Provisional Translation

Principles for Model Risk Management

(Consultation Document)

June 25, 2021

Financial Services Agency

Contents

I. Objectives

As financial firms' businesses become ever broader and increasingly more complex, they have been extending the use of models in order to support their decision making. Models are representations of reality and hence entail a great deal of simplification and assumptions. By their nature, there are various approaches in modeling and the output of a model is heavily dependent on assumptions and theories used. Models may even contain fundamental errors or be used inappropriately. Changes in the environment may turn once appropriate models into obsolete ones, making their use inappropriate.

All of these give rise to the risk of inaccurate or misinformed decision making, causing material financial and reputational damages to firms. Risks associated with models also have the potential to cause systemic consequences. Market-wide underestimation of risk caused by improper models, for example, could lead to risk accumulating in the financial system, followed by a sudden adjustment of financial markets.

If problems arising from models were to affect regulatory reporting or inputs to supervisory decision making, the integrity of financial supervision and regulation could be seriously undermined. This is particularly relevant for capital and other regulations where firms' internal models are used as an input for determining their own requirements. This lies in the background to the fact that international standard setting bodies, such as the Basel Committee on Banking Supervision, and national supervisory authorities, including the Financial Services Agency (the "FSA"), have been requiring firms to put in place a framework to effectively manage the risk arising from the internal models in question, as a precondition for the use of the models for regulatory purposes.

Given the wide range of adverse consequences that could result from models, the risk should be managed for all sorts of models that present material risk, regardless of whether a model is of regulatory purposes. The need for comprehensive model risk management is growing further, in light of the pervasive use of models in almost every aspect of firms' activities. While for the past decades models have been extensively used in pricing/valuation of products and prudential risk measurement (e.g., credit, market, 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. Some of those models are harnessing the technological advancements, such as increasing computational power and the development in methodologies such as machine learning and artificial intelligence.

The elevated uncertainty surrounding firms has also heightened firms' need to manage model risk. Many of the models are designed to predict the future from 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 development 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. By doing so, the FSA seeks to avoid hindering future developments in the practices of model risk management, while being mindful of the fact there would be no one-size-fits-all approach.

II. Scope and Application

This document is relevant to firms with systemic importance and firms with a significant presence from the market integrity perspective, namely:

- G-SIBs (Global Systemically Important Banks) headquartered in Japan;
- D-SIBs (Domestic Systemically Important Banks) designated by the FSA;

- Foreign G-SIBs' subsidiaries in Japan that have obtained approval from the FSA on the use of prudential models for regulatory purposes; and
- Other firms with a significant presence from a market integrity perspective, such as those providing a significant volume of market access to high-speed trading investors.

Where warranted, the FSA may expand the scope of the application in the future.

The principles are intended to cover a broad range of models. These include, but are not limited to, pricing models, market and credit risk quantification models, and models for non-prudential purposes, such as models for AML and market surveillance. This is based on the view that the risk should be managed for all sorts of models, as long as the models present material risk.

In building and enhancing a model risk management framework, appropriate prioritization should be given reflecting the differences among firms and risk of models. Build-up of a comprehensive model risk management framework is expected to take years. In light of this, firms may take roll-out approaches, starting from models that potentially present material risk or from areas of higher priorities in terms of effectiveness, followed by 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 models and the firm's tolerance to model risk.

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

III. Definitions

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

(a) Model

"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 and whose inputs are based on expert judgements.

(b) Model risk

"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 a 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 use of the model outside its intended use or beyond the model's limitation.

IV. Key Concepts of Model Risk Management

1) The Three Lines of Defense

A key to sound model risk management is 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 stripes, the fundamental framework for ensuring effective review and challenge comprises the three lines of defense (the three lines model). In a model risk management framework, the three lines of defense could take the following form:

- 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.

There are various ways of designing an organizational architecture of the three lines of defense and assigning the 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 a firm adopts, the firm should consider how to ensure that effective review and challenge take place in the framework.

2) Model Life Cycle

Effective review and challenge should be ensured in every step of a "model lifecycle," 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. Risk ratings form the basis of the risk-based approach to model risk management and are the key determinant of the level of controls of a model (e.g., rigor and frequency of validation).
- In the development process, comprehensive model documents are developed. This is to ensure that mechanisms, assumptions, and limitations of the model are well communicated 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 the use of the model if 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 an essential foundation of model risk management. Firms should assess the risk of models and manage and mitigate the risk informed by the assessment. Where firms identify high risk for certain models, they should appropriately address and mitigate the risk as needed. Where firms identify low risk, 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 coupled with the firm's tolerance to model risk. Firms should have comfort in the level and nature of model risk of the firm 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 ("Principles"):

Principle 1 – Governance. The board of directors and senior management should establish a robust 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 consistent with the Principles and commensurate with the firm's risk profile 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 practices in the industry and lessons learned from incidents of model risk management failure in the firm or in the industry.

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 definitions, roles and responsibilities, model inventories, model development, implementation, and model validation. Firms should also document the outputs of the model risk management activities.

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 and their allocation 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, firms 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 models and non-models.

2.2. Model Inventory

Firms should record information on models used, models under development, and models recently ceased to be used in a model inventory. A model inventory should be sufficiently comprehensive and should contain all the information necessary to support the model risk management activities of the firm. Whereas each line of business or department may manage their model inventory, firms should manage the group-wide model inventory and its responsibility resides in the 2LoD.

2.3. 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 are the key determinant of the level of controls (e.g., rigor and frequency of validation). Whereas the approach to risk ratings depends on firms, 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 sound model development process. Firms should adequately develop model documents and carry out model testing.

3.1. Model Development

In the model development process, firms should ensure that models are conceptually sound and the quality and relevance of data is suitable for the purpose of the models. Firms should develop comprehensive model documents so that model uncertainties and limitations are clearly communicated to stakeholders.

3.2. Model Document

Model documents should describe methodologies, assumptions, and limitations of the model and should be sufficiently detailed and comprehensive so that independent parties with relevant expertise (e.g., validators) can understand the functioning of the model.

3.3. Model Testing

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.

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 and to assess whether any changes in products, activities, market conditions and other factors necessitate adjustment or replacement of the model.

5.2. Approach to Ongoing Monitoring

The methods and other approaches of ongoing monitoring depend on the purpose, nature, and risk of models. Firms should choose the appropriate approaches of ongoing monitoring to ensure effectiveness. Ongoing monitoring should be a documented process: the frequency, methods, and other approaches 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 model usage, and limitations of models. 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 remediating actions (e.g., restrictions on the use of the models) 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 validation. After models go into use, the models should be subject to revalidation to evaluate whether the models are actually performing as intended.

6.3. Methods and Scope of Model Validation

The methods and scope of model validation depend on the purpose, nature, and risk of the model, as well as data availability and the stages of the model life cycle at which validation is conducted. Firms should choose the appropriate approaches of model validation to effectively carry out review of and provide a challenge to the model. Where applicable, the methods of validation should include outcomes analysis (comparison of outputs with corresponding actual data; e.g., backtesting). The scope of model validation should cover the evaluation of model designs and control activities by the 1LoD, which may include, but are not limited to, model documentation, methodology specification, assumptions, 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. Risk-Based Approach to Model Validation

The rigor, scope and other features of model validation should be commensurate with the risk of the model. In particular, the frequencies and prioritization of revalidation should be consistent with the risk rating of models, and should take into account factors such as changes in the business environment, deterioration of model performance, and model limitations. For low risk models, revalidation 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 has been observed.

Principle 7 – Vendor products and use of external resources. Where firms use vendor products or external resources, the firms should have in place adequate controls 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 information on methodologies, assumption, data, and control process of the products. Even with these constraints, firms should manage and mitigate the associated risk to an acceptable level, in a manner consistent with the firm's overall model risk management framework.

7.2. Risk Management of Vendor Products

Risk management of vendor models and other third party products involves approaches different from those for in-house models and products. Such approaches include, but are not limited to, selecting appropriate vendors and products, requesting vendors to provide necessary information, performing model validation based on available information, and contingency planning in case 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), the firms should be able to understand and evaluate the results of the activities performed by the external service

providers. Due diligence and other control processes associated with outsourcing should be consistent with the firms' 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 practices 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.

Published XXX, 2021