Principles for Model Risk Management

Version: v1.0

Date: August 1st, 2025

Model Risk Managers International Association

Raymond Anderson	Rayan Risk Analytics
Joseph Breeden	Deep Future Analytics
Thomas Dahlin	Centennial Bank
Alan Forrest	Edinburgh Business School (Associate)
Shannon Kelly	Quantitative Risk Partners
Peter Quell	DZ Bank AG

This document may be shared freely. Any comments or suggestions should be emailed to Raymond Anderson: rayanrisk@gmail.com

Table of Contents

1 Executive Summary

Models sit at the centre of modern decision-making, risk management, and operational processes. From credit scoring and capital planning to fraud detection and customer personalization, they help organizations turn data into actionable insights. However, as organizations rely more heavily on models — and as these models become increasingly complex — the risks they carry also grow. Poor design, inadequate validation, misuse, or neglect can undermine not only a model's performance but also stakeholder trust and regulatory compliance.

This document outlines a practical framework for managing model risk. It outlines clear principles and practices to help ensure that all models — regardless of type, complexity, or origin — remain reliable, transparent, and aligned with both business objectives and regulatory expectations. There are three main parts:

- **Core Principles:** These define best practices to be applied to all models throughout their life cycle, including principles for development, validation, governance, documentation, and ongoing management. These principles are foundational and apply equally to traditional statistical models and more modern analytic approaches.
- **Special Considerations:** Recognizing that certain types of models — specific application, vendor-developed, machine learning, and generative AI — present unique challenges, this section builds on the core principles with targeted guidance to address their particular risks and governance needs.
- **Regulatory Guidance:** A summary of global regulatory expectations and a practical checklist, enabling institutions to benchmark practices, strengthen governance, and ensure alignment with international model risk management (MRM) standards and supervisory principles.

Model Risk Managers International Association, a team of dedicated professionals with a passion for the topic, has prepared this document. We aim to support all stakeholders — from developers and validators to users, model owners, and governance bodies — in fostering a culture of accountability, transparency, and continuous improvement. By applying these principles, organizations can maximize the benefits of advanced analytics while minimizing the risk of model-related failures or regulatory concerns.

2 Principles

Model Risk Management (MRM) requires a clear and structured set of principles and practices to guide the development, validation, governance, documentation, and ongoing maintenance of models throughout their lifecycle. Together, they provide the foundation of a sound MRM framework, ensuring that every model remains:

- Fit for its intended purpose and scope.
- Conceptually sound and empirically validated.
- Appropriately documented, transparent, and reproducible.
- Regularly monitored, reviewed, and updated to remain relevant.
- Subject to robust governance and independent challenge.

The sections that follow provide a detailed description of these core principles. They apply to all models, regardless of type or complexity, and set clear expectations for each stage of the model life cycle.[1]

These are aspirational standards, and while not every ideal will always be achievable in practice, they serve as a benchmark for building and maintaining effective model risk management. Six key areas are covered: 1) Organisation and Governance, 2) Data, 3) Development, 4) Validation, 5) Documentation, and 6) Life Cycle Management.

2.1 Organisation and Governance

Effective organization and governance form the cornerstone of sound model risk management. They provide the structure and ensure appropriate oversight. Strong governance also fosters a culture where assumptions and decisions are openly challenged and continuously improved, helping to keep models aligned with business objectives, regulatory expectations, and emerging risks.

Principles for robust organisational and governance practices relate to 1) Roles and Responsibilities, 2) Governance Structure, 3) Model Inventory, 4) Oversight, 5) Challenge and Continuous Improvement, and 6) Regulatory Environment.

2.1.1 Clear Roles and Responsibilities

Every party involved in the model life cycle should have clearly defined and communicated responsibilities. This clarity ensures accountability and supports effective oversight and decision-making. Key roles include:

[1] Much aligns with the traditions of (and will be readily recognized by professionals in) operations, engineering, and information technology—e.g., Six-Sigma for quality assurance, ISO 27001 for data security, ISO31000 on risk assessment, etc.

- **Model Owner:** The business owner responsible for ensuring the model remains relevant, performing as expected, and is subject to regular monitoring and periodic review.
- **Model Developer:** The team or individual tasked with designing, building, and documenting the model.
- **Model Validator:** An independent party responsible for reviewing, challenging, and validating the model to ensure it is fit for its intended use.
- **Users:** Operational or front-line staff who use the model's outputs to inform decisions.
- **Governance Committees:** Senior-level groups that oversee model risk policy, approve models for use, and maintain the organization's model inventory.

It is also essential to ensure that everyone in these roles has the right skills and expertise, that adequate staffing levels are maintained to meet current and future needs, and that succession plans are in place. Organizations should actively retain institutional knowledge to prevent the loss of critical expertise when staff are lost.

2.1.2 Governance Structure

- **Model Risk Policy:**
  - Develop and maintain a written MRM policy that outlines the objectives, standards, and minimum requirements.
  - Define clear escalation paths for addressing issues that arise during development, validation, or monitoring.
  - Where appropriate, document approved procedures and methodologies that are nonetheless subject to challenge.
- **Model Risk Appetite:**
  - Define the risk appetite for model risk at the organizational level.
  - Provide means of quantifying it, along with limits on aggregate risk at the business unit and enterprise level.
- **Model Risk Framework:**
  - Embed MRM into the broader enterprise risk framework.
  - Align with regulatory guidance (e.g., SR 11-7, ECB TRIM, local regulatory expectations).

2.1.3 Centralized Model Inventory

- **Comprehensive Register:**
  - Maintain a central inventory of all models, including their purpose, owner, status, risk rating, and key metrics.
  - Include all material models, as well as simpler tools and retired/decommissioned models for completeness.

    - Provide a model landscape and note inter-model dependencies where one feeds another.
- **Risk Tiering:**
    - Classify models (low, medium, high risk) based on both probability and materiality to guide the frequency and depth of validation.
    - Use these to guide resource prioritisation for overseeing development, validation, and monitoring.
- **Change Tracking:** Record all approved changes, incidents, and decommissioning in the inventory.

2.1.4 Oversight and Decision-Making Bodies

- **Model Risk Committee:**
    - Oversees adherence to policy, reviews validation results, and approves or rejects models for use.
    - Escalate significant model issues to senior management and the board.
- **Periodic Reporting:** Provide regular updates on model performance, emerging risks, validation status, and inventory changes to relevant governance bodies.
- **Independent Challenge:** Committees and validators should challenge developers and owners to ensure that assumptions, methodology, and results are robust.
- **Involvement:** Wherever feasible, RACI (Responsible, Accountable, Consulted, Informed) matrices should be used to track individuals' and/or business units' participation in projects.

2.1.5 Culture of Challenge and Continuous Improvement

- **Challenging Assumptions:** Encourage open, constructive questioning of all aspects of models to mitigate complacency and groupthink.
- **Accountability:** Assign responsibility and track ownership of decisions and actions through documented approvals.
- **Benchmarks:** Benchmark/challenger models not used for decision-making should nonetheless be governed (inventory, document, review).

2.1.6 Regulatory Engagement

- **Compliance:** Ensure models and governance processes align with applicable regulatory requirements and guidance.
- **Transparency:** Be prepared to demonstrate model governance, documentation, and monitoring practices to supervisors and external auditors.

2.1.7 Human Resources

Robust model risk management depends on having the right people with the right skills in the right roles. Governance should explicitly address:

- **Adequate Resourcing:** Ensure sufficient staffing levels to support development, validation, monitoring, and governance, commensurate with the size, complexity, and risk of the model inventory.
- **Competencies:** Maintain appropriate expertise across quantitative methods, regulatory expectations, business context, and emerging technologies (e.g., ML and AI).
- **Training and Development:** Provide ongoing training to ensure staff remain current with best practices and evolving standards.
- **Succession Planning:** Identify key-person dependencies and establish succession and knowledge transfer plans.
- **Knowledge Retention:** Document institutional knowledge and maintain it in centralized repositories to reduce reliance on individuals.
- **Recruitment:** Identify alternative staffing sources inside and outside the organisation (agencies, academic institutions).

2.1.8 Summary

Strong organization and governance underpin of effective model risk management. When roles are clearly defined, policies are well-articulated, oversight is coordinated, and accountability is embedded in the culture, organizations can ensure that models are applied responsibly, risks are properly managed, and decisions are transparent and defensible.

2.2 Data

High-quality data is critical to building, validating, and maintaining effective models. Weak data practices are one of the most common causes of model failures and regulatory issues that can undermine even the most sophisticated methodologies. Robust data sourcing, preparation, and monitoring are essential. This section outlines best practices for managing data throughout the model life cycle: 1) Governance and Accountability, 2) Sourcing, 3) Quality Assessment, 4) Preparation and Cleaning, 5) Splitting and Sampling, 6) Documentation and Transparency, and 2) Ongoing Monitoring:

2.2.1 Data Governance and Accountability

- **Data Ownership:** Clearly define ownership and custodianship of each data source.
- **Lineage and Provenance:** Document where data originates, how it flows through systems, and how it is transformed before use in the model.

- **Data Stewardship:** Assign data stewards responsible for ensuring the quality, completeness, and appropriateness of datasets used in modelling.
- **Access and Security Controls:** ensure that access to data (development, production, etc.) is limited to authorized personnel, logged, and aligned with data protection policies.

2.2.2 Sourcing

- **Relevance and Representativeness:**
    - Select datasets that reflect the population or phenomenon the model is intended to address.
    - Avoid relying on data that excludes important sub-populations or fails to capture key variability.
    - Assess its credibility, completeness, and timeliness past and future, including periodic reviews.
- **Credibility of Sources:**
    - Ensure transparency of how the data was produced and what it means.
    - Prioritize internal, audited data or trusted external sources.
    - If using vendor-provided or publicly available datasets, validate their accuracy and appropriateness.
    - Document the rationale for choosing, prioritizing, or excluding the various alternatives.
- **Timeliness:** Prioritize the most recently available and frequently updated data while ensuring sufficient historical depth for stability testing.
- **Compliance:** Consider legal, ethical, and contractual implications, whether for internal or external data.
    - Data protection implications, esp. when used for purposes other than that for which it was collected without permission.
    - Fair-business considerations, especially demographic data that identifies protected groups.
    - Data privacy laws (e.g., GDPR, CCPA), especially for external data.
    - Contractual issues for external data providers, especially service-level agreements and exit clauses.

2.2.3 Quality Assessment

Assess data quality before development begins. Key dimensions include:

- **Completeness:** Check for missing records, fields, or time periods.
- **Accuracy:** Validate that data reflects reality (e.g., through reconciliations, spot checks).
- **Consistency:** Ensure no conflicting values across datasets or fields.

- **Validity:** Confirm that values conform to expected ranges and formats.
- **Uniqueness:** Remove duplicates and confirm that records represent unique entities.

Tools such as data quality dashboards, profiling tools, and business rules should support this process.

2.2.4 Preparation and Cleaning

Prepare data systematically to ensure it is suitable for modelling:

- **Imputation of Missing Values:** Choose appropriate imputation methods (e.g., mean/mode substitution, model-based, indicator flags) and document choices.
- **Outlier Detection and Treatment:** Identify extreme values and decide whether to retain, adjust, or remove them based on business context.
- **Normalization and Scaling:** Standardize units, formats, and scales to ensure comparability and model stability.
- **Encoding Categorical Variables:** Apply appropriate encoding (e.g., one-hot, ordinal, frequency, weight-of-evidence) aligned with the modelling methodology.
- **De-duplication and Filtering:** Remove irrelevant or duplicate records, ensuring the final dataset aligns with the defined scope.

2.2.5 Data Splitting and Sampling

- **Partitioning Data:**
  - Split into training, validation, and test sets to assess out-of-sample and/or out-of-time performance and avoid overfitting.
  - Use stratified sampling if needed to preserve distributions of key variables.
- **Sample Size and Power:** Ensure that sample sizes are sufficient for statistical robustness and regulatory expectations.
- **Time Horizon Alignment:** Align data periods with business cycles, regulatory reporting periods, and the intended use of the model.[2]

2.2.6 Documentation and Transparency

- **Data Dictionary:** Maintain a comprehensive data dictionary defining each field, its source, transformations, and allowed values.
- **Processing Log:** Record all data processing steps, including rationale, parameter settings, and tools used.

---

[2] Models are often overfitted to data from a limited window in time, which can confuse changes in subject behaviour with those in the broader environment. The incorporation of macroeconomic variables and/or survival concepts can aid model stability.

- **Reproducibility:** Ensure that any stakeholder can reproduce the prepared dataset from raw data using the documented process.

2.2.7 Ongoing Data Monitoring

- **Monitoring Data Drift:** After deployment, monitor for changes in data distributions, quality, or relevance that could degrade model performance.
- **Feedback Loop:** Use ongoing model performance to inform updates to data sourcing and preparation practices.

2.2.8 Summary

Sound data sourcing and preparation are essential to maintaining model integrity. With strong governance, rigorous data assessment and preparation, and clear, transparent documentation, organizations can significantly reduce model risk and build confidence in the reliability of their model outputs.

2.3 Development

Model development is the process of designing, building, and testing a model to ensure it performs its intended function effectively, transparently, and reliably. A strong development process helps ensure that each model is conceptually sound, empirically validated, and appropriate for its intended use. This section outlines key principles to guide model development, covering: 1) Purpose and Scope Definition, 2) Data Preparation and Analysis, 3) Methodology Choice, 4) Construction and Fitting, 5) Performance Evaluation, 6) Governance and Transparency, and 7) Implementation Readiness.

2.3.1 Define Purpose and Scope

- **Business Objective:** Clearly articulate the model's purpose, how it supports business objectives, and what decisions it will inform.
- **Intended Use:** Specify the target user groups and operational environment.
- **Scope & Limitations:** Document assumptions, applicability boundaries, and known constraints.
- **Regulatory & Ethical Considerations:** Incorporate compliance requirements and avoid discriminatory or unethical biases.

2.3.2 Data Preparation and Analysis

- **Data Identification:** Select data sources that are accurate, complete, relevant, and representative of the modelled population.
- **Data Quality Assessment:** Examine data for missing values, inconsistencies, outliers, and noise.
- **Exploratory Data Analysis:** Analyze distributions, correlations, trends, and anomalies.

- **Data Transformation & Cleaning:**
  - Impute or handle missing data systematically.
  - Normalize, standardize, encode, or transform variables as needed.
  - Document all data processing steps for traceability.
- **Data Partitioning:** Partition the dataset into training, validation, and test samples to avoid overfitting and assess generalizability.

2.3.3 Methodology Design

- **Model Type Selection:** Choose a model type appropriate to the problem, considering complexity, interpretability, and performance.
- **Justification of Methodology:** Document the rationale for selecting the chosen algorithm(s) over alternatives.
- **Assumptions Testing:** Validate that model assumptions (e.g., linearity, independence) hold in the data context.
- **Feature Engineering:** Create derived variables, ratios, interaction terms, or non-linear transformations that improve predictive power.
- **Feature Selection:** Evaluate variable stability and significance over time.
- **Segmentation:** Determine whether multiple models may be required to accommodate interactions affecting different subgroups.
- **Reject Inference:** Assess whether potential biases arise from model owners' decisions regarding acceptance and terms-of-business, and whether they can be addressed.

2.3.4 Model Construction and Fitting

- **Model Training:**
  - Use training data to estimate model parameters, ensuring reproducibility and convergence.
  - Prioritize trusted and readily available features over those less certain.
  - Assess whether over-predictive features should be downplayed.
- **Model Tuning:** Optimize hyperparameters using cross-validation or grid search methods (see 3.4.3 on machine learning).
- **Regularization:** Apply techniques (e.g., L1/L2 penalties, pruning) to avoid overfitting and improve generalization.
- **Benchmarking:** Compare performance against naive, baseline, or alternative models.

2.3.5 Performance Evaluation

- **Performance Metrics:** Select and report appropriate metrics for predictive power, accuracy, calibration, discrimination, and stability (e.g., Gini, KS, ROC-AUC, RMSE, etc.).
- **Robustness Testing:**

  - Assess model sensitivity to changes in inputs.
  - Perform scenario analysis and stress testing.
- **Out-of-Sample Testing:** Evaluate model performance on validation and test datasets not seen during training.
- **Stability Testing:** Assess model performance over time and across segments.

2.3.6 Governance and Transparency

- **Peer Review:** Subject the development process and results to internal review or challenge.
- **Audit Trail:** Maintain complete records of all development steps, data manipulations, code versions, and parameter settings.
- **Stakeholder Engagement:** Present findings to stakeholders for feedback and alignment.
- **Explainability:** Ensure the model is interpretable enough for its intended users to understand key drivers and behaviours.

2.3.7 Implementation Readiness

- **Reproducibility:** Ensure the model can be implemented consistently across environments (e.g., from development to production).
- **User Documentation:** Prepare clear documentation for implementation teams and end-users.
- **Monitoring Plan:** Define how the model's performance will be monitored post-implementation.

2.3.8 Judgmental Overlays

In some situations, overlays or adjustments may be applied to model outputs to account for risks, trends, or other factors not fully captured by the model (e.g., due to data limitations or emerging risks). Any overlays should adhere to the following principles:

- **Governance:** Clearly justified, documented, and approved by governance bodies.
- **Transparency:** Clarity of assumptions, calculation methods, and intended impact.
- **Review:** Periodically reviewed and updated, or removed as conditions change.

Overlays should complement (not substitute for) robust model development and monitoring. Their use should always align with the organization's risk appetite and meet applicable regulatory expectations.

2.4 Validation

Model validation is the independent assessment of a model's quality, soundness, and suitability for its intended purpose. It provides assurance that the model performs reliably, is conceptually appropriate, and does not expose the organization to unnecessary risk. This section outlines key principles of good validation practice: 1) Independence and Objectivity, 2) Scope, 3) Performance Assessment, 4) Monitoring Plan Review, 5) Documentation and Transparency, 6) Remediation and Follow-Up.

2.4.1 Independence and Objectivity

- **Validator Independence:** Validators must be independent of the development team (separate reporting line) to avoid conflicts of interest.
- **Unbiased Evaluation:** Validation should take a critical, objective view of assumptions, methods, and results.
- **Skillset & Expertise:** Validators should have the necessary domain knowledge, technical expertise, and awareness of regulatory expectations.

2.4.2 Scope of Validation

A comprehensive validation examines all key aspects of the model:

- **Conceptual Soundness:** Assess whether the development methodology is appropriate for the intended purpose, given the available data and business context.
- **Data Integrity:** Evaluate data inputs for relevance, accuracy, completeness, and consistency with business expectations.
- **Assumptions and Limitations:**
  - Challenge key assumptions to ensure they are justified.
  - Assess model boundaries and potential weaknesses.
- **Methodology Review:** Replicate key development steps where practical and verify the correctness of the approach.
- **Implementation Verification:** Confirm that the model's implementation in the production environment is consistent with the approved specification.

2.4.3 Performance Assessment

- **Performance Metrics:** Independently calculate and validate the performance metrics reported by developers.
- **Out-of-Sample and Back-Testing:** Evaluate model stability and predictive power on holdout and historical datasets.
- **Sensitivity & Stress Testing:**
  - Assess how model outputs respond to changes in inputs, assumptions, or scenarios, especially for high-risk models used for capital allocation and pricing.
  - Identify potential weaknesses under adverse conditions.
- **Benchmarks:**

  - Compare model performance to alternative methods, prior models, or industry benchmarks.
  - Benchmarks should themselves be conceptually sound, documented, and periodically reviewed to ensure continued appropriateness.
- **Overlays:** Where applied, their rationale, calculation, and impact should be assessed to ensure they are reasonable and appropriate.

2.4.4 Monitoring Plan Review

- **Monitoring Metrics:** Assess whether the planned performance monitoring metrics are suitable and sufficient to detect deterioration.
- **Thresholds:** Evaluate the appropriateness of monitoring thresholds and action plans.
- **Model Risk Tiering:** Confirm that the proposed monitoring frequency and depth are commensurate with the model's materiality and risk classification.

2.4.5 Documentation and Transparency

- **Validation Report:**
  - Prepare a formal validation report detailing the scope, methods, findings, and recommendations.
  - Clearly articulate validation limitations or areas requiring ongoing attention.
- **Traceability:** Ensure findings can be traced back to specific tests and data points.
- **Communication:** Present findings to stakeholders, including developers, business owners, and governance committees.

2.4.6 Remediation and Follow-Up

- **Action Plans:** Where issues are identified, recommend appropriate remediation steps and timelines.
- **Re-Validation:** Confirm that corrective actions have been implemented and are effective.
- **Escalation:** Escalate critical or unremediated issues to senior management or committees as necessary.

2.4.7 Summary

Effective model validation helps ensure that models remain appropriate, robust, and aligned with their intended purpose. By providing independent assurance and challenging assumptions where necessary, validation strengthens confidence in model-driven decisions among stakeholders and regulators alike. A thorough and well-documented validation process is a critical component of an MRM framework.

2.5 Implementation

Implementation is the process of deploying a model into production, where design and testing meet real-world application. It is critical to ensure that models a) perform as intended,[3] b) are used appropriately and c) integrate smoothly into business processes. Without strong governance at this stage, models can underperform, be misused, or introduce operational and compliance risks. Treating implementation with the same rigour as development, validation, and monitoring helps ensure reliable performance, operational readiness, and user confidence. This section addresses implementation under the following headings: 1) Implementation and Planning, 2) Readiness, 3) Readiness, 4) Production Testing, 5) Control Integration, 6) Governance and Handover, and 7) Post-Implementation Review.

2.5.1 Implementation Planning

A clear and structured implementation plan is essential to guide deployment and manage risks effectively:

- **Deployment Plan:** Create and document a comprehensive plan that defines objectives, scope, roles and responsibilities, timelines, and key dependencies. The plan should address both business and technical requirements.
- **Risk Assessment:** Identify potential operational, compliance, and reputational risks associated with deployment. Document mitigation strategies, contingency plans, and rollback procedures in case of issues.
- **Change Management:** Incorporate the deployment into the organization's formal change management process, ensuring proper approvals, communication, and tracking of all implementation activities.

2.5.2 Production Environment Readiness

Before deployment, ensure the production environment is fully prepared to support the model securely and reliably:

- **Infrastructure Preparation:** Verify that all production infrastructure — including hardware, software, and interfaces — is correctly configured, secured, and tested for stability.
- **Data Integration:** Validate that all necessary data feeds are in place, consistent with those used during development and validation, and that data privacy and security requirements are met.

[3] Implementation testing can only assess that the model and associated strategies are operating according to the design, and not whether the design is correct.

- **Access Controls:** Define and implement appropriate access rights and enforce segregation of duties among users, administrators, and monitoring teams to prevent unauthorized use or changes.

2.5.3 User Preparedness

Ensuring that users understand the model and how to apply it appropriately is critical to its effective and responsible use.

- **Training:** Provide targeted training to all user groups — including front-line staff, analysts, and decision-makers — covering the model's purpose, functionality, assumptions, limitations, and proper interpretation of outputs.
- **Usage Guidelines:** Develop and distribute clear guidance on the model's intended use, approved scope, and prohibited uses to prevent over-reliance or misuse.
- **Support Channels:** Establish ongoing support channels for users to ask questions, report anomalies, and receive updates on changes or findings related to the model.

2.5.4 Testing and Validation in Production

Before full deployment, it is essential to test the model in the production environment to confirm that it performs as expected under real-world conditions:

- **Parallel Testing:** Where feasible, operate the model in parallel with existing processes for a defined period to compare outputs, detect discrepancies, and validate performance in a live setting.
- **Output Verification:** Review model outputs against expected results to ensure consistency with development and validation benchmarks.
- **Issue Resolution:** Investigate and address any anomalies, errors, or deviations identified during testing, and document corrective actions taken before proceeding to full deployment.

2.5.5 Control Integration

Embedding robust controls during implementation helps ensure the model operates reliably and remains compliant from day one:

- **Operational Controls:** Implement automated checks, exception reporting, and validation routines within the production process to detect errors or unusual behaviour.
- **Monitoring Framework:** Set up monitoring dashboards and key performance indicators (KPIs) to track model performance and usage in real time.
- **Audit Trail:** Establish processes to log all key activities, changes, and decisions during and after implementation, providing a clear record for governance and audit purposes.

2.5.6 Governance and Handover

A disciplined governance process and a clear transition of responsibilities help ensure accountability and continuity after implementation.

- **Formal Approval:** Obtain final approval from designated governance bodies, confirming that all implementation requirements, testing, and controls have been satisfactorily completed.
- **Ownership Transition:** Document and formalize the handover of the model from development and validation teams to operational owners and monitoring teams.
- **Role Clarification:** Reaffirm and communicate the responsibilities of all parties involved in the model's ongoing use, monitoring, and oversight to prevent gaps or overlaps.

2.5.7 Post-Implementation Review

After deployment, conducting a structured post-implementation review helps validate early performance, identify improvement opportunities, and strengthen future implementations.

- **Initial Performance Assessment:** Review model outputs and operational performance after a defined period (e.g., 3–6 months) to confirm they align with expectations and meet business needs.
- **Issue Identification and Resolution:** Document any unexpected issues, their root causes, and the corrective actions taken to address them.
- **Lessons Learned:** Capture insights and recommendations to improve processes, controls, and governance for future model implementations.
- **Reporting:** Share the findings of the review with governance bodies to aid continued oversight and transparency.

2.5.8 Summary

A disciplined implementation process ensures that models deliver their intended value while minimizing operational and compliance risks. By planning thoroughly, preparing infrastructure and users, embedding controls, and maintaining clear governance, organizations can confidently transition models into production and strengthen trust in model-driven decision-making.

2.6 Monitoring & Use

Once a model is implemented, it must be actively monitored and used responsibly to ensure it continues to perform as intended and to identify emerging risks early. Continuous monitoring and disciplined use are critical for detecting changes in model behaviour, preventing misuse, and maintaining alignment with business objectives and regulatory expectations. This section outlines best practices for monitoring and use under the following headings: 1) Performance Monitoring, 2) Usage Controls, 3) Exception Handling, 4) Reporting and Oversight, and 5) User Awareness and Training.

2.6.1 Performance Monitoring

A structured approach to performance tracking helps detect early signs of degradation, drift, or misuse so that corrective action can be taken promptly.

- **Monitoring Plan:** Establish a formal plan that defines metrics, acceptable thresholds, and review frequency.
- **Key Performance Indicators (KPIs):** Track measures such as predictive accuracy, stability, discriminatory power, and error rates.
- **Benchmarking:** Compare current performance against development-phase results, historical benchmarks, and, where applicable, challenger models.
- **Drift Detection:** Implement statistical tests and automated alerts to identify data drift, concept drift, or changes in input-output relationships.

2.6.2 Usage Controls

Strong controls ensure the model is used as intended and remains appropriate as business needs evolve:

- **Intended Use Verification:** Confirm the model is used only for approved purposes and within defined boundaries.
- **Guidelines and Limitations:** Communicate clear instructions on proper use, limitations, and prohibited applications.
- **Context Review:** Assess whether changes in business context, customer behaviour, or regulations affect the model's appropriateness.

2.6.3 Exception Handling

Should deviations from approved expectations occur, a clear response minimizes risk and maintains governance standards:

- **Threshold Breaches:** Define and document procedures for responding to performance breaches, unexpected outputs, or operational issues identified through monitoring.
- **Escalation Protocols:** Ensure that material issues are escalated to governance bodies promptly and addressed within agreed timelines.
- **Interim Adjustments:** Where appropriate, apply overlays or operational mitigants while longer-term remediation is planned.

2.6.4 Reporting and Oversight

Transparent reporting and oversight maintain accountability and support continuous improvement.

- **Regular Reporting:** Produce periodic monitoring reports summarizing model performance, exceptions, and actions taken.
- **Governance:** Share with governance bodies, internal audit, and regulators as required.
- **Audit Trail:** Maintain a complete record of monitoring activities, findings, and decisions to demonstrate effective oversight.
- **Framework Review:** Periodically reassess the monitoring plan to ensure it remains fit for purpose as business needs and regulatory expectations evolve.

2.6.5 User Awareness and Training

Keeping users informed and engaged ensures models are applied responsibly and effectively.

- **Ongoing Training:** Provide refresher training to model users on proper use, limitations, and updated procedures.
- **Feedback Mechanisms:** Create channels for users to report concerns, anomalies, or suggestions based on their experience with the model in production.

2.6.6 Summary

Continuous monitoring and disciplined use are critical to ensuring that models remain reliable, relevant, and compliant throughout their operational life. By tracking performance metrics, managing exceptions effectively, and maintaining clear oversight and user awareness, organizations can mitigate risk and sustain confidence in model-driven decisions.

2.7 Documentation

Clear and comprehensive documentation is critical for transparency, knowledge transfer, auditability, and regulatory compliance. Well-maintained records ensure that models can be understood, reproduced, validated, and challenged — even years after development. The following covers: 1) Documentation's Purpose, 2) Development Documentation, 3) Validation Documentation, 4) Change and Incident Logs, 5) Version Control and Archiving, 6) Accessibility and Readability, and Regulatory and Audit Readiness.

2.7.1 Purpose

Good documentation ensures models remain transparent, auditable, and understood over their full life cycle.

- **Complete Record:** Provide a full and transparent account of the model's design, development, validation, and monitoring.
- **Independent Understanding:** Enable others to replicate, review, and fully understand the model without reliance on original developers.

- **Audit and Review Support:** Facilitate regulatory, internal audit, and governance reviews through clear and accessible documentation.
- **Knowledge Preservation:** Retain institutional knowledge to mitigate risks from staff turnover and maintain continuity.

2.7.2 Development Documentation

Comprehensive documentation must accompany the development process:

- **Model Overview:** Clearly state the model's purpose, scope, intended use, and known limitations.
- **Data Sources:**
  - Identify all datasets used, including their origin, coverage period, and any known data quality issues.
  - Document all data pre-processing steps, transformations, and underlying assumptions.
- **Methodology:**
  - Explain the choice of model type, theoretical underpinnings, and why alternatives were not selected.
  - Include assumptions, constraints, and simplifications made.
- **Feature Engineering:** Describe variable selection, transformations, derived features, and the justification for these choices.
- **Estimation and Testing:**
  - Detail training, validation, and testing procedures, including how data was split.
  - Report all performance metrics along with interpretation of results.
- **Sensitivity and Stress Testing:** Explain how the model was tested under different scenarios to assess robustness.
- **Governance Notes:** Record internal reviews, sign-offs, and key decisions made throughout development.

2.7.3 Validation Documentation

Validation findings should be documented clearly and maintained as a separate record from development materials. Key elements include:

- **Scope of Validation:** Define the boundaries of the review, including what aspects of the model were assessed and tested.
- **Methodology:**
  - Describe the tests, analyses, and review techniques performed.
  - Document any replication of key development steps.
- **Findings:** Summarize identified deficiencies, challenged assumptions, and any gaps in model performance.

- **Recommendations:** Outline remedial actions, along with assigned responsibilities and target completion dates.
- **Approval Status:** Record decisions and approvals from relevant validation governance bodies.

2.7.4 Version Control and Archiving

Proper version control ensures traceability and clarity throughout the model's life cycle.

- **Versioning:**
  - Assign unique version identifiers to each iteration of the model and its documentation.
  - Archive superseded versions securely for traceability.
- **File Management:** Apply standardized naming conventions and directory structures to maintain order and facilitate retrieval.

2.7.5 Change and Incident Logs

Records of changes and incidents are essential for ensuring transparency, accountability, and continuous improvement.

- **Change History:** Maintain a formal log of all model changes, including rationale, approver, date, and impact assessment.
- **Incident Record:** Record any performance issues, implementation errors, or failures, along with corrective actions taken.

2.7.6 Accessibility and Readability

For documentation to be effective, it must be easy to access, understand, and use. Key practices include:

- **Central Repository:** Store all documentation in a secure, centralized location accessible to relevant stakeholders.
- **Readability:** Ensure documentation is written clearly and concisely, suitable for both technical and business audiences.
- **Templates and Standards:**
  - Use standardized templates to promote consistency across documentation.
  - Follow organizational style guides and meet applicable regulatory expectations.

2.7.7 Regulatory and Audit Readiness

Transparent and readily available documentation should also support regulatory compliance and audit processes.

- **Transparency:** Ensure documentation is comprehensive and meets regulatory expectations for clarity and completeness.

- **Responsiveness:** Maintain it such that it is readily available upon request for internal auditors, external auditors, and supervisory authorities.

2.7.8 Summary

Robust model documentation strengthens transparency, supports independent validation, preserves institutional knowledge, and reflects strong governance. Well-documented models are easier to monitor, review, and defend, helping to reduce model risk and build confidence in model-driven decisions among stakeholders and regulators.

2.8 Life Cycle Management

Like any business process, models have a natural life cycle — from initial conception through development, implementation, and ultimately retirement. Managing models effectively at every stage helps ensure they remain fit for purpose, robust, and aligned with both business objectives and regulatory requirements throughout their operational life. This section outlines key principles for managing the model life cycle: 1) Life Cycle Definition, 2) Change Management, 3) Performance Monitoring, 4) Periodic Review and Re-validation, 5) Incident Management, 6) Decommissioning, and 7) Governance Oversight.

2.8.1 Defined Life Cycle Stages

Clearly define and document each stage of the model's life:

- **Conception:** Identify the business need, define objectives, and assess feasibility.
- **Development:** Build, document, and test the model in accordance with development principles.
- **Validation:** Conduct an independent review and approve the model prior to deployment.
- **Approval:** Obtain formal sign-off from governance bodies before implementation.
- **Implementation:** Deploy the model into production, ensuring appropriate controls and monitoring are established.
- **Monitoring & Use:** Continuously track performance and usage to detect drift, misuse, or emerging risks.
- **Review & Re-Validation:** Periodically reassess assumptions, methodology, and performance.
- **Retirement/Decommissioning:** Remove the model from active use when it becomes obsolete or is replaced, ensuring proper documentation and transition.

2.8.2 Change Management

- **Formal Change Control:** Subject all material changes to formal review, testing, and approval before implementation.
- **Impact Assessment:** Evaluate how changes affect model performance, risk, and business processes.
- **Versioning:** Assign and track new version identifiers for every material change.
- **Documentation Update:** Update all documentation, monitoring plans, and inventory entries following any change.

2.8.3 Performance Monitoring

- **Ongoing Monitoring:**
  - Monitor predictive power, calibration, stability, and business impact.
  - Compare actual outcomes with model predictions to detect deterioration.
- **Thresholds & Triggers:** Define clear thresholds for performance indicators and pre-determined actions when they are breached.
- **Usage Monitoring:** Track how the model is used in practice to ensure alignment with the intended scope.

2.8.4 Incident Management

- **Incident Reporting:** Record and investigate incidents where the model fails, underperforms, or produces unexpected results.
- **Root Cause Analysis:** Analyze incidents to identify and address underlying issues.
- **Escalation and Remediation:** Escalate material incidents promptly and implement corrective actions.
- **Overlays:** Apply temporary or structural overlays should unforeseen factors demand it, but follow governance to address the identified gap.

2.8.5 Periodic Review and Re-Validation

- **Scheduled Reviews:** Conduct periodic full-scope reviews based on the model's risk rating and age, including reviews of change and incident logs.
- **Re-Validation:** Independently re-validate assumptions, data, methodology, and implementation.
- **Benchmarking:** Compare with newer models or industry best practices to assess continued relevance.

2.8.6 Decommissioning

- **Retirement Planning:** Formally plan and document the model's retirement when it becomes obsolete.

- **Inventory Update:** Update the central inventory to reflect retired status and archive all supporting materials.
- **Impact Mitigation:** Ensure transition to replacement models or alternative processes with minimal disruption.

2.8.7 Governance Oversight

- Ensure governance bodies receive regular reports on model performance, incidents, changes, and reviews.
- Require formal approval for significant events in the model life cycle, such as deployment, material change, or retirement.

2.8.8 Summary

Proactive life cycle management ensures models remain reliable, relevant, and aligned with business needs. By defining each stage clearly, monitoring performance continuously, and managing changes and retirement thoughtfully, organizations can reduce model risk and enable more effective, confident decision-making.

3 Special Considerations

As advanced analytics and artificial intelligence (AI) become more prevalent, organizations are relying on a wider variety of models across business areas. While external vendors initially developed many models, larger firms are increasingly building and maintaining their own. At the same time, traditional statistical models are being supplemented — and in some cases replaced — by more complex approaches such as machine learning (ML) and generative AI.

These developments introduce new risks and challenges that need to be addressed within the model risk management framework. Common concerns include reduced transparency, greater complexity, data privacy risks, validation challenges, and potential ethical and regulatory issues.

This section highlights special considerations for managing these types of models, with guidance to help ensure that their development, validation, deployment, and use remain aligned with organizational goals, regulatory expectations, and sound risk management practices. The areas covered include: 1) Application Across Business Lines, 2) Smaller Institutions, 3) Vendor-Developed Models, 4) Machine Learning, 5) Generative AI, and 6) Other Model Types.

3.1 Risk Tiering across Business Lines

The core principles of MRM — covering development, validation, governance, documentation, and monitoring — apply to all models. However, how these principles are applied should reflect the specific context, risk profile, and objectives of each business line. Different use cases bring differing levels of regulatory scrutiny, business impact, and operational constraints, all of which need to be considered.

This section explains how to tailor MRM practices across common business areas. The goal is to ensure that approaches remain risk-based and proportionate, yet stay aligned with organizational priorities and maintain effective oversight.

3.1.1 Originations

Models that support origination decisions — such as application scorecards and affordability assessments — are among the most critical. They have a direct impact on customers, are subject to significant regulatory scrutiny, and carry substantial implications for overall portfolio risk.

- **Risk Tier:** Typically, **high**.
- **Special Considerations:**
  - Rigorous validation of discriminatory power, calibration, and stability.

  - Fair lending/equal treatment testing to detect and mitigate bias.
  - Explainability is paramount for regulatory and customer transparency.
  - Monitoring for model drift due to economic cycles or demographic shifts.
- **Governance:** Senior-level approvals and independent validation are mandatory.

3.1.2 Collections

Models used to guide collections strategies — such as prioritization and treatment path assignment — typically carry less regulatory sensitivity and risk impact than origination models. However, they still play an important role in shaping customer experience and influencing recovery outcomes.

- **Risk Tier:** Usually **medium to low**, depending on scope.
- **Special Considerations:**
  - Emphasis on operational effectiveness and minimizing customer harm.
  - Monitor for unintended consequences, such as disproportionate impact on vulnerable customers.
  - Flexibility to adapt to rapidly changing conditions (e.g., during a crisis).

3.1.3 Account Management

Models used in account management — such as facility increase assessments and behavioural scorecards — are operationally important, but they typically carry lower risk and regulatory sensitivity compared to origination models (excepting 3.1.5.).

- **Risk Tier:** Typically, **medium**.
- **Special Considerations:**
  - Stability over time is critical as these models are usually applied repeatedly on the same accounts.
  - Monitor for overextension risk and adverse selection.
  - Governance proportional to materiality but aligned to originations principles.

3.1.4 Insurance

Models used in insurance — for pricing, underwriting, and reserving — are subject to distinctive actuarial standards and regulatory requirements, reflecting the sector's specific risk and compliance expectations.

- **Risk Tier:** Often **high**, particularly pricing and solvency models.
- **Special Considerations:**
  - Actuarial soundness and compliance with sector-specific regulations.
  - Long-term stability and scenario-based stress testing for reserving.
  - Transparency and customer fairness in pricing decisions.

3.1.5 Capital Allocation & Planning

These models are used to assess capital requirements for different risk exposures and to allocate capital effectively across business units, ensuring alignment with risk appetite and regulatory expectations.

- **Risk Tier:** Typically **high**, given their impact on solvency and regulatory compliance.
- **Special Considerations:**
  - Ensure assumptions and risk weightings are aligned with regulatory guidance and internal risk appetite.
  - Stress testing under extreme but plausible scenarios is essential.
  - Strong governance over methodological changes, as these can materially impact reported ratios.
  - Full traceability and documentation, including backtesting against realized losses.
  - Should behavioural models provide inputs, they should also be given the highest risk tier.
- **Governance:** Senior-level approvals and independent validation are mandatory.

3.1.6 Asset & Liability Management

ALM models are used to manage interest rate risk, liquidity risk, and balance sheet mismatches across different time horizons, supporting sound financial and risk management practices.

- **Risk Tier:** Typically, **high**.
- **Special Considerations:**
  - Scenario-based testing, including rising/falling rate environments, market shocks, and behavioural assumptions.
  - Monitoring of behavioural model assumptions (e.g., prepayment rates, deposit stickiness).
  - Alignment with liquidity coverage and net stable funding ratio requirements, where applicable.
  - Governance over assumptions is particularly critical given the judgment often involved.

3.1.7 Other Business Lines

For other areas — including treasury, fraud detection, marketing, capital planning, and operational risk — the same MRM principles apply. However, their application should be tailored to reflect the materiality, impact, and specific context of each.

- **Fraud Detection:** Often machine-learning-based, with low explainability but high operational value; requires special monitoring for false positives.
- **Marketing:** Typically, low risk tier; governance focused on fairness and data privacy.
- **Stress Testing**: High-tier models due to regulatory impact and systemic importance.

3.1.8 Overarching Guidance

- Apply risk-based proportionality: The higher the risk tier, the more stringent the scrutiny during validation, monitoring, and governance.[4]
- Ensure documentation and monitoring plans clearly state the business context and materiality.
- Retain independence and accountability regardless of use case.
- Include business line input in the model development and validation processes to reflect operational realities.

3.1.9 Summary

The core principles of model risk management apply across all business lines, but their implementation should reflect the specific impact, regulatory sensitivity, and operational needs of each context. By tailoring practices to the level of risk, organizations can maintain strong oversight where it matters most, while avoiding unnecessary burden where risks are lower.

3.2 Smaller Institutions

For smaller banks, insurers, and other organizations with limited modelling activity, establishing an MRM framework can pose unique challenges. While the same fundamental principles apply, the framework should be tailored to fit the institution's size, complexity, and risk profile — i.e., be proportionate and practical.

3.2.1 Proportionality

- The governance and controls applied to each model should be commensurate with its materiality and impact rather than rigidly uniform.
- Focus resources on high-tier, high-impact models; simpler tools and low-risk calculators may require lighter-touch oversight.
- Avoid unnecessary administrative burden by streamlining documentation and validation where appropriate, while maintaining traceability.

---

[4] Refer to PRA SS1/23 (UK) for tiering criteria, which distinguish models by both impact (e.g., business exposure, speed of failure propagation) and complexity (e.g., interpretability, interdependencies, developer familiarity). These principles are broadly applicable across jurisdictions.

3.2.2 Governance and Expertise

- Smaller institutions may lack separate, specialized validation or model risk teams.
  - Consider cross-training staff in development and validation disciplines while ensuring functional independence.
  - Where independence is not feasible internally, engage external validators to meet governance expectations.
- Senior management and board-level oversight remain critical, even in a scaled-down framework.

3.2.3 Documentation and Monitoring

- Even with limited resources, maintain clear documentation of model purpose, assumptions, limitations, and testing.
- Monitoring should focus on key indicators and material risk exposures.
- Establish a central inventory, even if small, to track and control all models in use.

3.2.4 External Vendors and Shared Services

- Smaller institutions often rely on vendor-developed or shared-service models.
  - Pay special attention to vendor due diligence, documentation adequacy, and validation of externally supplied models.

3.2.5 Flexibility and Scalability

- Build a framework that is flexible enough to accommodate growth in modelling activity or regulatory expectations over time.
- Document policies clearly, including when and how the institution applies proportionality in validation, monitoring, and governance.

3.2.6 Summary

Smaller institutions should aim for a fit-for-purpose approach to model risk management, with controls that are effective yet proportionate to their complexity and risk exposure. This helps ensure that, even with limited resources, the institution remains accountable for its models and adheres to sound risk management practices.

3.3 Vendor Developed Models

Many organizations use externally developed models or third-party tools to support critical processes. While the outsourcing of model development can bring specialized expertise and operational efficiency, it also introduces distinct risks and governance challenges that must be addressed. This section outlines best practices for managing vendor-developed models, focusing on 1) Ownership and Accountability, 2) Vendor Due Diligence, 3) Model Transparency, 4) Independent Validation, 5) Monitoring and Change Management, 6) Contractual and Regulatory Considerations

3.3.1 Ownership and Accountability

Organizations are responsible for the outcomes of their decisions.

- **Internal Accountability:** Retain full responsibility for the model's use, performance, and impact, even when developed externally.
- **Designated Owner:** Assign an internal owner who understands the model and ensures it aligns with business objectives and risk appetite.
- **Governance Oversight:** Subject vendor models to the same internal approval, monitoring, and governance processes as internally developed models.

3.3.2 Due Diligence on the Vendor

- **Vendor Qualification:** Assess the vendor's technical capabilities, reputation, regulatory compliance record, and experience with similar implementations.
- **Transparency and Access:** Ensure the vendor is willing and able to share sufficient information about the model's design, data requirements, and assumptions.
- **Information Security and Confidentiality:** Evaluate the vendor's data protection and confidentiality controls, especially when sensitive data is involved.
- **Contingency and Continuity Planning:** Assess the vendor's ability to support the model over time and provide business continuity in case of disruptions.

3.3.3 Transparency of the Model

- **Data Provenance:** Verify data ownership because of the consequences of using models inappropriately trained.
- **Documentation Availability:** Require comprehensive documentation from the vendor, including:
  - Model objectives, scope, and limitations.
  - Methodology, assumptions, and data requirements.
  - Validation results and performance metrics.
- **Explainability:** Ensure the model can be explained to internal stakeholders, regulators, and auditors, even if proprietary components are used.
- **Access to Logic and Testing:** Negotiate rights to inspect or test the model logic, or at minimum, validate inputs and outputs independently.

3.3.4 Independent Validation

- **Internal Validation:** Independently validate vendor models, using available documentation, output testing, benchmarking, and challenge processes.
- **Black-Box Models:** For proprietary "black-box" models, focus validation efforts on input appropriateness, output reasonableness/benchmark assessments, performance monitoring, and testing of extreme scenarios.
- **External Review (if needed):** Consider engaging an independent third-party to supplement internal validation if internal expertise is insufficient.

3.3.5 Monitoring and Change Management

- **Ongoing Monitoring:** Continuously monitor performance and usage, even if the vendor manages maintenance.
- **Change Notification:** Ensure contracts obligate the vendor to notify the institution of all changes, updates, or issues that could affect model performance or assumptions.
- **Internal Approvals:** Subject vendor-initiated changes to internal governance and approval processes before implementation.

3.3.6 Contractual and Regulatory Considerations

- **Service Level Agreements (SLAs):** Define clear SLAs covering support, availability, response times, and update frequency.
- **Compliance Obligations:** Ensure vendor models meet all applicable regulatory, legal, and ethical requirements.
- **Audit Rights:** Include rights for internal audit, regulators, or third parties to review the vendor's processes and controls as needed.
- **Exit Strategy:** Define procedures for transitioning away from the vendor-developed model if necessary, minimizing disruption to business processes.

3.3.7 Summary

Vendor-developed models can deliver significant value, but they demand heightened oversight, transparency, and governance. Institutions remain fully accountable for these models and must ensure they are properly validated, continuously monitored, and fully integrated into the organization's risk management and governance frameworks.

3.4 Machine Learning

Machine Learning (ML) models bring powerful capabilities, enabling the detection of complex patterns in data and delivering highly accurate predictions. However, they also introduce unique challenges that set them apart from traditional rule-based or statistical models. Effectively managing ML models requires adapting established MRM principles to address these differences. This section outlines key considerations for ML models — including AI approaches that do not involve generative AI — to ensure they remain transparent, reliable, and aligned with organizational and regulatory expectations.

3.4.1 Conceptual Soundness and Explainability

- **Fit-for-Purpose:** Confirm that a machine learning approach is appropriate for the business problem and that its added complexity is justified over simpler alternatives.
- **Interpretability:**
  - Use inherently interpretable models (e.g., decision trees, GAMs) if transparency is critical.
  - For "black box" models (e.g., neural networks), supplement with explainability tools (e.g., SHAP, LIME) to identify key drivers and maintain accountability.
- **Bias and Fairness:**
  - Assess for hidden biases in data or algorithms that could lead to discriminatory outcomes.
  - Conduct fairness testing and apply mitigation strategies where disparities are detected.

3.4.2 Data Requirements

- **Volume and Quality:** ML models often require much larger and cleaner datasets than traditional models.
- **Feature Engineering vs. Feature Learning:** Many ML methods implicitly "learn" features, but human-led feature engineering may still improve performance and interpretability.
- **Data Drift Sensitivity:** ML models are particularly sensitive to changes in input distributions (concept drift), requiring robust monitoring.

3.4.3 Model Complexity and Overfitting

- **Overfitting Risk:** ML models are prone to overfitting, especially in high-dimensional spaces or with limited data.
  - Use cross-validation, regularization, dropout (for deep learning), and pruning as appropriate.
- **Hyperparameter Tuning:** Systematically tune hyperparameters using established methods (e.g., grid search, Bayesian optimization) and document choices (see 2.3.4).

3.4.4 Validation and Testing

- **Performance Evaluation:**
  - Ensure that the sample data used to evaluate the model is truly independent, representative of expected application environments, and free from data leakage.
  - Testing strategies should reflect the model's use case and data dynamics.
- **Benchmarking:** Compare ML models against simpler baselines to justify the added complexity.
- **Robustness Checks:** Test sensitivity to outliers, noise, and adversarial inputs where applicable.

3.4.5 Monitoring and Maintenance

- **Performance Decay:** ML models are particularly susceptible to performance deterioration due to evolving data patterns.
- **Drift Detection:** Implement automated/periodic monitoring/backtesting for data drift and concept drift.
- **Re-Training Strategy:** Define triggers for models' re-training/calibration and validation, and redeployed.

3.4.6 Governance and Documentation

- **Transparency of Development Process:** Maintain clear records of architecture, algorithms used, hyperparameters, training procedures, and tuning.
- **Ethical Considerations:** Explicitly evaluate the ethical implications of automated decisions made by ML models.
- **Auditability:** Ensure that the model is auditable despite complexity — retain code, scripts, and random seeds for reproducibility.

3.4.7 Regulatory and Compliance Considerations

- **Regulatory Expectations:** Recognize that regulatory guidance may impose higher standards of explainability and fairness, even if technically complex models perform better.
- **Human Oversight:** Retain meaningful human involvement where required (e.g., under GDPR "right to explanation").

3.4.8 Summary

Machine learning models offer enhanced predictive power and flexibility, but they also introduce greater complexity, reduced transparency, and heightened sensitivity to data drift. Managing these models responsibly requires additional focus on interpretability, robust monitoring, and ethical considerations — all while maintaining adherence to sound MRM principles.

3.5 Generative AI

Generative AI (GenAI) models — including Large Language Models (LLMs), generative adversarial networks (GANs), and diffusion models — represent a distinct class of technology. Unlike traditional predictive or classification models, GenAI models create new content (such as text, images, or audio) based on patterns learned from their training data. These models bring unique risks and challenges, including issues of accuracy, bias, misuse, and explainability, which require tailored governance, oversight, and controls to manage effectively.

3.5.1 Purpose and Appropriateness of Use

- **Use-Case Justification:** Carefully assess whether a generative model is appropriate for the intended task. Avoid use in critical decision-making processes without robust safeguards.
- **Scope Definition:** Clearly define what the model is *and is not* intended to produce (e.g., summaries, suggestions, draft content vs. final automated decisions).

3.5.2 Explainability and Transparency

- **Opacity of Logic:** Recognize that LLMs and other generative models operate as "black boxes" with low interpretability of their internal mechanisms.
- **Output Traceability:** Implement logging and metadata capture to record model prompts, outputs, and context for accountability.

3.5.3 Output Risks

- **Tiering:** Where usage changes, risk categories must include "Uncertain" or "Unknown", due to the creative and dangerous ways that users may interact with them.
- **Hallucination Risk:** Generative models may confidently produce false or fabricated information (hallucinations). Implement human review of outputs before acting on them.
- **Inappropriate or Harmful Content:** Use content filters, prompt engineering, and monitoring to reduce the risk of offensive, biased, or otherwise harmful outputs.
- **Stochasticity:** Acknowledge that outputs may vary for the same input; establish controls for consistency when necessary.

3.5.4 Data Privacy and Intellectual Property

- **Training Data Risks:** LLMs and similar models may have been trained on proprietary, copyrighted, or sensitive data.
- **Output Ownership and Compliance:** Define policies on intellectual property rights and compliance with data privacy regulations when using outputs.

3.5.5 Validation and Monitoring

- **Testing Outputs:** Validate that outputs meet quality, factual accuracy, ethical, and business standards.
- **Scenario-Based Validation:** Test with a range of realistic, edge-case, and adversarial prompts to assess robustness.
- **Monitoring Usage:** Continuously monitor real-world usage and feedback for inappropriate patterns or drift in performance.[5]

3.5.6 Human Oversight and Governance

- **Human-in-the-Loop (HITL):** A requirement for human review and approval for critical use cases. Automating decisions based solely on generative outputs is discouraged.[6]
- **Governance Policies:** Establish clear organizational policies specifying approved use cases, prohibited uses, and escalation procedures for issues.

3.5.7 Regulatory and Ethical Considerations

- **Compliance:** Stay informed about evolving laws and guidelines specific to AI transparency, fairness, and accountability (e.g., EU AI Act, US Blueprint for an AI Bill of Rights).
- **Bias and Fairness:** Assess and mitigate biases that may emerge in generative outputs.
- **Responsible AI Principles:** Align use with ethical principles of fairness, accountability, transparency, and respect for human dignity.
- **Human benchmarking:** • When GenAI deployments replace humans, comparison should be relative to human performance.

3.5.8 Summary

Generative AI models carry distinct risks compared to traditional predictive and classification models, particularly around output quality, ethical use, and accountability. Institutions should approach these models as high-risk tools, ensuring they are deployed only with clear governance, rigorous validation, continuous monitoring, and meaningful human oversight.

3.6 Other Model Types

While the core principles of MRM apply to all models, certain types present unique challenges that merit additional attention. Organizations should adjust

5 Monitoring should consider not only outputs but inputs, i.e., whether they are being used appropriately (e.g., searches for loopholes in policy retrieval documents).

6 Oversight is necessary, but pure HITL is doomed to fail due to the mental demands. Some success is being achieved with AI-augmented HITL.

governance, validation, and monitoring practices to address the specific risks and characteristics of these models effectively. The following sections highlight additional model types that require particular focus and tailored approaches: 1) Expert Judgment, 2) Hybrid, 3) Stress Testing and Scenario, 4) Macroeconomic, 5) Real-Time and High-Frequency, 6) ESG and Sustainability.

3.6.1 Expert Judgment and Models

Expert judgment and expert models are often necessary where a) data is limited or b) the business environment is highly dynamic. Additional governance is needed to ensure they remain appropriate, transparent, defensible, and that the uncertainty of the models is clear.

- **Transparency:** Clearly document the assumptions, rationale, and methodology underlying expert inputs.
- **Validation:** Independently challenge the reasonableness of expert judgments through benchmarking, sensitivity analysis, and backtesting, where possible.
- **Monitoring:** Regularly assess the continued relevance of assumptions as more data becomes available.
- **Bias mitigation:** Guard against cognitive or organizational biases that can distort expert assumptions.
- **Process Audit:** Assess whether the process was fair, balanced, and transparent.[7]
- **Governance:** Ensure governance committees formally review and approve expert-based models with the same rigour as data-driven models.

3.6.2 Hybrid Models

Hybrid models integrate statistical analysis, machine learning, expert judgment, and/or business rules within a single framework. They require additional transparency and governance:

- **Documentation:** Record each component, its assumptions, and its role in the overall model.
- **Interaction Risks:** Identify and monitor potential unintended interactions between components.
- **Validation:** Challenge the individual components and the integrated model as a whole.

[7] Consider whether a) the experts were qualified and properly briefed; b) the range and uncertainty of expert views were documented; c) biases or dominant voices were mitigated; and d) dissent was recorded.

3.6.3 Stress Testing and Scenario Models

Stress testing and scenario models are widely used in capital planning, solvency assessment, and risk management. They rely heavily on expert judgment and forward-looking assumptions:

- **Scenario Design:** Ensure scenarios are transparent, plausible, and aligned with regulatory expectations.
- **Validation:** Focus validation on the plausibility, internal consistency, and sensitivity of results rather than predictive accuracy.
- **Governance:** Subject assumptions and results to independent challenge and senior-level oversight.

3.6.4 Macroeconomic Models

Macroeconomic models support strategic planning, provisioning, and capital adequacy. They are highly sensitive to external forecasts and uncertain trends:

- **Recalibration:** Periodically recalibrate to reflect current economic conditions.
- **Benchmarking:** Compare against alternative forecasts to test for robustness.
- **Documentation:** Clearly record the sources, assumptions, and limitations of macroeconomic inputs.

3.6.5 Real-Time and High-Frequency Models

Real-time and high-frequency models are used in trading, fraud detection, and payments, operating under strict latency and reliability requirements:

- **Operational Controls:** Implement controls to mitigate risks from latency, outages, or anomalies.
- **Data Monitoring:** Continuously monitor the quality and integrity of streaming input data.
- **Contingency Planning:** Establish robust fallback procedures in case of system failures.

3.6.6 ESG and Sustainability Models

Environmental, Social, and Governance (ESG) models are a growing area, often relying on new data and methodologies, to promote an organization's long-term sustainability and responsible behaviour:

- **Assumptions Scrutiny:** Critically assess assumptions and their alignment with evolving ESG standards.
- **Transparency:** Clearly disclose methodologies, data sources, and known limitations.
- **Monitoring:** Reassess models regularly as ESG data quality and standards improve over time.

3.6.7 Pricing Models

The models that guide securities and commodities traders are diverse, including Monte Carlo Simulation, stochastic differential equation, and various physics-inspired methods.

Assumptions: Must be consistent with market conditions.

Validation: Specialist tools are required (e.g., "The Greeks" testing, hedging effectiveness);

4 Regulations and Guidance

This section provides an overview of key international and regional regulations, guidelines, and best practices that inform model risk management standards worldwide. It summarizes major initiatives and supervisory expectations across North America, Europe, Africa, and Asia-Pacific, along with cross-cutting considerations such as data privacy laws.

Each subsection highlights notable regulatory documents, their scope, and their relevance to internal model governance. Together, they reflect the growing global alignment around core principles — transparency, independent validation, and effective oversight — even in jurisdictions where formal, standalone MRM regulations have yet to emerge.

4.1 International

- **Acronyms**:
  - **BCBS:** Basel Committee on Banking Supervision.
  - **ICAAP:** Internal Capital Adequacy Assessment Process.
  - **IFRS:** International Financial Reporting Standard.
  - **SREP:** Supervisory Review and Evaluation Process
- **Basel Framework:**
  - While not a regulation per se, BCBS principles under Basel II/III Pillar 2 require banks to properly validate, govern, and oversee internal models used for regulatory capital.
  - ICAAP and SREP are the vehicles through which model governance is assessed.
- **IFRS 9:** Applies globally (but strongly enforced in the EU); mandates forward-looking Expected Credit Loss (ECL) models for financial reporting, requiring transparency and governance.
- **ICAAP:** A self-assessment process that evaluates internal capital adequacy under normal and stressed conditions, relative to its business strategy, risk profile, and regulatory requirements.

Many jurisdictions do not yet have a standalone MRM regulation; however, they expect firms to follow principles set out in SR 11-7, Basel Pillar 2, or ECB TRIM. Regions like French West Africa, Southeast Asia, and parts of Latin America are increasingly referencing these global best practices in ICAAP reviews and supervisory expectations. Data privacy laws, such as GDPR (EU) and CCPA (California), also impact how personal data is used in models globally.

4.2 North America

4.2.1 United States

- **Acronyms:**
  - **CCAR:** Comprehensive Capital Analysis and Review
  - **CCPA:** California Consumer Privacy Act: A state-level privacy law, effective January 1, 2020, that grants residents rights over their personal data and imposes obligations on businesses that collect or sell such data
  - **FRB:** Federal Reserve Board of the Federal Reserve Bank (national).
  - **OCC:** Office of the Comptroller of the Currency.
  - **SR:** Supervisory Release.
  - **DFAST:** Dodd–Frank Act Stress Test..
- **SR 11-7 and OCC Bulletin 2011-12 (2011):**
  - Guidance issued by the FRB, but used as a template internationally.
  - Identical texts defining principles, emphasizing model development, validation, governance, documentation, and independent oversight.
  - Both are titled “Supervisory Guidance on Model Risk Management.”
  - SR 11-7 for institutions of all sizes under FRB supervision.
  - OCC Bulletin for OCC-supervised institutions.
- **CCAR (2011)**: An annual FRB exercise requiring banks to demonstrate sound capital planning and stress testing, with emphasis on robust, validated models.
- **DFAST (2012)**: Mandates periodic stress tests to ensure credible and well-governed models.
- **CCPA (2020):** A state-level privacy law that grants residents rights over their personal data and imposes obligations on businesses that collect/sell such data.

4.2.2 Canada

- **Acronyms:**
  - **E-23:** Enterprise-Wide Model Risk Management for Deposit-Taking Institutions.
  - **OSFI:** Office of the Superintendent of Financial Institutions.
- **E-23 (2017, OSFI):**
  - Closely modelled on SR 11-7, it outlines principles and expectations for managing model risk throughout the lifecycle.
  - Applied to federally regulated deposit-taking institutions (banks and similar).

- While less prescriptive than SR 11-7, it emphasizes proportionality — meaning smaller institutions can scale controls to the complexity and materiality of their models.

4.3 Europe

4.3.1 European Union / Eurozone

- **Acronyms:**
  - **EBA:** European Banking Authority.
  - **ECB:** European Central Bank.
  - **EEA:** European Economic Area.
  - **EU:** European Union.
  - **GDPR:** General Data Protection Regulation.
  - **GL/2021/05:** Guidelines on Internal Governance.
  - **TRIM:** Targeted Review of Internal Models.
- **TRIM (2016–2021, ECB):**
  - A multi-year initiative to assess internal models used for Pillar 1 capital requirements (credit, market, counterparty risk) across significant banks in the eurozone.
  - Ensures compliance, consistency, and reliability of internal models.
- **Solvency II (2016, EEA)**: Mandates strict validation, governance, and documentation of internal models used by insurers.
- **GDPR (2018, EU):** Requires that personal data used in models be collected, stored, and processed lawfully, transparently, and with proper safeguards.
- **GL/2021/05 (2021, EBA):** Guidance outlining governance and control expectations for internal models and risk management practices.

4.3.2 United Kingdom

- **Acronyms:**
  - **PRA:** Prudential Regulation Authority:
  - **SS1/23:** Supervisory Statement re Principles for Model Risk Management.
- **PRA SS1/23 (2023):**
  - Adapts and formalizes principles similar to SR 11-7 for UK-regulated firms, reflecting post-Brexit supervisory priorities.
  - Focuses on the model lifecycle, tiering, governance, and independent validation.

4.4 Africa (including French West Africa)

4.4.1 French West Africa

- **Acronyms:**
  - **BCEAO:** Banque Centrale des États de l'Afrique de l'Ouest (Central Bank of West African States.
  - **UEMOA**: Union Économique et Monétaire Ouest-Africaine (West African Economic and Monetary Union.
- **BCEAO Guidelines:**
  - Provides general guidance for UEMOA banks.
  - There is no dedicated MRM regulation yet, but banks are expected to align with Basel II/III Pillar 2 principles, including internal model governance and ICAAP.
  - Local central banks often reference ECB/BCBS principles informally.

4.4.2 South Africa

- **Acronyms:**
  - **SARB:** South African Reserve Bank.
- **SARB:**
  - Applies Basel standards and emphasizes sound risk management and internal model validation through ICAAP submissions.
  - No formal "MRM" guidance document, but banks use SR 11-7 as a benchmark.

4.5 Asia-Pacific

4.5.1 Hong Kong

- **Acronyms:**
  - **CR-G-5**: HKMA guidance on Country Risk Management.
  - **HKMA:** Hong Kong Monetary Authority.
- **CR-G-5 (2001)**: Module validation expectations for country-level credit risk management included within the HKMA Supervisory Policy Manual.

4.5.2 Singapore

- **Acronyms:**
  - **MAS:** Monetary Authority of Singapore.
- **MAS Guidelines (2024):**
  - An "Information Paper" on AI Model Risk Management
  - It outlines key practices across AI model governance, risk systems, development and validation, deployment, monitoring, and Generative AI risks.

  - This aligns MAS with other major regulators (Basel Committee, SR 11-7) in requiring robust oversight, validation controls, inventories, documentation, and ICAAP-style risk-based assessments.

4.5.3 Thailand and Malaysia

- **Acronyms:**
  - **BOT**: Bank of Thailand.
  - **BNM**: Bank Negara Malaysia.
- **BOT and BNM:** Local regulators provide guidance aligned with Basel II/III on internal models and stress testing, emphasizing validation and governance.

4.6 Checklist

There are many commonalities across the guidance and regulations presented above. The following is an overarching checklist that will help institutions ensure that they tick all the boxes.

4.6.1 Governance & Policy

- A formal, board-approved **Model Risk Management (MRM) policy** exists and is regularly reviewed.
- Clear **roles and responsibilities** (e.g., RACI) are defined for model development, validation, approval, use, and oversight.
- A dedicated **Model Risk Committee** (or equivalent governance body) oversees MRM activities and escalates key issues to senior management and the board.

4.6.2 Model Inventory & Documentation

- A complete and current **model inventory** exists, covering all models, tools, and calculators in use.
- Models are **classified or tiered** by materiality and risk level.
- Comprehensive **model documentation** exists and is kept up to date, including:
  - Methodology and conceptual soundness.
  - Assumptions and limitations.
  - Development history and implementation details.

4.6.3 Development & Implementation

- Models are designed to be **conceptually sound**, with an appropriate purpose and justification for use.
- The **development process** includes proper controls, reviews, and approvals before deployment.
- Data used in development is **accurate, complete, and compliant with privacy regulations** (e.g., GDPR, CCPA).

4.6.4 Validation & Testing

- All models are subject to **independent validation**, separate from the development team.
- Validation is performed **both initially (pre-implementation) and periodically thereafter**.
- Validation findings are **documented, communicated, and addressed** before models are put into production.
- Routine **backtesting, benchmarking, and sensitivity testing** are performed to assess performance.

4.6.5 Monitoring & Change Management

- Ongoing **monitoring of model performance** is conducted, with key metrics tracked (e.g., stability, predictive power, drift).
- Defined **thresholds and triggers** are in place to detect material deterioration or changes in model behaviour.
- A structured **change management process** exists for model updates, with proper review and approval.
- Model-related incidents or breaches are logged and investigated.

4.6.6 Data Protection & Privacy

- Personal data used in models is processed in compliance with **GDPR, CCPA, and/or local privacy laws**.
- Individuals' rights over their personal data (e.g., right to know, right to delete) are respected in model processes.
- Data access and retention are controlled and limited to authorized purposes.

4.6.7 Stress Testing & Capital Adequacy (where applicable)

- Models used for **CCAR, DFAST, ICAAP, SREP, or Solvency II** meet regulatory expectations and are properly documented.
- **Stress testing assumptions and scenarios** are well-founded, transparent, and regularly reviewed.
- Model outputs for capital adequacy are consistent, reliable, and defensible under regulatory scrutiny.

5 Conclusion

Effective model risk management is essential to ensuring that all models — whether traditional, vendor-developed, machine learning, or generative AI — perform reliably, remain transparent, and align with both organizational objectives and regulatory expectations.

5.1 Principles

This document has outlined **core principles** for every stage of the model life cycle:

- **Model Development**, ensuring models are purpose-built, rigorously tested, and appropriately documented.
- **Model Validation**, providing independent assurance of conceptual soundness, performance, and fitness-for-use.
- **Organization and Governance**, establishing accountability, clear roles, and a culture of challenge supported by robust oversight structures.
- **Documentation**, maintaining transparency, reproducibility, and auditability across the model's history.
- **Life Cycle Management**, monitoring and managing models from conception to retirement with proper controls at every stage.

5.2 Special Considerations

We have also addressed special considerations that arise in specific contexts:

- **Business Areas**: Variations in approach, whether operational or financial.
- **Smaller Institutions**: Proportionate application of principles considering materiality and practicality.
- **Vendor-developed Models**: Require strong oversight, clear accountability, and thorough validation despite their external origins.
- **Machine learning Models:** Introduce added complexity, lower interpretability, and heightened sensitivity to data drift.
- **Generative AI Models:** Bring unique ethical, legal, and operational risks that demand tailored governance and meaningful human oversight.

Across all of these areas, one principle remains constant: accountability. Organizations are fully responsible for the models they rely on, regardless of who developed them or how sophisticated they may be. Maintaining sound governance, rigorous controls, clear documentation, and continuous monitoring is essential to preserving confidence in model outputs and mitigating potential risks. By applying the principles and practices outlined in this document, organizations can harness the full potential of advanced modelling techniques while safeguarding their integrity, stakeholders, and reputation.

5.3 Regulations and Guidance

The global regulatory landscape for model risk management reflects both alignment and divergence. Foundational principles — rooted in Basel Committee guidance, ECB TRIM, and U.S. SR 11-7 — are widely recognized, yet national regulations vary significantly in formality, prescriptiveness, and timelines. Regions such as the EU, U.S., and UK have issued clear supervisory statements, while others, including parts of Africa and Southeast Asia, apply these principles more informally or proportionately through ICAAP reviews.

For institutions operating across jurisdictions, navigating this patchwork of expectations requires more than compliance with local rules. A comprehensive, jurisdiction-agnostic model risk management checklist — grounded in universal best practices for governance, documentation, validation, monitoring, and data privacy — provides a robust benchmark. Mapping local requirements against such a standard ensures consistency, resilience, and defensibility across operations.

By embedding these global principles throughout the organization, firms can maintain compliance, strengthen oversight, and enhance operational resilience in an increasingly complex supervisory environment.

6 Glossary of Terms

accountability: obligation and expectation to take ownership of specific tasks, decisions, or outcomes.

AI (Artificial Intelligence): Systems and algorithms that perform tasks typically requiring human intelligence (reasoning, learning, problem-solving, decision-making, perception, and language understanding).

algorithm: A set of rules or procedures for solving a problem or performing calculations, forming the basis of a model.

assumption: Statement or condition accepted as true in the model's design, which should be tested and documented.

AUC (Area Under the Curve): For randomly chosen cases, the probability that a binary classifier will rank true higher than false.

backtest: The comparison of a model's predictions against historical data to assess performance.

benchmark: A reference point — such as a standard, model, or set of results — used to compare, assess, and evaluate the performance, reasonableness, or appropriateness of another model.

bias: Systematic error in a model's outputs due to flaws in data, assumptions, or methodology.

black Box: A model whose internal workings and decision logic are opaque and difficult to understand.

calibration: The extent to which predicted probabilities or values align with observed outcomes.

central repository: A secure and accessible system where all model documentation, code, and outputs are stored.

challenger: An alternative model developed to test or potentially replace an existing model.

change: any modification to design, inputs, assumptions, methodology, or use after implementation; **~ log:** A documented record of all modifications made to a model, including rationale, date, and approver.

classification model: A model that assigns observations to predefined categories or classes.

concept: (1) An abstract idea, principle, or mental representation that defines the meaning, purpose, or intended use of something; (2) the foundational idea or rationale behind a system, model, or method; **~ drift:** changes in the statistical relationship between input variables (features) and the target variable that a model is trained to learn.

conceptual soundness: The degree to which the model's design and methodology logically reflect the intended real-world phenomenon.

contingency: An event that may or may not occur in the future; **~ plan:** Predefined actions to respond effectively to potential disruptions or unexpected events.

control: a process or mechanism to ensure a model is used correctly, performs as intended, and stays within acceptable risk limits.

cross-validation: A technique for assessing model performance by dividing the data into multiple training and testing splits.

data: Raw facts, figures, or observations (numbers, text, symbols) regarding events, objects, or conditions, that are recorded, stored, and analyzed; **~ drift:** Gradual changes in the statistical properties of input data over time that can degrade model performance; **~ governance:** Policies and practices for managing the availability, integrity, security, and usability of data used in models; **~ lineage:** A record of where data originates, how it moves through systems, and how it is transformed; **~ protection:** The practices, policies, and technologies used to safeguard personal or sensitive data from unauthorized access, misuse, alteration, loss, or destruction.

decommission: To retire a model and remove it from active use through a formal process.

deposit-taking institution: Entity authorized to accept money from the public in the form of deposits, which are repayable on demand or after a fixed term, and to use those funds to make loans or investments.

development: Phase where models, systems, or processes are designed, built, and tested in a controlled (non-production) environment.

discrimination: A measure of a model's ability to distinguish between different outcomes, often assessed using metrics like ROC-AUC.

documentation: Written, organized collections of materials that describe business processes, their purpose, steps, participants, inputs, outputs, rules, controls, and supporting systems — in a way that enables understanding, execution, oversight, and improvement by others.. **~ standards:** Organizational guidelines for how models should be documented to ensure clarity and consistency.

Dodd-Frank Act (2010): a sweeping U.S. financial reform law passed after the 2007–8 global economic crisis to promote financial system stability.

drift: A gradual, often unintentional change in a model's inputs and/or outputs over time; **~ detection:** The identification of deviations from expected patterns.

due diligence: A thorough review to assess risks, suitability, and compliance before making a decision or commitment.

EBA: Ensures the prudential regulation and supervision of banks in the European Union.

ECB: the central bank for the euro currency and the eurozone (EU countries that use the euro).

empirical: Based on observation, experience, or experiment rather than theory or pure logic.

ESG (Environmental, Social, and Governance): A framework for assessing an organization's performance with respect to broader society.

EU: A political and economic union of countries that have agreed to work together under shared laws, institutions, and policies.

exception: Instance where a model's performance, behaviour, or use deviates from approved expectations, thresholds, or intended scope.

exogenous: Originating from outside a system, model, or process and not determined by it.

expert: A person with deep knowledge, skill, and experience recognized, able to provide reliable insights, analysis, or decisions in a specific domain; **~ model:** One whose design, structure, parameters, or weights are largely or partly based upon expertise as opposed to empirical data.

explainable: Whether a system, model, process, or decision is understandable and interpretable by humans. **~ AI (XAI):** Methods and practices to make the inner workings of complex AI models more interpretable.

external: Originating from or located outside a given system, organization, or boundary; **~ data:** obtained from outside the organization; **~ library:** computer code developed outside the current project or business area.

fair: impartial, equitable, and just; free from bias, favouritism, or unjust discrimination.

feature: An input variable used by a model. **~ engineering:** The process of creating, transforming, or selecting input variables to improve model performance.

FRB (Federal Reserve Board): The "Board of Governors of the Federal Reserve System", which oversees the 12 regional Federal Reserve Banks.

GDPR: Data privacy and protection law enacted by the European Union.

Gini: A model's discriminatory power, scaled from 0 (no discrimination) to 1 (perfect discrimination).

governance: Rules, processes, roles, and oversight mechanisms that ensure decisions and activities are carried out responsibly, transparently, and in alignment with objectives, policies, and regulatory obligations. **~ committee:** A body that oversees model risk management activities, approvals, and escalations.

holdout dataset: A reserved portion of data used to test the final model's out-of-sample performance.

human: Relating to a person or people; **~ oversight:** Active supervision, review, and intervention to ensure operation is correct, legal/ethical, and with intended results; **~ resources:** The workforce and the function or department responsible for managing them.

hybrid: Something that combines elements of two or more different types, systems, or approaches to create a single, integrated solution; **~ model:** One that combines judgment and empiricism.

hyperparameter: A configurable setting that defines how a machine learning algorithm learns from data, which is set before training and not estimated by the model itself. **~ tuning:** The process of optimizing parameters that govern a model's learning process.

implement: To put a plan, model, system, or process into effect by deploying it for actual use in its intended environment.

incident: An event where a model behaves unexpectedly or fails, thus requiring investigation due to potential added risks.

independent validation: An unbiased assessment of a model by a team not involved in its development.

institutional knowledge: The collective understanding, experience, practices, and information accumulated over time of how things are done, why, and what has worked (or not) in the past.

interpretability: The ability to understand how and why a model produces its outputs.

judgment: opinion or evaluation based on knowledge, experience, reasoning, and values rather than solely on mechanical rules or quantitative models.

KPI: Key Performance Indicator, any metric used to assess and monitor model-related risk.

KS (Kolmogorov–Smirnov statistic): The maximum difference between the cumulative distributions of good and bad (or two classes), indicating how well a model separates them.

LIME (Local Interpretable Model-agnostic Explanations): A technique that explains the predictions of any machine learning model by approximating it locally with a simple, interpretable model.

machine learning: A subset of artificial intelligence in which algorithms learn patterns from data to make predictions or decisions without being explicitly programmed.

macroeconomic: Relating to the broader economy, rather than individual markets or actors.

materiality: The potential impact a model has on business decisions or risk exposure, used to determine its priority.

metadata: data that describes and provides information about other data, such as its source, structure, or context.

methodology: structured, systematic approach and set of techniques, assumptions, and procedures used to design, develop, and implement a model that serves a specific business or financial purpose.

metric: a quantitative measure used to assess performance, quality, or progress toward a specific object.

mitigate: to reduce the severity, impact, or likelihood of a risk.

ML: machine learning.

model: a quantitative or qualitative method, system, or approach that processes inputs and applies assumptions and algorithms to produce outputs that support decision-making, analysis, or risk measurement. **~ card:** A standardized report summarizing a model's purpose, design, performance, and limitations. **~ inventory:** A complete list of all models in use, under development, or retired.

model risk: The potential for adverse consequences arising from decisions based on incorrect, misused, or underperforming models. **~ management (MRM):** A systematic framework of policies, processes, roles, and controls designed to identify, assess, mitigate, monitor, and report the risks associated with the use of models.

monitoring: Ongoing observation, measurement, and assessment to detect changes, ensure performance, or identify issues.

MRM: model risk management.

OCC (Office of the Comptroller of the Currency): federal agency (USA) that charters, regulates, and supervises national banks, federal savings associations, and federally licensed branches and agencies of foreign banks.

originations: Processes dedicated to reviewing applications from new and existing customers.

outlier: Data point(s) that are unusually far from the rest of the data and may distort model results.

out-of-sample data: Data not used for model training but rather to assess generalization, whether from the same or another period (holdout versus out-of-time).

out-of-time data: Data from a later period that can be used to assess data and model output drift.

overfit: Model training such that it performs well on training data but poorly on new data.

overlay: adjustment (usually expert) to a model's output reflecting factors not captured by the model.

performance metric: A quantitative measure of how well a model achieves its intended purpose.

predictive: The ability to forecast, estimate, or anticipate future outcomes or behaviours based on current or historical data, patterns, or models; **~ accuracy:** A measure of how close model predictions are to actual outcomes, which is related to but different from predictive power; **~ power:** The ability of a model to discriminate between outcomes, i.e. to rank-order or make correct classifications.

principle: a fundamental rule or guideline that informs decisions and actions to achieve consistent, sound outcomes.

procyclicality: The tendency of models to reinforce economic or financial cycles, potentially amplifying risks.

production: The operational environment where models, systems, or processes use real-world (current) data to generate outputs or decisions.

proportionality: The principle that controls should be commensurate with the probability and potential severity of a model's faltering.

regulation: rules, requirements, and standards imposed by a governing authority to achieve specific public policy objectives.

regularization: A technique to prevent overfitting by adding penalties to overly complex models.

reproducible: Able to replicate a model's results using the same data and methodology.

residual: The difference between a model's predicted value and the actual observed value.

responsibility: the obligation to carry out a task and be answerable for its outcome.

risk appetite: The level of risk an organization is willing to accept in pursuit of its objectives, applied here to model risk.

risk tier: A classification to indicate the probability and potential impact on the organization if the model fails, is misused, or underperforms.

RMSE (Root Mean Squared Error): A measure of prediction error; the square root of the average squared differences between predicted and actual values, indicating model accuracy.

robust: Strong, reliable, and effective even when subjected to stress, uncertainty, variability, or adverse conditions.

role: A function or set of responsibilities performed by an individual or group within a process or organization.

reserve bank: An institution responsible for managing a country's or region's monetary policy, financial stability, and currency.

ROC (Receiver Operating Characteristic): Graphical plot indicating a model's ability to distinguish between two classes.

SARB (South African Reserve Bank): National reserve bank.

scenario: A possible future state or situation for the purpose of planning, analysis, or testing. **~ analysis:** A performance evaluation under a range of defined, hypothetical scenarios.

scope: Defined boundaries, extent, and focus of an activity, process, or assessment — specifying what is included, what is excluded, and the objectives to be achieved.

security: measures to protect assets, systems, and data from unauthorized access, misuse, or harm.

sensitivity: (1) The degree to which someone or something responds to, detects, or is affected by changes, stimuli, or conditions. (2) The ability of a system, model, or test to detect a condition or event when it is actually present; **~ analysis:** Assessing how changes in inputs affect model outputs.

SHAP (SHapley Additive exPlanations): A method based on cooperative game theory that explains the contribution of each feature to a model's prediction by fairly attributing the output among the input features.

SR 11-7: A U.S. Federal Reserve and OCC supervisory guidance titled "Supervisory Guidance on Model Risk Management," issued in April 2011, which outlines principles for managing risks associated with models in banks and financial institutions..

stability: Consistency over time, whether data values/quality, model outputs, or business processes. **~ testing:** Checking whether data and models' performance remains consistent over time and across different segments.

stress: Subject a model or process to plausible but extreme, adverse, or unusual conditions that test its limits and reveal vulnerabilities.

supervisory expectations: Regulatory guidance on how models should be developed, validated, and governed.

testing: Evaluation of a system, process, model, or component under controlled conditions to determine whether it performs as intended.

threshold: A defined point or limit that indicates potential problems that suggest a change, action, or response is required (see also *trigger*).

transparency: Clarity of understanding and the ability to communicate models' data, development methodology and outputs.

training: The process of fitting a model to a dataset by adjusting its parameters to learn patterns and relationships that minimize error or maximize predictive accuracy. **~ dataset:** The data used to fit a model's parameters during development.

trigger: A specific event or condition that initiates a predefined action, response, or process.

TRIM (Targeted Review of Internal Models): An ECB project (2016–2021) that reviewed banks' capital requirement models and procedures.

UEMOA (Union Économique et Monétaire Ouest-Africaine): regional economic and monetary union of eight West African countries, aimed at promoting economic integration and sharing a common currency.

users: Individuals who interact with or rely on a system, process, model, or service to perform their work, make decisions, or achieve specific objectives.

validation: An independent assessment to determine whether inputs and outputs are fit for purpose and consistent with internal standards and regulatory expectations.

version control: The systematic tracking of changes to model code, documentation, and configuration.

white box: A model whose internal workings and decision logic are transparent and understandable.

7 Index