. Identification and inventory should include all models, applications, systems, and EUC tools. The inventory process should include a risk assessment and tiering for each model. It should also identify and eliminate duplicate or superfluous models.
2. The model development processes should function as a first control against model risk and should require a competent practitioner to build the model. The developer should reference a challenger model to provide comparative results, conduct pre-implementation testing to ensure the model works properly, and clearly communicate with the requester and users to ensure proper usage in the future. The developer should share key assumptions, data inputs, methodologies, and outputs with stakeholders and solicit their feedback prior to model completion.
3. The pre-implementation phase should include performance testing against challenger models with explanations of differences, sensitivity analysis for all inputs and assumptions, spurious input testing, system compatibility and crash sensitivity, monotonicity and continuity analysis, and any other tests deemed relevant.
4. Model documentation should include clear statements on objectives, conceptual model design, inputs, development methodology, alternatives, and the criteria used to justify selections, assumptions and parameters, unaddressed risks, and known usage limitations. Model documents should provide sufficient detail to allow a competent third party to fully understand and replicate the model. Screenshots of code and user functionality is also a valuable practice, as are links to code repositories and raw data.
5. Model validation should function as a second line of defense and should require a competent practitioner, independent of the model's requestor or developer and their reporting lines. The validation process should verify assumptions, choices, and findings from the development process. Validators should use the effective challenge principle as a guideline, document their work, and retain all validation input and output data. Interim findings should be shared with model developers to allow for iterative refinement before issuing an approval, a conditional approval, or a rejection. Documented approvals should include an expiration date and future re-validation requirements.
6. Implementation processes should be subject to the organization's normal change management and IT implementation procedures, including code lockdown, version release testing, and change control permissions and authorities. Implementation documentation should clearly describe the implementation context, upstream data dependency assumptions, known downstream dependencies, communication and training plans, pre-and post-implementation tests to be conducted, and a rollback plan if the implementation fails. Implementation plans should ensure that adequate data lineage can be maintained between the inputs, model processing components, and its outputs. Finally, implementation documentation should identify the users, their relevant roles, access permissions, and training requirements.
7. Models should be restricted to intended uses. Model users should be able to run the model, access its outputs, and receive training when necessary. Model owners should closely supervise access permissions and usage, ensure performance parameters are

logged, and confirm that process controls exist to prevent misuse or unintended outcomes.

8. Regular statistical performance reviews should be carried out. Any deviation from the stated use cases or predefined tolerance parameters should be escalated to the model governance, validation, and model development teams. Additionally, back-testing should be regularly conducted to ensure the model is properly calibrated to current market conditions. Model owners should have clear controls and processes for model stoppage, change management, and recalibration if ongoing monitoring or backtests indicate a need for change.
9. Models and their challenger models should be reviewed and re-validated on a regular basis. The validation team should have the option to grant a continuation of the existing model validation status, seek a minor revalidation, or pull the model out of use during a major revalidation or redevelopment process. The frequency of re-validation should be tied to the model's risk tier as determined by the validation team.

### 5.3. Organizational Structure

A sound MRM program should have a well-supported team of expert stakeholders inclusive of users of the outputs and controls functions. The MRM team should be comprised of individuals responsible for developing, implementing, supporting, and governing analytics and models.

The team should carefully outline the skills, roles, responsibilities, and support activities needed for each analytic and modeling capability. In addition, it should establish where each resides within the organization inclusive of lines of reporting and spans of control.

In standing up an MRM support structure, the company should first assess its current state. That assessment should include the company's understanding of how model development is organized, structured, tested, documented, and approved, who has institutional and technical knowledge, what vendor dependencies exist and where they reside, and what control activities exist.

**Recommendations:**

1. Model developers and independent validation specialists should have proper training, skills, and knowledge.
2. Model owners should review the approved use of models, review ongoing monitoring and back-testing results, have the responsibility to evaluate overrides, determine the root cause of errors, and discern whether the model should be updated.
3. Model governance and validation personnel should have the authority and independence to provide an effective challenge, including the authorization to halt model usage if they deem it excessively risky or erroneous.
4. Roles and responsibilities should be clearly defined with appropriate descriptions of accountability across the model development lifecycle.

### 5.4. Framework Delivery

The MRM framework should be used to determine what should be designed and implemented as part of the MRM program rollout. A sound MRM program should have standards addressing analytics, model development, and documentation as noted in 4.2. Formalized processes and approvals for implementing, testing, validating, usage, and monitoring should accompany the company's MRM standards. When designing the program, companies should begin with an initial current state assessment and consider structured processes for model approval and deployment, backtesting, deficiency tracking, and remediation. Final delivery should include appropriate stakeholder engagement, change management, and staff education to ensure meaningful adoption.

**Recommendations:**

1. Determine the standards, processes, approvals, and other controls to be implemented, assess the company's current state and readiness, and develop a plan to implement an MRM program consistent with the company's risk profile.
2. Define a clear, actionable structure for tolerance threshold exceptions during validation and approval processes.
3. Maintain centralized templates and documentation guidance at all model life cycle stages.
4. Engage stakeholders in the design and delivery of the MRM program, and employ change management principles to ensure a successful rollout.

### 5.5. Inventory

Model inventories provide consistent identification and storage of models and analytical methods. The inventory process should involve identifying functional capabilities delivered to the organization via analytics and models. This includes vendor models, internally developed models, spreadsheets and EUCs, outsourced analytics and models, and legacy modeling processes. Model inventories should be supported by technology to enable secure storage and management of the inventory and related workflows.

**Recommendations:**

1. Model inventories should catalog models at all stages in the model lifecycle, including categories for models that are in development, deployed, and retired.
2. Inventories should capture relevant modeling metadata such as model identification, purpose, risk assessment, and business function alignment.
3. Inventory systems should store or link to current model documentation, including model development, validation, and implementation materials.

4. Inventories should capture and track findings identification, backtesting results, issue resolution, and model changes.
5. Traceability to model versions and residence should be included in inventory documentation.

### 5.6. Data

Model performance is dependent on underlying data accuracy, integrity, and applicability. Accordingly, an MRM program should define information requirements, master data strategy, data quality and remediation efforts, data quality KPIs, data monitoring and validation, and data aggregation. It is critical to understand the available data, processes for data traceability and data lineage, and controls in place to maintain data integrity.

**Recommendations**

1. Establish originating data sources and authoritative data sources for data inputs.
2. Develop processes and support technology to ensure accuracy when data originates from an unstructured source (e.g. document, flat file, etc.).
3. Create data lineage diagrams to steward the flow of critical data elements through sources, models, spreadsheets, EUCs, systems, reports, and other outputs.
4. Procedures and systems should be developed to test the integrity of data mapping and any stale, omitted, or egregious data outliers.
5. Employ Data Management Software, if applicable.

### 5.7. Vendor Models

Although companies may not have ideal insight into vendors' model life cycle processes, they should still apply model risk management principles to vendor models. Different vendors will offer varying levels of insight, so the extent of risk management practices may differ by vendor or model. At the very least, it is critical for companies to receive reasonable assurance that the model works as intended, train users, calibrate assumptions and inputs to current conditions, and comply with relevant IT controls.

**Recommendations**

1. Establish vendor due diligence process, including assessment of vendors' reputation, expertise, model life cycle capabilities, validation process, implementation plans, operational stability, and long-term service viability.
2. Establish vendor model selection process, including assessment of model need, functionality, fit-for-purpose, performance expectation, cost, data requirements, hardware requirements, compatibility with existing IT systems, and contractual requirements.

3. Embed reasonable model risk management requirements into procurement documentation, including performance guarantees, audit rights, reasonable model documentation, and the company's ownership of model outputs and related data.
4. Establish vendor model validation, system integration, and ongoing monitoring processes.
5. Document vendor models to the extent practical, provide model training to users and limit access to qualified individuals with a legitimate business need to use the vendor model.
6. Assign model ownership and include the vendor model on the company's model inventory.
7. Develop backup plans if the vendor model fails, including collaboration plans for vendor maintenance and replacement strategies if the vendor model needs replacement.

## 6. Conclusion

The value of a well-defined MRM program extends beyond regulatory compliance. The CCRO acknowledges and observes a paradigm where institutions look to MRM to drive value through reduced operational risk and higher overall value creation. Superior data quality, proper process controls, robust algorithms, advanced analytics, engaged oversight, and continuous improvement shall be the supporting forces.

The CCRO recognizes the challenges facing the industry and believes that an effective MRM program is essential for building, understanding, and developing trust in the new models needed for emerging areas and difficult markets. This paper provides an overview of the MRM framework along with recommended practices that the CCRO suggests its members consider for implementation. This document should be seen as a starting point in the continuous effort to enhance the energy industry's approach to model risk management, as well as a set of recommendations for companies to consider regarding the MRM framework best suited to their specific needs.

Lastly, the CCRO notes that there is no regulatory compulsion for model risk management in the energy industry as there is in banking. Similarly, there is no model risk standard that companies are beholden to. The recommendations in this white paper are explicitly for companies to review industry practice and determine which framework components and MRM activities best fit their own risk needs.


For more white papers, or if you are interested in learning how to become part of the Committee of Chief Risk Officers, please contact us:

p: 281-382-2538

e: info@ccro.org

w: www.ccro.org

**Committee of Chief Risk Officers**

8000 Research Forest Dr, 115-278

The Woodlands, TX 77382