Model Risk Policy

Risk Policy | Global

Version 2.0 · July 2026 · Confidential — Internal Use

This document is a template intended to be reviewed, tailored and approved by your organisation before use.
Replace all references to “the Company” with your organisation’s name.

Document Control

Document name	Model Risk Policy
Document type	Risk Policy
Jurisdiction	Global
Owner	Chief Risk Officer
Approved by	Board Risk Committee
Version	2.0
Effective date	July 2026
Review cycle	Annual
Next review due	July 2027
Classification	Confidential — Internal Use

Contents

1. Purpose

the Company uses models to inform decisions across credit, liquidity, capital, pricing, financial reporting, stress testing, fraud detection, financial crime monitoring and customer engagement. Errors in the design, data, implementation or use of these models can produce financial loss, poor customer outcomes, regulatory breaches and reputational damage. This Policy establishes the framework through which model risk is identified, measured, controlled, monitored and reported across the Company.

The Policy sets minimum, enforceable standards for the full model lifecycle: identification and registration, tiering by materiality, development, independent validation, approval, implementation, ongoing monitoring, change control and retirement. It applies heightened requirements to artificial intelligence and machine-learning (AI/ML) models and to models sourced from third parties, reflecting the additional risks these models present.

This Policy forms part of the Company's enterprise risk management framework and gives effect to international supervisory expectations on model governance, including the Basel Committee on Banking Supervision's standards for internal models and its corporate governance and operational risk principles, which require boards and senior management to understand the limitations of the models on which they rely and to subject them to effective, independent challenge. It is approved by the Board Risk Committee and owned by the Chief Risk Officer, who holds executive accountability for model risk management under the senior manager accountability regime applicable in the Company's jurisdiction(s).

2. Scope

This Policy applies to all entities within the Company's group, in every jurisdiction in which the Company operates, and to all directors, employees, contractors and secondees who develop, own, validate, approve, operate, use or oversee models.

It covers all models regardless of origin or technology, including:

- models developed internally, whether by specialist teams or business units (including qualifying End User Computing tools);
- third-party and vendor models, including models embedded in purchased software or consumed as a service;
- AI/ML models, including generative AI and large language models used to produce outputs that inform business decisions;
- models used for regulatory purposes (capital, liquidity, expected credit loss provisioning under IFRS 9 or the equivalent applicable accounting standard), financial reporting, credit decisioning, pricing, stress testing, fraud and financial crime detection, and customer-facing processes.

Simple deterministic calculators and tools that involve no estimation, prediction or statistical inference are outside scope; the MRM function makes the final determination where classification is uncertain and records the decision and

rationale in the Model Inventory. Exclusion from this Policy does not relieve a tool of applicable EUC, data governance or information security controls.

Jurisdictional application. This Policy states international best practice for model risk management. The Company must map the requirements of this Policy to the law and regulatory requirements of each jurisdiction in which it operates — including any supervisory requirements for internal models used for regulatory capital, data protection law governing model data, and rules on automated decision-making — and where local law or a local regulator imposes a stricter requirement, that stricter requirement prevails.

3. Definitions

Term	Definition
Model	A quantitative method, system or approach that applies statistical, economic, financial, mathematical or machine-learning theories, techniques and assumptions to process input data into estimates, forecasts, scores, classifications or other quantitative outputs used to inform decisions. Inputs may be partly qualitative or judgement-based provided the output is quantitative or drives a decision.
Model risk	The risk of adverse financial, customer, regulatory or reputational consequences arising from decisions based on models that are incorrectly designed or implemented, rely on flawed or unrepresentative data, or are used inappropriately or outside their validated purpose.
AI/ML model	A model whose parameters, structure or decision logic are wholly or partly derived from data through machine-learning techniques (including supervised, unsupervised and reinforcement learning, and generative or large language models), rather than being fully specified by a human developer.
Model Owner	The first-line individual accountable for a model across its lifecycle, including its purpose, data, assumptions, documentation, performance, controls and compliance with this Policy.
Model Developer	The individual or team that designs, builds, calibrates, tests and documents a model under the direction of the Model Owner.

Model User	An individual who runs a model or relies on its outputs for reporting or decision making, without authority to change the model's structure or parameters.
Model Validator	A suitably qualified individual, independent of the model's development, ownership and use, who performs independent validation and issues a validation opinion.
Model Risk Management (MRM) function	The second-line function, reporting to the Chief Risk Officer, that owns the model risk framework, maintains the Model Inventory, sets validation standards and provides oversight and challenge.
Model Inventory	The single, enterprise-wide register of all models in use, in development, provisionally approved, restricted or retired, maintained by the MRM function.
Model tier	The materiality-based classification of a model (Tier 1 to Tier 3) that determines the intensity of validation, approval, monitoring and documentation applied to it.
Material model change	A change to a model's methodology, mathematical or learning technique, key assumptions, source data, training data population, feature set or business purpose that could materially alter model outputs or use.
Independent validation	A critical, evidence-based assessment of a model's conceptual soundness, data, implementation, performance and use, performed by a Model Validator with no stake in the model's outcome.
Effective Challenge	Critical and constructive questioning of assumptions, decisions and proposals, before and during their implementation, by objective and informed parties with the standing, information and independence to identify limitations and require changes to the outcome; one of the foundational indicators of a sound risk culture identified by the FSB.
Explainability	The extent to which a model's individual outputs and overall behaviour can be interpreted, articulated and evidenced to model users, customers, management, validators and supervisors.
Third-party model	A model developed, hosted or materially maintained by an external vendor or

	service provider, including models embedded in vendor software or delivered as a service.
Model drift	Degradation in model performance over time caused by changes in input data distributions, relationships between variables, portfolio composition or the external environment.
Challenger model	An alternative model or benchmark used to compare against and challenge the outputs of a production model on the same data.
End User Computing (EUC) tool	A spreadsheet or user-developed application used in business processes. EUC tools that meet the definition of a model are subject to this Policy; the MRM function determines classification in cases of doubt.

4. Regulatory Framework

The key legislation, regulations and standards relevant to this document include (as amended from time to time):

Instrument / Standard	Relevance
Basel Framework (BCBS) — internal model requirements	Sets binding standards for the development, validation, governance and supervisory approval of internal models used for regulatory capital, including credit, market and counterparty risk models, where the Company uses such approaches.
BCBS Corporate Governance Principles for Banks	Requires the board and senior management to understand the limitations of models and other risk measurement techniques on which they rely, and to ensure independent, effective challenge.
BCBS Principles for the Sound Management of Operational Risk (2021)	Positions model failure as an operational risk to be identified, assessed, monitored and mitigated within the operational risk management framework.
BCBS Principles for Operational Resilience (2021)	Requires resilience of critical operations, including contingency arrangements where those operations depend on models or on third-party model providers.
BCBS 239 — Principles for Effective Risk Data Aggregation and Risk Reporting	Sets the standards for accuracy, completeness and timeliness of the data on which models and model risk reporting depend.

End of preview

This is a preview extract. The complete document continues beyond the pages shown here.

The full document is supplied as a single, fully editable Microsoft Word (.docx) file immediately after purchase — including every remaining section, the definitions, the regulatory framework references and all appendices and templates.

Bracketed prompts such as [30 days] mark the points where your own thresholds, committee names and local regulatory references are inserted.

finance-policies.com