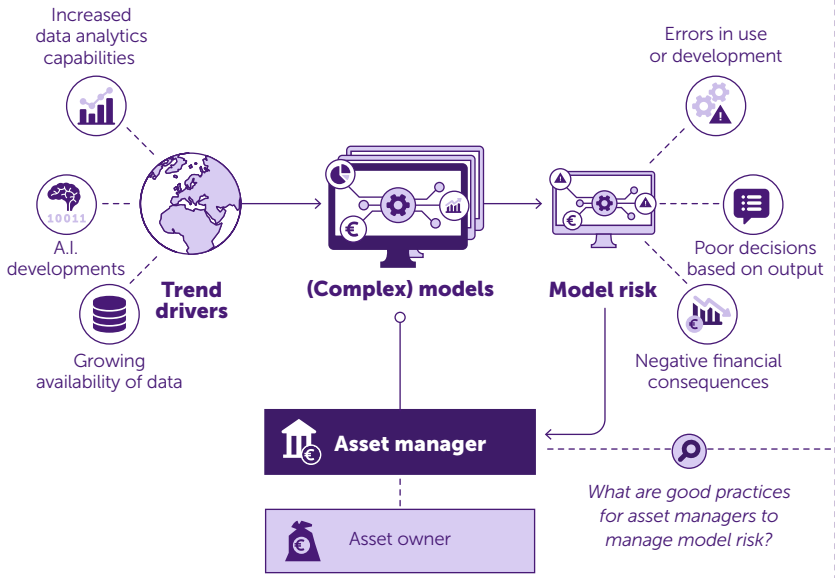
SUPERVISION VISUAL SUMMARY

Model risk management by asset managers

In short Technological developments and digitalisation are changing the asset management sector. Due to the growing availability of data and the added value of data analysis, asset managers are increasingly using models to support portfolio decisions and risk management. The development of new applications, such as artificial intelligence, also has consequences for the size and scope of these models. The increased use and complexity of models is likely to raise the asset manager's exposure to model risk. Managing risks, including model risk, remains important for asset managers. This report provides several good practices to support asset managers in strengthening their model risk management.

Asset managers are increasingly using (complex) models. This raises their exposure to model risk.



Asset managers must manage model risk where applicable. Model Risk Management involves identifying, assessing, managing, monitoring and reporting such risks.

8 Good Practices for Model Risk Management (MRM)

Governance
1 Establish a dedicated model governance structure covering model risk.
2 Implement a model definition to support common understanding.

Risk Management
3 Define Risk Appetite and Key Risk Indicators to support MRM.
4 Establish a model inventory as an integral component of MRM.

Model Lifecycle
5 Validate models before implementation and ensure periodic revalidation.
6 Adopt a lifecycle process for models.
7 Ensure similar responsibilities for internal and third-party models.

People
8 Maintain internal knowledge and expertise on models and model risk.

NOVEMBER 2025

AFM

Management summary

Asset managers increasingly use complex models to support a broad spectrum of activities, including day-to-day operations, investment strategy, risk management, portfolio construction and regulatory compliance. Drivers of this trend include the growing availability of data, increased data analytics capabilities and the adoption of machine learning/artificial intelligence techniques.

The increased use and complexity of models is likely to raise asset managers' exposure to model risk. In line with the requirements of the Financial Supervision Act (Wft)[1], asset managers must ensure sound and controlled business operations. To meet these requirements, asset managers are expected to manage the risks they encounter in their day-to-day operations, including model risk. Model risk can be managed and mitigated in various ways. Model risk management refers to the activities that are performed to identify, assess, manage, monitor and report on model risk.

In an exploratory study, the Dutch Authority for the Financial Markets (AFM) has gained insight into the way asset managers deal with model risk management (MRM) in practice. For the purpose of this study, and in the absence of an explicit definition within the asset management remit, the following definition of model risk is used as a reference for assessing implications for sound and controlled business operations: *the potential loss an institution may incur, as a consequence of decisions that could be principally based on the output of models, due to errors in the development, implementation or use of such models.*[2] This definition stems from prudential requirements that are not directly applicable to the population in scope of this study. It is solely used for reference purposes. In addition, prudential models are out of scope of this study.

The study explores four main themes: Governance, Risk management, Model lifecycle and People. For each theme, the AFM shares observations and good practices aimed at supporting asset managers in establishing processes, systems and internal controls to manage and mitigate model risk. These good practices have been drafted on the basis of the input obtained from the participating asset managers.

Key observations:

- Many asset managers recognize the importance of model risk management, but apply varying definitions and approaches.
- Governance around models is often arranged implicitly; clear role allocation and alignment with the Three Lines Model are considered good practice.
- Risk appetite regarding model risk is not often formally defined; establishing risk parameters and monitoring processes provides guidance.
- A central model inventory and independent validation are essential for maintaining control over the model portfolio.
- Third-party models require additional control measures within the existing MRM framework.
- Employee knowledge and awareness are crucial; targeted training and role-specific support enhance the effectiveness of model risk management.

1 Section 4:14 of the Financial Supervision Act (*Wet op het financieel toezicht, Wft*)

2 Article 3(1)(11) of Directive 2013/36/EU (CRD IV)

Introduction

The Dutch Authority for the Financial Markets (AFM) supervises compliance with the business operations requirements applicable to asset managers.[3] As part of their sound and controlled business operations, asset managers must ensure effective risk management practices, including in relation to the risks associated with models in use (model risk).

Stemming from this supervisory task, the AFM has gained insight into how asset managers manage model risks. Based on the results of the survey, certain good practices have emerged. Good practices are examples of how institutions can comply with legislative and regulatory requirements which, in the opinion of the AFM, provide a good interpretation of the relevant legal obligations. Good practices set out suggestions or recommendations; institutions are free to adopt a different approach, as long as they comply with the relevant laws and regulations and can demonstrate such compliance.

The purpose of this report is to share the good practices that have emerged from the survey amongst market participants. In this report, the AFM does not intend to be complete, either in observations or in proposed good practices, and both may vary in breadth and depth.

The insights resulting from the study on MRM were derived from a two-phased research approach. Phase 1 consisted of a market-wide, closed-ended survey distributed to Dutch investment firms, managers of UCITS, managers of AIFs, proprietary traders, trading venues and MiFID top-ups (collectively referred to as "asset managers"). 250 asset managers participated in Phase 1. Phase 2 involved a more in-depth open-ended questionnaire where input was sought from a sample of entities. 14 asset managers participated in Phase 2. They were selected on the basis of 'assets under management' (AuM) and 'dominant investment strategy', amongst other aspects, to arrive at a selection that was representative of the entire asset management sector.

The Dutch asset management sector comprises several large or very large asset managers alongside a substantial number of smaller entities. In recognition of the diversity of the Dutch asset management sector, in both size and complexity, the good practices presented in this report should be interpreted in proportion to the organisation's size, complexity and intensity of model use.

3 Section 4:14 of the Financial Supervision Act (*Wet op het financieel toezicht*)

Good practices

Good practice 1 - Establish a dedicated model governance structure covering model risk

Model governance refers to the set of policies, procedures and activities that formalise model responsibilities and decision-making within the organisation. A governance framework is considered to be dedicated to model risk when it includes risk management activities to identify, control and monitor model risk and establishes accountability and oversight of model risk.

Observations

Out of 250 participating entities, 86 asset managers (34%) indicated that they had established a dedicated model governance structure. Out of those 86 entities:

- Most firms stating that they have a dedicated model governance structure in place have assigned the roles of user, owner and developer. 51 firms (59%) have established the role of independent validator.
- 61 firms (71%) have organised governance and responsibilities with regard to risks of the models used within the organisation in line with the Three Lines Model.
- 46 firms with a model governance structure in place also have a dedicated model governance committee (55%). These firms tend to make extensive use of models and have multiple departments involved in the development, use and monitoring of models. Other entities have either defined a clear escalation path as an alternative to a model governance committee or have integrated model risk in existing committees.

Analysis

Strong governance, policies and controls in line with the complexity of the models used and the intensity of model usage within the organisation will support the effective understanding and management of model risks.

Good practice – Establish a dedicated model governance structure covering model risk

- Formalise responsibilities for development, implementation, maintenance, validation, change management and termination of models.
- Organise governance and responsibilities relating to model risk in line with the Three Lines Model.
- Depending on the intensity and complexity of model usage within the organisation, effective governance may require a dedicated model governance committee. For some entities, an escalation framework with clear procedures may be sufficient. Integrating model risk oversight into existing committees is also a possible alternative.

Good practice 2 - Implement a model definition to support common understanding

Since model risk can be defined in multiple ways and at various levels, a shared understanding is needed within the organisation about what qualifies as a model and what model risk encompasses.

Observations

Out of the 250 survey respondents, 72 organisations (29%) indicated that they had implemented a model definition. From the various model definitions provided by these respondents, it is noted that in general a model definition may include the following elements: (1) **input data**, (2) **a quantitative system or methodology** processing the input data and (3) **output** supporting or informing decision-making processes. Some organisations also opt to include an indication for "recurring use", which can help distinguish formal models from one-off or *ad hoc* tools that may fall outside the scope of model risk oversight.

Analysis
A formal and established model definition will support the effectiveness of model risk management and help determine the scope for the organisation's MRM framework.

Good practice – Implement a model definition to support common understanding
- Establish and formalise a definition of what constitutes a *model*.
- Document and communicate this model definition.
- Determine which types of tools or models fall within the scope of MRM.

Good practice 3 - Define risk appetite and risk indicators to support MRM

Defining the level of model risk the organisation is willing and able to accept by implementing a risk appetite for model risk supports model risk management. By substantiating the model risk appetite in terms of clear model risk limits – preferably through quantitative thresholds – and actively monitoring these limits, the organisation can monitor whether the model activities stay within the boundaries set by the risk appetite.

Observations
Out of the 250 survey respondents, 56 entities (22%) have defined a risk appetite for model risk as part of their risk appetite statement. 9 out of 14 asset managers that participated in phase 2 indicated that they had defined a risk appetite for model risk, as part of their organisation-wide risk appetite statement (RAS).

Organisations may choose to formulate model risk appetite as a standalone category, especially when model risk is significant or subject to specific regulatory scrutiny. Alternatively, model risk can be integrated into other risk categories such as operational or IT risk, treating it as a subset of those broader risk domains, including the accompanying risk appetite. In this way, model risk could be reflected as a separate key risk indicator (KRI) with accompanying risk limits under the defined risk appetite for that risk category.

Translating model risk appetite into measurable KRIs and monitoring these helps to track and manage identified risks. The study showed that where model risk appetite is defined, this was in some cases further specified into KRIs that are actively monitored. Examples of KRIs provided by respondents to the study include the number of models employed without validation, the number of reported deviations in model output and the frequency of overdue model reviews.

Analysis
By including model risk in the organisation's risk appetite and monitoring the risk appetite on the basis of defined risk limits (KRIs), unambiguous management of model risk within the organisation will be supported.

Good practice - Define risk appetite and key risk indicators (KRIs) to support MRM
- Define the organisation's model risk appetite.
- Translate the model risk appetite into KRIs.
- Set up a monitoring process for KRIs.
- Align controls and procedures with the model risk appetite and/or KRIs.
- Some entities aim to mitigate model risks through general enterprise, operational or IT risk management. To ensure effectiveness, model-specific governance elements could be included, such as assigning clear model ownership.

Good practice 4 - Establish a model inventory as an integral component of MRM

The organisation's model inventory is an overview of all models used within the organisation. A model inventory is a centralised repository that captures key model-specific information, such as ownership, user roles and version history. It may also include a risk classification of the model. In the context of this report, it is not a so-called digital place where all model documentation is stored.

Observations

The study revealed that out of the 250 participating entities 67 asset managers (27%) use a model inventory. In the second phase of the study, 6 out of 14 asset managers (43%) indicated that they had a model inventory in place.

Asset managers responding to the study appear to include the following elements in their model inventory:

- Model identifier (name or ID)
- Model purpose
- Owner
- Developer
- User
- Lifecycle status (e.g. active, under development, terminated)
- Risk classification/tiering (the risk associated with a model, often based on complexity and impact, as assessed by model owner and risk officer)
- Version
- Date of latest validation.

Depending on the organisation's use of models, model complexity and risk appetite, additional elements should be added to the model inventory:

- Language of the model (code)
- Location where the model is stored and operated
- An identifier for the business process supported by the model
- Complexity of the model
- Impact of the model
- Frequency of model employment
- An indicator of whether the model employs AI or ML techniques.

Analysis

A model inventory can be considered a cornerstone of an MRM framework. To be in control and ensure oversight and accountability, it is recommended that an organisation maintains a complete and accurate set of information in relation to the models it develops and employs.

Good practice – Establish a model inventory as an integral component of MRM

- Formalise a model inventory.
- Use the model inventory as the "central hub" of the organisation's MRM framework. Assign clear ownership and accountability, include risk classification and track lifecycle status to support effective oversight.
- Establish which elements are necessary features of the model inventory.

Good practice 5 - Validate models before implementation and ensure periodic revalidation

Model validation involves assessing models both before deployment and periodically during their use, to ensure they remain fit for purpose. The validation process is intended to offer an independent and objective view on whether a model works adequately and produces reliable results for its intended application.

Observations

The study revealed that model validation is sometimes interpreted as model review, whereas these activities serve different purposes. Model review is a broader and continuous process of assessing model performance, including adherence to policies. Model validation, on the other hand, is a specific test of model input and mechanics, providing assurance about the model's accuracy and reliability.

In the study, 58 respondents (23%) indicated that they had a model validation process in place. Of these 58 entities, 23 organisations (40%) only validate internal models, while 35 entities have a validation process in place for both internally developed models and models from external providers.

Entities included in phase 2 of the study provided details on the design of their model validation process. The validation process varies between entities, depending on factors such as model complexity, risk appetite and entity size. In general, when organisations have a formal model validation process in place, the following is observed:

- **The nature and frequency of the validation is determined on the basis of model risk classification.** Risk classification is used by multiple entities to decide how often and rigorously models are validated. High-risk models typically require mandatory and formal validation.

- **Validation of models before first-time use is standard practice; periodic validation is less common.** To ensure a model is working properly, it is typically validated before first-time deployment, even if no formal validation process is in place. Revalidation is less common, with frequencies ranging from annually to once every couple of years, based on the model's risk classification.

- **Independent validation may depend on firm size.** Larger entities often have an independent model validation function in place, while smaller entities sometimes organise model validation on the basis of the four-eyes principle or peer review. Model validation is typically carried out by independent personnel from inside the company, but external validators are also used.

Analysis
Organisations should have a model validation process to provide independent and effective challenge to model development and model use. Model validation can be considered one of the key components of risk mitigation throughout the model lifecycle and an important part of the asset manager's MRM. Model validation activities should be performed independently from the model developers and users, to provide robust and unbiased validation.

Good practice – Validate models before implementation and ensure periodic revalidation
- Formalise a model validation process.
- Validation before first deployment of the model is ensured. The nature and extent of revalidation may differ for models depending on risk classification or model tiering, as determined in the model inventory.
- Validation is performed by an individual who is independent of model development or model use.

Good practice 6 - Adopt a lifecycle process for models

The purpose of a model lifecycle process is to provide a structured framework for managing models throughout all stages of their lifespan - from initiation to retirement. A model lifecycle process helps ensure that models are developed, validated, implemented and monitored in a way that supports operational effectiveness, regulatory compliance and sound risk management. Each phase of the lifecycle involves distinct roles, responsibilities and governance standards.

Observations
Based on the study results, it is observed that 50 respondents (20%) have a model lifecycle process in place. From the survey results, the following illustrative examples (stages and roles) were noted that asset managers generally adopt in a model lifecycle process:
- **Initiation:** *Model owner* defines purpose and business need. *Risk management* reviews initial risk level.
- **Development:** *Model developer* builds and documents model. *IT/data* supports infrastructure and data sourcing.
- **Testing/validation:** *Model developer* tests the model to determine whether it is fit for purpose. *Model validator* independently tests and validates the model.

- **Go live decision:** *The responsible formal body or person* (as defined in the model governance set-up) decides on a formal go/no-go to start using the model in production.
- **Production/monitoring/maintenance:** *Model user* flags issues or unexpected results. *Model owner* tracks performance and usage. *Risk management* reviews ongoing risk exposure.
- **Termination:** Formal retirement decision mandated by *an executive model risk committee*. *Model owner* is responsible for follow-up on retirement. *IT/Data* removes model from system and data flows.

It is noted from the study that asset managers who have implemented a model lifecycle process typically include some form of initiation, development, validation and production stages. However, a termination phase or a process for changes and/or updates is not always provided for.

Analysis

Management of the model lifecycle aims to ensure that appropriate controls are in place to address model risk and support operational effectiveness and regulatory compliance. The model lifecycle includes the various stages of a model, from inception to termination. Model termination may be needed when a model is no longer performing as expected or supported by IT resources. Given the rapid evolution of data availability and model capabilities, structured change management and termination should be embedded in model lifecycle processes to ensure models remain current and secure.

Good practice – Adopt a lifecycle process for models

- Establish a model lifecycle process which includes each lifecycle stage – from initiation to termination – with clear roles, controls and documentation requirements for each phase.
- In view of developments in data and model capabilities, structured change management and a formal termination phase should be included in model lifecycle processes.

Good practice 7 - Establish MRM principles for both internal and third-party models

Asset managers may use models that are developed internally as well as models sourced from external parties. While third-party models can offer efficiency and specialised expertise, they may also introduce additional risks – such as challenges relating to oversight and concentration exposure. **Ultimately, the asset manager remains responsible for risk management and regulatory compliance, including when using models from third-party vendors.**
To understand how third-party model risks affect the organisation's risk profile, the members of the governing body (being ultimately accountable for maintaining effective oversight of the entity's exposure to third-party risks) should have appropriate skills and competence.

In addition, the entity is expected to have in place a robust third-party risk management framework, with sufficient attention to third-party model risk management where relevant. These expectations, amongst others, stem from the principles that ESMA has developed to address the observed increase in risks in the use of outsourcing, delegation and other third-party services by financial organisations.[4]

Observations

It was noted from the study that organisations mostly deal with internal and external third-party models in a similar manner in their overall approach to model use and risk management. With respect to governance, model lifecycle and risk management, respondents to the survey generally apply the same standards and procedures to models that are developed internally and those sourced externally.

Some respondents highlighted that the validation of third-party models presents challenges. As third-party providers do not provide access to all features of the models, it was noted from the survey that full model validation is not always feasible. In addition, due to limited access, model validation of third-party models may focus only on parameter settings instead of the underlying model code.

4 ESMA (2025). *Principles on Third-Party Risks Supervision*

Since asset managers remain responsible for the models and the outcomes of these models, respondents to the survey often also establish validation processes for third-party models but try to minimise the problem of limited access by adding responsibilities for the model owner. In such cases, the role of model owners goes beyond overseeing model use or model implementation; they are accountable for ensuring that external models are of adequate quality.

Analysis

When using models from third-party vendors, the knowledge and expertise relating to these models resides mainly with the vendor. To address the potential challenges to the asset manager's model risk management activities resulting from the use of these vendor models, the asset manager should be in close cooperation with the vendor. Despite the proprietary aspects of the vendor models, asset managers need assurance that the model is fit for purpose, e.g. based on sufficiently granular details captured in model documentation and data sources and on model testing and validation. Asset managers require vendor documentation showing the independent validation outcomes (if the validation is performed by the vendor) as well as the governance arrangements and process for model changes and performance monitoring. Including the vendor product in the asset manager's systematic procedures for model risk management and validation will help to understand the vendor model's capabilities, applicability and limitations. In addition, ensuring that third-party risk management principles for these models are up to par and that relevant controls are in place will support effective oversight of third-party model risk.

Good practice – Establish MRM principles for both internal and third-party models

- Ensure robust and effective third-party risk management practices in the organisation.
- Apply model risk management principles to manage and mitigate model risk when using third-party models from external vendors.
- Obtain sufficiently granular details of the vendor models and assurance that vendor models are appropriately validated.

Good practice 8 - Maintain internal knowledge and expertise of models and model risk

In addition to the modellers, personnel testing and critically analysing model risk management must have relevant knowledge to be able to perform their tasks effectively.

Observations

It was noted from the study that knowledge of models and model risk is mainly passed on through documentation or informally in staff meetings. Respondents indicated that they relied on the existing expertise of model developers and users.

The second phase of the study provided details of a variety of approaches to promote and maintain knowledge of models and model risk – including providing background documentation during onboarding, informal knowledge-sharing, lessons learned in staff meetings and more structured methods such as peer learning and formal training.

Analysis

In view of the ongoing rapid developments relating to data availability, data usage and model complexity, knowledge of models and model risk requires continuous attention. To ensure the MRM framework operates effectively, staff must be equipped with appropriate skills. Internal know-how and expertise can be encouraged and maintained through structured training, documentation and knowledge-sharing practices, thereby reducing the dependency on individual employees (key man risk).

Good practice – Maintain internal knowledge and expertise of models and model risk

- Ensure that internal knowledge and expertise relating to models and model risk is developed and maintained.
- Embed knowledge and expertise in sufficient parts of the organization to mitigate key man risk.

Next steps

The AFM expects asset managers to pay continuous attention to the requirements for controlled and sound business operations. This also includes adequate management of risks related to the development and use of models in business operations and investment decisions. The good practices resulting from the exploratory study can further support asset managers in establishing processes, systems and internal controls for model risk management.

In the upcoming period, the AFM will continue to focus on the various aspects of risk management by asset managers, including the risk management practices around the development and use of models.