Provisional Translation

Principles for Model Risk Management

November 12, 2021

Financial Services Agency of Japan

金融庁
Financial Services Agency

Contents

I. Objective

Financial institutions have been extending the use of models to support their decision making, driven by technological advances and increasing broadness and complexity in their activities. By presenting simplified representations of reality, models provide information that aid decision making in wide-ranging activities from business and risk management to compliance. A model, however, intrinsically entails a great deal of simplifications and assumptions. Modelling involves different possible choices of methodologies and assumptions, which could significantly alter the output of the model. Models may even contain fundamental errors or be used inappropriately, and changes in the environment may turn a once appropriate model into an obsolete one, resulting in the misuse of the model.

All of these give rise to the risk of inaccurate or misinformed decision making, consequently causing a potential material damage on a financial institution's earnings, financial positions, or reputation. As well as bringing about a potential merit in improving decision making, models present such risk (i.e., model risk) to financial institutions. Adverse consequences arising from a model could have far-reaching impacts beyond the financial institution using the model; they may even result in system-wide financial instability, for example, where the use of improper models could cause market-wide underestimation and accumulation of risk, ultimately followed by a sudden market reversal.

If problems arising from models were to affect regulatory reporting or inputs to supervisory decisions, the integrity of financial regulation and supervision could be seriously undermined. This is particularly relevant for capital and other regulations where financial institutions' internal models are used for determining their own requirements. The need for adequate controls on such internal models has long been recognized in the regulatory community: international standard setting bodies, such as the Basel Committee on Banking Supervision, and national supervisory authorities, including the Financial Services Agency (FSA), have been requiring the financial institutions to effectively manage the risk arising from the internal models in question, as a precondition for the use of the model for regulatory purposes.

However, given the extent to which models pose the risk of wide-ranging adverse consequences, financial institutions need to manage the risks stemming from all sorts of the models, regardless of whether the models are used for regulatory purposes. The need for comprehensive model risk management is gaining greater significance in light of the pervasive use of models in almost every aspect of financial institutions' activities. While models for previous decades have been extensively used in pricing/valuation of financial products and risk measurement (e.g., credit, market, and operational risk), more recently models have been finding their ways in broader areas. To name a few, provisioning, anti-money laundering (AML), fraud detection, and algorithmic trading are becoming increasingly model-based. Those models are often harnessing the technological advancements, such as increasing computational power and development in methodologies of machine learning and artificial intelligence.

The elevated uncertainty surrounding financial institutions has also heightened their need to manage model risk. Many of the models are designed to predict the future based on the past or estimate an unobservable object from what has been observed. The Covid-19 pandemic and the subsequent economic and market dislocation have reminded us of the fact that observed patterns in the past would not necessarily hold in the future, highlighting the nature of the risk intrinsic to models. Effective and proactive model risk management is the key to exploiting the opportunities provided by the technological advancements in the highly uncertain environment.

This document is intended to clarify the FSA's approach to model risk management, thereby catalyzing further development of the model risk management practices in the industry. The FSA is articulating its expectation as a list of principles rather than prescriptive rules, acknowledging the evolving nature of model risk management practice, while being mindful of the fact there would be no one-size-fits-all approach.

II. Scope and Application

1) Scope of a Financial Institution

This document is relevant to a financial institution with systemic importance, namely:

- G-SIBs (Global Systemically Important Banks) headquartered in Japan;
- D-SIBs (Domestic Systemically Important Banks) designated by the FSA; and
- Foreign G-SIBs' subsidiaries in Japan that have obtained approval from the FSA on the use of a model for regulatory purposes.

For the purpose of this document, these financial institutions are collectively referred to as "firms." Where warranted, the FSA may expand the scope of the application in the future.

2) Scope of a "Model"

Model risk management described in this document covers a broad range of models, without limiting its scope to particular model categories. For example, the scope of a model could include, but is not limited to, models used for pricing, risk quantification (credit risk, market risk, etc.), AML, and market surveillance. This document is based on the view that risk should be managed for all sorts of models, as long as the models present risk. It should also be noted that this document is not for the purpose of providing guidance on the management of a particular model, but for setting out a general framework to comprehensively manage the risk arising from any kind of models.

3) Application

In building and enhancing a model risk management framework, firms should establish appropriate prioritization. The build-up of a comprehensive model risk management framework requires substantial time and effort. Accordingly, firms may take roll-out approaches, such as starting from models that potentially present material risk or from areas of higher priorities in terms of effectiveness, followed by an expansion of the coverage. When adopting a roll-out approach, firms are expected to do so with an appropriate prioritization based on the potential risk of the model and their tolerance to model risk.

The FSA's supervision and monitoring of model risk management focuses more on the functioning of the model risk management framework as a whole, rather than checking compliance with each element of the principles in isolation. Firms may customize the practical application of the principles in a manner consistent with the risk profile, the extent of the model use, the complexity of the models used, and the overall risk management framework of the firm. Firms are expected not only to build a framework but also continue to ensure its effectiveness through engagements of the board of directors and the senior management.

III. Definition

For the purpose of this document, the terms "model" and "model risk" are defined as follows.

(a) Model

The term "model" refers to a quantitative process or a system of quantitative processes that apply theories and assumptions to process data into an output(s) such as estimates, forecasts, scores or classification. Models include a quantitative process whose inputs or outputs are wholly or partially qualitative or whose inputs are based on expert judgements.

(b) Model risk

The term "model risk" refers to the potential for adverse consequences resulting from misinformed decision making based on inappropriate or misused models. Model risk could result in deterioration in the prudential position, non-compliance with laws and regulations, or damages to the firm's franchise. Generally, model risk occurs because of: (1) inaccurate output resulting from fundamental errors of a model when viewed against its intended use; or (2) inappropriate use of a model, which includes the use of the model outside its intended use or beyond the model's limitation.

Uncertainty is a key characteristic of models. Whereas modelling involves various choices of methodologies and assumptions, the output of a model is highly sensitive to the choices made (i.e., uncertainty from modelling choices). Furthermore, the output of a model is an estimate of something

not directly observable, such as a forecast and parameter estimate, the nature of which inevitably entails uncertainty (i.e., uncertainty from the nature of an output). These uncertainties bring about the possibilities of erroneous decision making, thereby giving rise to model risk.

IV. Key Concepts of Model Risk Management

1) The Three Lines of Defense

A key to sound model risk management is to establish a framework to ensure effective review and challenge. This should be grounded on the risk culture that welcomes challenge, transparency of and healthy skepticism toward models, and efforts not to let models be "black boxes."

As in other risk management, different roles of model risk management can be classified into the *Three Lines of Defense* (the Three Lines Model) as the fundamental framework for ensuring an effective review and challenge. In a model risk management framework, the Three Lines of Defense could typically take the following forms:

- The first line of defense ("1LoD") consists of units or individuals who are responsible for the ownership of models or have a direct stake in model development or usage (e.g., model owners, model developers, and model users).
- The second line of defense ("2LoD") consists of units or individuals that control the model risk via review and challenge to the 1LoD. Their roles include, but are not limited to, the maintenance of the model risk management framework, the independent oversight of overall model risk and compliance with the firm's policies, and independent validation of models.
- The third line of defense ("3LoD") consists of internal audit functions that assess the overall effectiveness of the model risk management framework of the firm.

In presenting the principles for model risk management, this document puts an emphasis on the Three Lines of Defense as a way to promote effective review and challenge. Firms have various ways to design their organizational architecture in terms of the Three Lines of Defense and assign roles and responsibilities to each of the lines. There may also be cases where a complete separation of defense lines is not practicable. Regardless of the model risk management framework that firms adopt, they should consider how to ensure that an effective review and challenge takes place in their framework.

2) Model Life Cycle

Effective review and challenge should be ensured in every step of a *model life cycle*, a process along which models evolve through the passage of time – from identification of models to risk rating, development, use, change, and exit. For the purpose of illustration, this may take the following steps:

- A firm defines and identifies "models" – the scope of model risk management. Models are recorded in a comprehensive "model inventory," a set of information on all models the firm has identified.
- Each model is assessed for its risk and assigned a risk rating. Model risk ratings form the basis of the risk-based approach to model risk management and the key determinant of the level of controls for individual models (e.g., rigor and frequency of validation).
- In the development process, comprehensive model documents are developed. This is to ensure that methodologies, assumptions, and limitations of the model are sufficiently transparent to stakeholders.
- Prior to their official use, models are tested by the 1LoD and independently validated and approved by the 2LoD.
- After a model goes into use, the model undergoes ongoing monitoring by the 1LoD and revalidation by the 2LoD. These are carried out to evaluate whether the model is actually performing as intended. The 2LoD has the authority to restrict or reject the use of the model when material deficiencies are identified.
- When material changes are made to a model, additional validation is carried out on the model as needed.
- The 2LoD assesses the overall model risk of the firm. The results of model risk assessments are reported to the board of directors.
- The 3LoD, the internal audit function, assesses the overall effectiveness of the model risk management framework of the firm.
- All of the processes above are articulated in policies and procedures, and outputs are documented at each step.

3) Risk-Based Approach

The *risk-based approach* is essential for effective model risk management. For the purpose of this document, the risk-based approach refers to assessing the risk of models, managing and mitigating the risk informed by the assessment.

Where firms identify high risk for certain models, they should appropriately address and mitigate the risk as needed. If a model risk is identified as low, they may take actions accordingly. This will enable firms to efficiently allocate resources and effectively mitigate the model risk. The risk-based approach is not only

about individual models. Firms should also take into account the risk of models in the aggregate (e.g., interdependence of different models) in their model risk management and address the risk appropriately.

The risk-based approach should be aligned with the firm's tolerance for model risk. Firms should have a thorough understanding of their own model risk and mitigate the risk effectively to an acceptable level.

V. Principles for Model Risk Management

In building and implementing a model risk management framework, firms should have regard to the following principles:

Principle 1 – Governance. The board of directors and senior management should establish a framework of comprehensive model risk management.

1.1. Board of Directors and Senior Management Responsibilities

The board of directors and senior management should establish a robust framework of comprehensive model risk management, as part of the firm's overall risk management framework. The board of directors may delegate its responsibilities to execute and maintain a model risk management framework to senior management or relevant committees. In the same manner as for other risk stripes, the overall model risk and compliance with the policies should be periodically reported to the board of directors.

1.2. Model Risk Management Framework

The model risk management framework should be commensurate with the firm's characteristics, risk profile, nature of model risk, and tolerance for model risk. It should also be on a group-wide basis and an appropriate level of consistency should be sought across entities, regions and jurisdictions. The model risk management framework should also be built upon due consideration on sound industry practice and lessons learned from incidents of model risk management failure inside or outside the firm.

1.3. Policies and Procedures

Firms should set the policies and procedures to formalize the model risk management framework and activities. Policies and procedures should cover all aspects of model risk management, including model definition, roles and responsibilities, model inventory, model development, implementation, and model validation.

Firms should also document the results produced by each process in the model risk management activities. While the required level of documentation depends on the purpose of the document, they need to ensure that documentation is sufficiently detailed and granular in light of the purpose so that the necessary information is clearly communicated to the stakeholders.

1.4. Roles and Responsibilities

Firms should clearly articulate the roles and responsibilities of relevant stakeholders in model risk management. Whereas the roles and responsibilities vary depending on the model risk management framework of the firm, these should include: (i) ownership of models, and (ii) control of model risk by independent parties:

(i) For each model, a firm should designate a "model owner," a unit or an individual who is accountable for the use and performance of the model as part of the 1LoD.

(ii) The risk should be controlled by a "model risk management function(s)," the 2LoD functions responsible for the maintenance of the model risk management framework and the independent oversight of overall model risk and compliance with the firm's policies.

Principle 2 – Model Identification, model inventory, and model risk rating. Firms should identify models, record them in a model inventory, and assign a risk rating to each of the models.

2.1. Model Identification

Based on the definition set out in their model risk management framework, firms should identify "models" – the scope of model risk management. Typically, the 1LoD should be responsible for identification of models and the 2LoD should be responsible for assessment of a model and non-model.

2.2. Model Inventory

Firms should record information for models used, under development, or recently ceased to be used in a model inventory. The model inventory should be sufficiently comprehensive and should contain all the information necessary to support the model risk management activities of the firm. While each line of business, entity, and department may maintain its own inventory, firms should maintain a firm-wide inventory and the 2LoD is responsible for the firm-wide inventory management.

2.3. Model Risk Rating

Each model in the inventory should be assessed for its risk and assigned a risk rating. Risk ratings form the basis of the risk-based approach to model risk management and the key determinant of the level of controls for each of the models (e.g., rigor and frequency of validation). Whereas the

approach to risk ratings depends on the firm, the risk assessment of a model may take into account factors such as materiality, complexity, and usage of the model.

Principle 3 – Model development. Firms should have in place a sound model development process. Firms should adequately develop model documents and carry out model testing.

3.1. Model Development

Firms should have a model development process in place to ensure that a model is appropriate for the intended use, in terms of its conceptual soundness, and data quality and suitability for the model.

3.2. Model Document

In the model development process, the firms should develop a comprehensive model document. The methodologies, assumptions, limitations, and weaknesses underlying the model should be well documented so that each mechanism and feature of the model is transparent to the stakeholders. Model document should be sufficiently detailed so that independent parties with the relevant expertise (e.g., model validators) can understand how the model operates.

3.3. Model Testing

In the model development process, the 1LoD should carry out model testing before the official use of a model. Model testing should evaluate various components and the overall functioning of the model and assess potential limitations to determine whether the model is performing as intended. Results of model testing should also be appropriately documented.

Principle 4 – Model approval. Firms should have a robust process of model approval at various stages of a model lifecycle, e.g., at the inception, material changes, and revalidation of a model.

4.1. Model Approval

Prior to its official use and material changes of a model, the model should be subject to validation and internal approval by the 2LoD. Where a model undergoes revalidation, the model should be internally approved for continued use. A model approver should have the authority to grant a conditional approval (e.g., an approval with restriction on the use of the model) or reject the use of the model.

4.2. Exception to Model Approval

Firms may have a process for exception of model approval. Where a firm allows exceptions to use a model without model approval, this should be temporary and subject to rigorous control by the 2LoD. Such exceptions should be commensurate with the risk of the model.

Principle 5 – Ongoing monitoring. After a model goes into use, the model should undergo ongoing monitoring by the 1LoD to confirm that the model is performing as intended.

5.1. Ongoing Monitoring

Once a model goes into use, the model should undergo ongoing monitoring. Ongoing monitoring is typically conducted by the 1LoD and aims to confirm on a regular basis that the model is performing as intended.

While a firm verifies that a model performs as intended at inception, the model may subsequently experience deterioration in its performance, due to changes in products, business activities, market conditions or any other circumstances. Ongoing monitoring plays an essential part in evaluating if the obsolescence of a model has occurred and verifying if the model needs to be modified or decommissioned.

5.2. Approach to Ongoing Monitoring

The methods and other approaches of ongoing monitoring depend on the purpose, nature, and risk of a model. Firms should choose the appropriate approaches of ongoing monitoring to ensure its effectiveness. Ongoing monitoring should be a documented process: the approaches (e.g., the frequency and method) and results should be adequately documented.

Principle 6 – Model validation. As an integral element of review and challenge by the 2LoD, models should be subject to independent validation. This includes initial validation prior to use, validation of material model changes, and revalidation after a model goes into use.

6.1. Model Validation

Models should be subject to independent validation. Model validation checks the soundness of the model design and concept, appropriateness of the model usage, and the need for restrictions on the use of the model. The results of model validation should be adequately documented and considered as an input for model approval. The 2LoD should have the authority to require the 1LoD to take appropriate remedial actions (e.g., restriction on or suspension of the model use) when material deficiencies are identified.

6.2. Types of Model Validation

Model validation should take place at various stages of a model lifecycle. All models should undergo initial validation prior to their official use unless an exception set out in 4.2. is granted. Where material changes are made to a model, the 2LoD should consider the necessity of a validation. After models go into use, the models should be subject to revalidation to evaluate whether they are actually performing as intended.

6.3. Methods and Scope of Model Validation

The methods and scope of a model validation depend on the purpose, nature, and risk of the model, as well as the data availability and validation type. Firms should choose appropriate approaches of model validations to effectively challenge the model. Where applicable, the methods of validation should include outcomes analysis (a comparison of outputs with actual corresponding data—e.g., backtesting).

The scope of model validation should cover evaluation of both model designs and control activities by the 1LoD. This may include, but is not limited to, model documentation, methodology specification, assumption, data, developmental evidence, model implementation, model usage, and ongoing monitoring.

6.4. Independence of Model Validation

Firms should ensure a sufficient level of independence of those who undertake model validation from the 1LoD. Independence may be supported by separation of reporting lines and/or incentive structures. Whereas in some cases model validation may be carried out by the 1LoD, such validation work should be subject to a review by the 2LoD.

6.5. The Risk-Based Approach to Model Validation

The frequency, rigor, and scope of model validation should be commensurate with the risk of the model. In particular, the frequency and prioritization of revalidation should be consistent with the risk rating of a model, and firms should also take into account factors such as changes in the environment, deterioration in model performance, and restrictions of model usage.

As part of the risk-based approach, revalidation of low risk models may be carried out on a non-regular basis e.g., where there has been a material change in the environment or a sign of deterioration in model performance.

Principle 7 – Vendor products and use of external resources. Where firms use vendor products or external resources, the firms should have adequate controls in place over the use of those products and external resources.

7.1. Vendor Products

As many elements of vendor models and other third-party products (e.g., data and parameters used in a model) are often proprietary, firms are likely to have limited access to product information, such as the methodologies, assumptions, and data. Even with these constraints, the firms should manage and mitigate the associated risk to an acceptable level under their overall model risk management framework.

7.2. Risk Management of Vendor Products

The risk management of vendor models and other third party products involves approaches different from those for in-house models and products. Examples of such approaches include: selecting appropriate vendors and products; requesting vendors to provide information as detailed as possible so that the firm could have a better understanding of the model's limitations and assumptions; performing model validation based on the best available information; and developing contingency plans for cases in which vendor products are no longer available.

7.3. Use of External Resources

Where firms use external resources in executing certain activities of the model risk management (e.g., model validation and model review), they should be able to understand and evaluate the results of the activities performed by the external service provider. Due diligence and other control processes associated with outsourcing should be consistent with the firm's existing third-party risk management framework.

Principle 8 – Internal audit. As the 3LoD, internal audit functions should assess the overall effectiveness of the model risk management framework.

8.1. Roles of Internal Audit

Internal audit functions should independently evaluate and verify whether the model risk management framework and the practice are comprehensive, rigorous, and effective. As part of the firm's overall internal audit activities, findings from internal audit related to model risk management should be documented and reported to the board of directors or its relevant committees.