Guideline

Title	Enterprise-Wide Model Risk Management for Deposit-Taking Institutions - Guideline (2017)
Category	Sound Business and Financial Practices
Date	September 30, 2017
Sector	Banks Trust and Loan Companies
No	E-23

Table of Contents

This Guideline outlines OSFI's expectations around institutions' establishment of sound policies and practices for an enterprise-wide model risk management framework. It applies to banks, bank holding companies, federally regulated trust and loan companies and cooperative retail associations, and collectively referred to as 'institutions'.

1. Introduction

This Guideline outlines OSFI's expectations for the establishment of an enterprise-wide model risk management framework at institutions. Taking an enterprise-wide view of risk implies that these principles should be appropriately applied across the entire spectrum [1] of models used by institutions for risk management purposes. It is an institution's responsibility to develop a consistent set of policies and/or procedures in order to identify, assess, manage and control the risks inherent in any model – as defined in Section 2 [2] .

OSFI recognizes that large complex institutions with internal models approved for regulatory capital purposes already have the necessary risk control infrastructure in place, whereas others might apply controls only in materially relevant areas. As a result, this Guideline should be interpreted in the context of a proportionality principle whereby applicability is commensurate with the nature, size, complexity, and risk profile of the institution.

OSFI will distinguish between internal models approved institutions (IMAIs) and other standardized institutions (SIs). The dividing line will be contingent on whether or not the institution has received OSFI approval to use an internal model for regulatory capital purposes. If approval has been granted then the institution is considered to be among the IMAI cohort; otherwise it will be treated as an SI.

- **IMAIs** should comply with all components of this Guideline including relevant sections of Appendix A, which provides references to additional model risk management requirements for credit risk, operational risk, market risk and 'Pillar II components' (i.e., Internal Capital Adequacy Assessment Processes (ICAAP) and interest rate risk in the banking book (IRRBB)) and Margin Requirements.

- **SIs** should strive to comply with this Guideline but OSFI's minimum expectations are that the institution:
    - Provide an inventory to OSFI of all models (not just capital models) that are in use (as described in Section 9),
    - Identify and assess the most material models from a model risk perspective (as described in Section 4.1)
    - Comply with governance and control requirements noted in Appendix A with respect to the Pillar II components and margin requirements (referenced in Section 5.5 but broadly applicable to all facets of Section 5 and the use of vendor models in Section 6.).

2. Definitions

Model – A model generally refers to a methodology, system, and/or approach that applies theoretical and (expert) judgmental assumptions and statistical techniques to process input data in order to generate quantitative estimates. A model has three distinct components: i) a data input component that may also include relevant assumptions; ii) a processing component that translates the inputs into estimates; and iii) a result component that presents these estimates in a format that is useful and meaningful to business lines and control functions.

Model risk – The risk of adverse financial (e.g., capital, losses, revenue) and reputational consequences arising from the design, development, implementation and/or use of a model. It can originate from, among other things, inappropriate specification; incorrect parameter estimates; flawed hypotheses and/or assumptions; mathematical computation errors; inaccurate, inappropriate or incomplete data; inappropriate, improper or unintended usage; and inadequate monitoring and/or controls.

Model user – The unit(s)/individual(s) that relies on the model's outputs as a basis for making business decisions. While model users may be involved in the early stages of model development and ongoing monitoring activities, this involvement is no substitution for independent and objective review.

Model developer – The unit(s)/individual(s) responsible for designing, developing, evaluating and documenting models which may also perform ongoing monitoring and outcomes analysis as well as periodic reassessment once a model is in use.

Model owner – The unit(s)/individual(s) responsible for the model selection, coordinating model development, initial testing, ongoing monitoring, outcomes analysis, administering changes and documentation. The model owner could also be the model developer or user.

Model reviewer – The independent unit(s) responsible for model vetting, validation, [3] , [4] and reporting its findings and recommendations to the model approver. Other responsibilities might include providing the model developer and user with guidance on the appropriateness of models for defined purpose.

Model approver – The individual(s) and/or committee(s) responsible for assessing the model reviewer's findings and recommendations and approving the use and/or limitation of use of any new model or changes to pre-existing models. Depending on the size and complexity of the institution,along with the materiality of the model being reviewed, it may be acceptable for the roles of model reviewer and approver to be combined as long as there is no potential conflict of interest and independence is maintained. For the purposes of this guideline, the terms 'model risk committee' and 'model approver' are used interchangeably.

3. Scope and Key Characteristics

This model risk guideline takes an enterprise-wide view that describes common policies and processes applicable to any model that could materially impact the risk profile of an institution. At minimum, this includes all models approved for use in the calculation of inputs to regulatory capital models used for institutions' internal assessments of risk.

Institutions should have model risk management frameworks that exhibit each of the following key characteristics, which are elaborated on in the subsequent sections:

- Appropriate and commensurate governance systems over model usage.
- Model materiality classifications and limitations, where appropriate, over the use of individual models.
- Policies and processes around model selection and development.
- Independent vetting and ongoing validation/review processes that continually assess the model's performance and suitability. [5]
- Change control processes governing each stage of the model's life cycle.

- Internal audit functions to independently assess the model risk management governance and compliance framework.
- A model inventory that catalogues the type, classification and performance of all models in use, or that have been developed, and approved for use, or recently decommissioned that could act as a benchmark or necessary substitute for a model in use.

4. Model Risk Framework

Given the importance of models, the governance structure surrounding their use should be aligned, as appropriate, within an institution's broader corporate governance framework. [6] To this end, model risk management begins with a sound governance framework consisting of policies and procedures that identify all relevant stakeholders along with the necessary processes and controls to ensure compliance with this guideline. These policies and/or procedures should encompass each stage of a model's life cycle, including: model development, validation, approval, review, modification and decommission. These policies and/or procedures should identify relevant model stakeholders and articulate their roles, responsibilities and authorities in identifying, assessing, managing and reporting model risk within the institution.

Enterprise-wide model risk management policies should be developed and operationalized by Senior Management. Institutions should clearly specify which individuals are responsible for this policy and describe their requirements to develop and promote it.

Ownership of each in-use model should be clearly assigned to an individual and/or team, which may be either a business line or housed within a risk management function. Institutions should develop a process that enables a model owner to manage the model's evolution from inception to decommission, in an increasingly rigorous manner commensurate with its materiality. Model owners should be responsible for maintaining thorough documentation – that is easily accessible to all model stakeholders – at each stage of a model's life cycle. This documentation should be itemized in the model inventory maintained by the institution (see example in Section 9).

For IMAIs, an independent [7] model reviewer should be responsible for the initial model vetting and ongoing validation. In addition, the reviewer might provide recommendations on approvals, enhancements, and any other

limitations on usage. The model reviewer should have the requisite quantitative skills to conduct a model review but, ideally, the demonstrated expertise in the business area for which the model is being designed. During pre-approval vetting or post-approval validation processes, the model reviewer can provide feedback to the model owner but it should separately report its findings and recommendations directly to a model approver function. For SIs the model reviewer could also act as the model approver provided it remains independent from the model owners/users.

In order to ensure effective control over model risk it is important that the governance structure vests internal approval and oversight authority primarily with parties who are independent from individuals with a direct stake (such as revenue generating functions or business line management) in the model's approval.

4.1 Model risk materiality

Senior Management should implement an appropriate model risk materiality classification scheme applicable to the relevant models. Its design and approval should be integrated with the governance structure for model approval. Size and complexity of model inventories may require, as appropriate, separate governance structures.

For IMAIs, this classification scheme should be consistent with model modification materiality definitions as described in Section 5.6. Ideally, an institution should design a system that is capable of ranking the level of risk posed by each of the models used, which provides the basis for prioritizing model reviews and scheduling ongoing validation work. Depending on the sophistication of the institution, this system should include both quantitative and qualitative aspects. [8]

For SIs, model risk materiality assessments should, at a minimum, identify material models that pose the most significant risks to the institution.

Model risk materiality assessments should be periodically reviewed by all institutions and updated as appropriate based on experience. In the latter case, institutions should establish triggers that mandate the re-assessment of a model's materiality and/or the imposition of limitations on usage. [9]

5. The model management cycle

Increasingly sophisticated institutions should be striving towards a consistent enterprise-wide process for choosing, developing, reviewing, approving and monitoring each of its material models. OSFI believes this resembles a life cycle process (i.e., a perpetual activity that is continually refurbished and updated as the model evolves with the passage of time) that considers a series of phases such as i) the rationale for modeling; ii) model development; iii) independent review (vetting); iv) model approval; v) ongoing monitoring and review (validation); and vi) modification / decommission. Institutions should ensure that each stage of a model's life cycle is addressed by the model risk policy and adequately documented. OSFI expects IMAIs to adhere to all elements of the model life-cycle while SIs must use appropriate measures, as suggested in Section 5.5, to determine their most material models and broadly apply, where relevant, to Pillar II components and margin requirements. Additional considerations that should be taken into account in each phase are provided below.

5.1 Rationale for modeling

Prior to model development, the relevant first line of defence business area (e.g., model users) should identify an economic or business rationale for developing a new model and/or the need to change an existing model. Institutions should ensure that model owners that have been assigned the production task have the necessary training and/or experience in the relevant areas under consideration for model construction. Model owners should identify and understand the proposed purpose of the model and ensure that modelling choices are documented and evidence is provided on the suitability of the selection for the proposed purpose. This proof should include, for example, a comparison with other candidate models where appropriate, including ones previously considered or already used for the same purpose.

5.2 Model development

IMAIs should have development processes for model owners to follow once the model choice has been made. The intent is to implement a model that can accurately quantify the desired measures and report them back to the model users. The development process is a first line of defence activity and should consider items such as:

- the determination of suitable data, and of critical assumptions and the quantification of key parameters;

- the determination of the methodology used to arrive at desired outputs and preliminary measures of performance;
- programming of the necessary code for measurement; and
- devising the formatting of outputs in a manner so that model users can effectively make proper business decisions and model owners can monitor ongoing model performance.

Documentation is a necessary ingredient in the model development process. It ensures that other parties can understand the model, implement it and construct suitable benchmarks for comparison. In addition, it makes the model risk management process more transparent to third party reviewers. Finally, it ensures the preservation of knowledge at the institution as model users and owners change over time, which is essential for business continuity.

Documentation related to the model development process should be comprehensive and address the modelling techniques adopted, any assumptions and approximations employed (including justifications and/or reasonability assessments for all key assumptions, covering both judgmental and qualitative aspects), the data sources and data proxies utilized, and any relevant model weaknesses and limitations.

5.3 Independent review (vetting)

Independent review is a critical component of the model lifecycle. IMAIs should have independent model vetting processes in place as a second line of defence to check whether models are sound and fit for their intended purpose. Independent review should include, at a minimum, the following features:

Verification and assessment: this includes checking that all documentation is up to date and available for third party review; reviewing the model owner's model selection decision relative to other possible candidates; and, evaluating the three components – inputs, computation processes, and reporting processes [10] – of the development process.

Secondary review: this includes an appraisal of conceptual soundness and model performance against criteria for success that is reflective of model purpose and product scope. The process may involve evaluation against alternative benchmark models, where appropriate, that assess the accuracy of the model; and, sensitivity testing in

order to assess the model's predictive capacity over a range of assumptions to identify weaknesses and limitations.

The results from this model review/vetting process should be documented, made available to all model stakeholders, and should form the basis for approval recommendations along with any conditions on usage that reflect identified model weaknesses and limitations. In this process, the model reviewer should remain objective and well informed but should not direct or engage in model development so as to ensure the principle of independent effective challenge is preserved. Where appropriate, internal audit may be involved in the review of the vetting work as a third line of defence and provide a positive opinion prior to approval.

5.4 Approval

Models used for regulatory capital inputs or internal risk assessment and control and related valuations should not, unless an exception has been granted and documented, be approved for operational use without first undergoing an independent review.

IMAIs should have a dedicated model risk committee(s) or a model approver(s) for the purpose of approving for use new models along with any material model modifications. The model reviewer is responsible for providing to the model risk committee or approver its vetting, validation and review report along with an initial recommendation on the model approval petition, as applicable. If there are identified weaknesses or limitations, the model could be recommended for conditional approval provided that compensating mitigations are in place. That being said, conservatism in assumptions should not be a substitute for fundamental analysis and should be balanced against model accuracy where appropriate. For instance, pricing and provisioning models should prioritize accuracy. Institutions should have policies that articulate their use of conservatism in models and, where appropriate, overlays on model outputs.

5.5 Ongoing monitoring and review (validation)

Once the model has been approved, ongoing monitoring becomes a joint responsibility of model users, owners and validators. Model owners, users, or where appropriate, other first line stakeholders have the initial responsibility for monitoring. Models should be subject to a periodic review with a frequency that is consistent with their model risk materiality assessments. This is an important part of model risk mitigation since, with the passage of time, multiple

aspects (e.g., changes to markets; regulations; theoretical advancements; and financial institution policies) can alter the inherent level of model risk. At a minimum, reviews should occur annually for models that exhibit the highest degree of model risk (see Section 4.1). Alternatively a review might be initiated in instances where there has been a material change in a model's scope, assumptions, methodology, and exposure or exception history.

Model owners (and other first line process stakeholders) and validation (as a second line process) should, during model review, consider a re-assessment of the quality of the model design and its construction. This process should consider, but is not limited to, items such as:

- reaffirming the completeness of existing documentation;
- revisiting the assumptions and data chosen as well as the effects of any modifications;
- benchmarking analysis, and
- re-examining any noted model limitations or documented weaknesses.

For models, whose deficiencies have the greatest potential to generate immediate and material losses, both IMAIs and SIs (in the context of Pillar II components and margin requirements) are expected to use various measures, such as backtesting, discriminatory analysis, stress-testing, sensitivity analysis, etc., in their ongoing validation and review process. Institutions should have clear guidelines for determining a maximum tolerance on performance exceptions whereby once that threshold is breached, an exception event is considered to have occurred, which should trigger an escalation process.

Exceptions and Escalations

For models that pose material levels of model risk, institutions should have policies and processes in place to manage model exceptions. [11] Further, institutions should have escalation processes in place so that the model risk committee and/or Senior Management are promptly made aware of a model exception. Policies and/or procedures should specify notification and reporting responsibilities of the model owner and reviewer in an exception event. Upon escalation, the oversight authority should have the power to impose restrictions on the model's usage. Institutions should have an established policy dictating circumstances that merit the removal of the model or imposing conditions that limits model usage. Under limited circumstances, and for a limited time period, the model could continue to be used provided the model owner has a documented and approved plan to remedy

the exception situation with clearly defined constraints on use, proposed actions and assessment milestones in the interim. Internal audit should maintain an ongoing review of the exception and escalation process and performance to ensure it is being conducted in a manner that is consistent with established policy.

5.6 Modifications and decommission

The process around model modifications and the deactivation of models due to poor performance or obsolescence is an important component of an institution's model risk policy. All institutions should maintain a holistic process that articulates what constitutes a material [12] model modification. [13], [14] When such a modification is undertaken, institutions should apply the same level of rigour in vetting and validation as is involved with a new model approval. If the model modification is not considered to be material, the model owner should still document the scope and details of the change along with any implications for the model's performance. No individuals should have the authority to change a model or model use without re-approval of the changed model or use, which may be by a summary process for immaterial changes.

Institutions should establish a process for managing and documenting material model modifications. This process should consider, for example: a series of controls governing authorizations to change model components; a record of validation sign-offs since model inception on a go-forward basis; and a record of empirical test results to assess whether or not model results have changed. Such a process should identify the personnel or authority that can change and or modify the model. The change control function and validation record prevents a divergence between the approved model and the one used in operation. This provides an efficient mechanism for prioritizing ongoing validation work, whether ex-ante or ex-post depending on materiality, after events such as systems upgrades, which tend to affect numerous models simultaneously.

The decommissioning of a model should not be considered the end of the model risk lifecycle as there is an expectation that a new model will replace the decommissioned one. A decommissioned model could, however, act as a benchmark or might need to be re-commissioned if the new model fails to be implemented properly or perform up to minimum risk tolerances.

Institutions should have policies and/or procedures in place for decommissioning models, which includes notifying relevant stakeholders of the upcoming event. In addition, there should be transitional arrangements available to

govern situations when there is a timing gap between the inception of the new model and expiration of the old. Institutions should have a policy for the length of time it will continue to maintain the old model's information in its model inventory system and a record of which model it is replaced by.

6. Vendor products

Institutions might wish to rely on third-party vendor sources for models or data, where it is understood this information might be proprietary. Aside from outsourcing the model development phase, adopting a vendor product does not eliminate the need to apply a similar process for vetting, approval, ongoing validation, decommissioning and overall documentation, as would be conducted for in-house developed models and data sources. Institutions should have ultimate accountability for all outsourced activities [15] and should seek access from the vendor to adequate technical documentation related to the model to understand how the model is designed, calibrated and operating, as would be expected for an internally developed model. IMAIs must demonstrate to OSFI's satisfaction that there are conditions surrounding the vendor's proprietary intellectual property that inhibit their access to documentation. Institutions should establish policies and/or procedures, with clearly specified authorizations, around the selection, ongoing monitoring and retention of vendor models. Institutions should develop contingency plans for material models that consider the event where the vendor product is inadequately supported.

7. Models of Foreign Bank Subsidiaries

OSFI expects all foreign bank subsidiaries to comply with the scope requirements established in Section 1. That is, all should maintain an inventory of models, identify and assess material sources of model risk, and comply with Pillar II components and margin requirements noted in Appendix A. If a foreign bank subsidiary relies on models which are approved for use by their parent institution, it must demonstrate that, where material, such models are fit for intended purpose within their model risk management processes. The level of process required should be interpreted in the context of a proportionality principle whereby the level expected is commensurate with the nature, size, complexity, and risk profile of the foreign bank subsidiary in Canada, subject to the minimum expectations noted above.

The concept of materiality of a model will differ when applied to the foreign bank subsidiary on a standalone basis. This implies that material models, including those beyond regulatory capital usage, may require as much rigour at all stages beyond the model development stage as models developed locally and in-house. A foreign bank subsidiary should have access to technical documentation from its parent in order to assess and manage model risk unique to its risk profile. Before receiving permission to use their parents' models for regulatory capital purposes, IMAI foreign bank subsidiaries should first demonstrate to OSFI a minimum level of competence and compliance with the relevant requirements outlined in Appendix A.

8. Internal Audit

Internal audit, as the third line of defence, should assess the overall effectiveness and adequacy of the model risk policy, in general, and determine compliance by the various stakeholders with that policy. This assessment should be undertaken by individuals that are independent of model development, validation or use. For all institutions, internal audit should determine:

- *Policy existence:* confirm there are model approval, modification and decommission processes and there is an adequate process around model risk materiality; and, that authorizations around the model change control process are clearly specified.
- *Policy adherence:* assess whether validation work conducted by model reviewers is sufficiently independent and occurring on schedule; and confirm that the exception and escalation record are consistent with stated policies and/or procedures.
- *Documentation:* perform a check for consistency and completeness in documentation and reporting including the model inventory records.

Institutions are ultimately responsible to manage model risk but can, when appropriate and necessary, use an independent external service as a resource with the expertise and objectivity to assess the model risk management process including the review by internal audit. This may include outsourcing of validation work and performing aspects of the internal audit function on model risk assessment, provided the institution's governance controls and processes are in place and effective.

9. Model inventory

Institutions should maintain a catalogue of models since inception in order to be able to identify, understand and track the performance, risks and limitations associated with each and affirm that a model is used for its original purpose. As such, OSFI expects IMAIs and SIs to maintain an up-to-date inventory of all models in use and recently decommissioned. All institutions should establish a list of individuals within the institution that have the sole authority to control and maintain a centralized model inventory. The model inventory should be made available upon request by OSFI and should have the following components on a model-by-model basis, where applicable:

- Model name and description of key features.
- Model risk ranking andmateriality assessment.
- Identification of the model owner and/or developer.
- References to the type and sources of data used by the model.
- Which products and business lines that the model is approved for use.
- References to vetting and validation reports including an itemization of deficiencies and limitations.
- Date of inception, approval for use and exception history.
- Detailed summary of material model modifications.
- References to outcomes analysis (e.g., backtesting results).
- References to internal audit findings as they pertain to the model.

Appendix A. Model risk management requirements referenced in OSFI Guidelines

OSFI expects institutions to comply with model risk guidance expectations referenced in other OSFI guidelines. This Appendix provides institutions with a set of references to OSFI guidelines, broken out into those specific to particular Pillar I and Pillar II internal capital models and those related to margin requirements and accounting models. Note that the Pillar II internal capital model pertains to both IMAIs and SIs.

1. Credit risk
    - Internal Ratings Based approaches (IRB)
        - Capital Adequacy Requirements (CAR) Chapter 6

        - Implementation Note: Approval of Regulatory Capital Models for DTIs (i.e. materiality considerations)
        - Implementation Note: Risk Quantification at IRB institutions
        - Implementation Note: Validating Risk Rating Systems at IRB Banks (i.e. validation issues)
    - Supervisory Formula Approach (SFA) for securitisations (CAR Chapter 7)
    - Counterparty credit risk and Credit Valuation Adjustments (CVA) (CAR Chapter 4 – Settlement and Counterparty Risk)
2. Operational risk (CAR Chapter 8)
    - General requirement for rigorous procedures for operational risk model development and independent model validation (paragraph 48)
    - Requirements for the use of internal data, and required validation (paragraphs 58, 59, 60, 61)
    - Requirements for the use of external data, and required validation (paragraph 62)
    - Expectations related to the use of scenario analysis (paragraph 63)
    - Expectations related to the use of business environment and internal control factors (paragraph 64)
3. Market risk (CAR Chapter 9)
    - Standardized – Options Scenario based approach (paragraph 172 states that institutions using the scenario method should meet the appropriate qualitative standards set forth in the section on the internal models approach.).
    - VaR and stressed VaR – Section 9.11.2 summarizes minimum qualitative standards that OSFI expects institutions to meet before they are permitted to use a models-based approach. Section 9.11.3 provides guidance in specifying a minimum set of risk factors for internal models. Section 9.11.4 specifies the minimum quantitative standards for internal models and stressed VaR. Section 9.11.7 describes OSFI's expectations for stress testing programs for internal VaR models. Section 9.11.8 describes the expectations around validation processes for the internal VaR model.
    - Specific risk VaR – Section 9.11.5.1 describes minimum requirements of specific risk VaR models. Section 9.11.6 specifies the backtesting requirements for specific risk VaR models.
    - Incremental risk charge (IRC) – Appendix 9-9 describes the IRC charge. Section II.B outlines the key supervisory parameters for computing the IRC. Section III specifies validation requirements.

- Comprehensive risk charge – Section 9.11.5.2 describes the minimum model requirements for a comprehensive risk measure model for correlation trading portfolios. Appendix 9-10 provides stress testing guidance for correlation trading portfolio comprehensive risk measures.

4. Interest rate risk in the banking book – Guideline B-12 on Interest Rate Risk Management states that "OSFI supports the principles outlined in the Basel Committee's July 2004 document." Institutions should refer to this document and, in particular, Principles 6 to 9 on risk measurement, monitoring and control functions, and Principle 10 on internal controls.
5. ICAAP – Guideline E-19 provides OSFI's expectations for institutions around internal capital adequacy assessment processes. Key considerations pertaining to model risks are described throughout Sections I through VI however particular attention should be made to 'Pillar II components' when such risks are quantified via models.
6. Margin requirements for non-centrally cleared derivatives – Guideline E-22 provides expectation around institutions use of internal models for calculating initial margin requirements. Particular attention should be paid to Section 3.2 for institutions using an internal model for initial margin.
7. OSFI's Guideline *IFRS 9 Financial Instruments and Disclosures* – Section 2 Impairment

Footnotes

1 This spectrum includes regulatory capital models, internal risk management models, valuation/pricing models (including those used for accounting purposes), business decision-making models for risk management (such as credit adjudication and scoring models), and stress testing models.

2 Foreign bank branches are not in scope for this Guideline; however OSFI expects Branch Management to be accountable for ensuring there are appropriate controls over model risk, where material, as described in OSFI's Guideline E-4.

3 The terms "validation" and "vetting" are often used interchangeably. However, for the purposes of this document, validation is distinguished from vetting. Vetting is a discrete activity, occurring only at some pre-defined event or timing (e.g., initial model approval). By contrast, validation is a continuous activity (e.g., ongoing model performance assessments). The general phrase "review" will be used in the document wherever there is a need to address both activities.

4 Independence of the vetting and validation function is expected among IMAIs, while SIs can house the vetting and validation function within an overall risk management unit and/or rely on external auditors as described in Section 7. Regardless of the governance structure used by an institution, OSFI expects that an overriding principle of 'effective oversight over the use of models' be maintained.

5 Ibid.

6 OSFI's *Corporate Governance Guideline* articulates OSFI's principles and expectations with respect to corporate governance of institutions.

7 Independence implies that the model reviewer has no stake in the approval of the model, which enhances the credibility of the model risk control paradigm via effective challenge on the model's appropriateness.

8 For instance, institutions could consider quantitative factors such as the size and growth of the portfolio that the model covers in addition to its capital impact (e.g., VaR). Qualitative factors such as model age, complexity, purpose and strategic importance may also be considered, where relevant, as long as this is done in a consistent fashion.

9 Examples of triggers include, among others: changes in underlying business environment; increases in the size or scope of a business line; deterioration in model performance and material model modifications.

10 The evaluation of inputs could include an assessment of the rationale behind key assumption choices and data quality vetting. The evaluation of computation processes could include checking for computer code errors and the quality of the programming and theory. The evaluation of reporting processes could include evaluating the communication of outcomes analysis and results to Senior Management.

11 Exceptions can occur, for example but not limited to, when: models not approved for usage by the appropriate oversight entity are being used; a validated model is used outside its intended purpose; a model that displays persistent breach of performance metrics continues to be used; or backtesting suggests the model results are inconsistent with actual outcomes.

12 For greater context on the notion of model materiality, institutions can refer to the OSFI's Implementation Note: Approval of Regulatory Capital Models for Deposit-Taking Institutions pg.13.

13 Modifications could include, but are not limited to: the introduction of a new data source; a change in the technology/infrastructure used to supply the data or determine outputs; a change in the underlying methodology; or a change in the model's operating environment.

14 This is necessary for SIs in order to be able to identify and rank the materiality of various models in use.

15 Institutions relying on vendor models should also refer to Guideline B-10 Outsourcing of Business Activities, Functions and Processes.