UBS

Public

From Risk Model Governance to Model Risk Governance

Risk Day 2021

Michael Amrein, Dr. sc. ETH Zürich, Aktuar SAV
Head AI, Monitoring & Surveillance Models Validation
Model Risk Management & Control

September 17, 2021

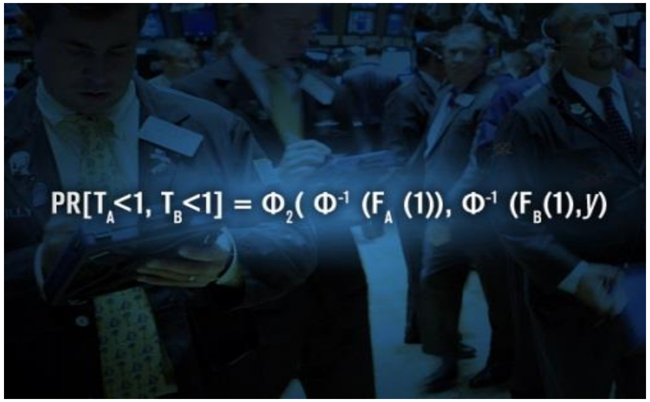
Disclaimer

The views and opinions expressed in this presentation are those of the author, may not reflect the views and opinions of UBS and should not be cited as being those of UBS.

This document/presentation and the information contained herein are provided solely for information purposes, and are not to be construed as a solicitation of an offer to buy or sell any securities or other financial instruments in Switzerland, the United States or any other jurisdiction. No investment decision relating to securities of or relating to UBS AG or its affiliates should be made on the basis of this document. Refer to UBS's first and second quarter 2021 report and its Annual Report on Form 20-F for the year ended 31 December 2020 for additional information. These reports are available at www.ubs.com/investors. No representation or warranty is made or implied concerning, and UBS assumes no responsibility for, the accuracy, completeness, reliability or comparability of the information contained herein relating to third parties, which is based solely on publicly available information.

Model Risk

Growing relevance of model risk in the financial industry due to increasing reliance on models.

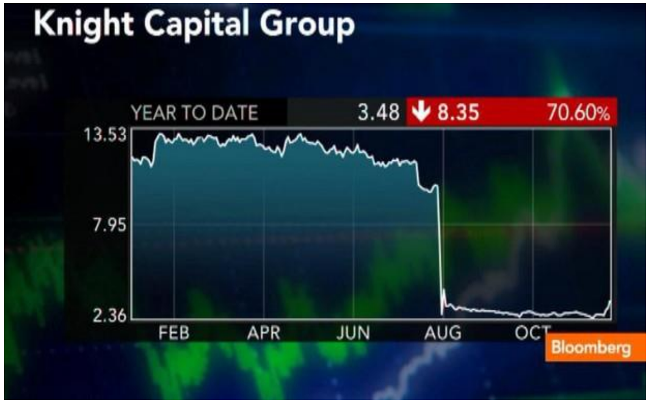


Recipe for Disaster: The Formula That Killed Wall Street

(WIRED, Feb 23, 2009)

Relevance: Rating agencies and banks underestimated both the probability and magnitude of stress losses as well as default correlation.

Impact: Large U.S. and European banks lost more than $ 1tn on toxic assets between 2007 and 2009.



Software Testing Lessons Learned From Knight Capital Fiasco

(CIO, Aug 14, 2012)

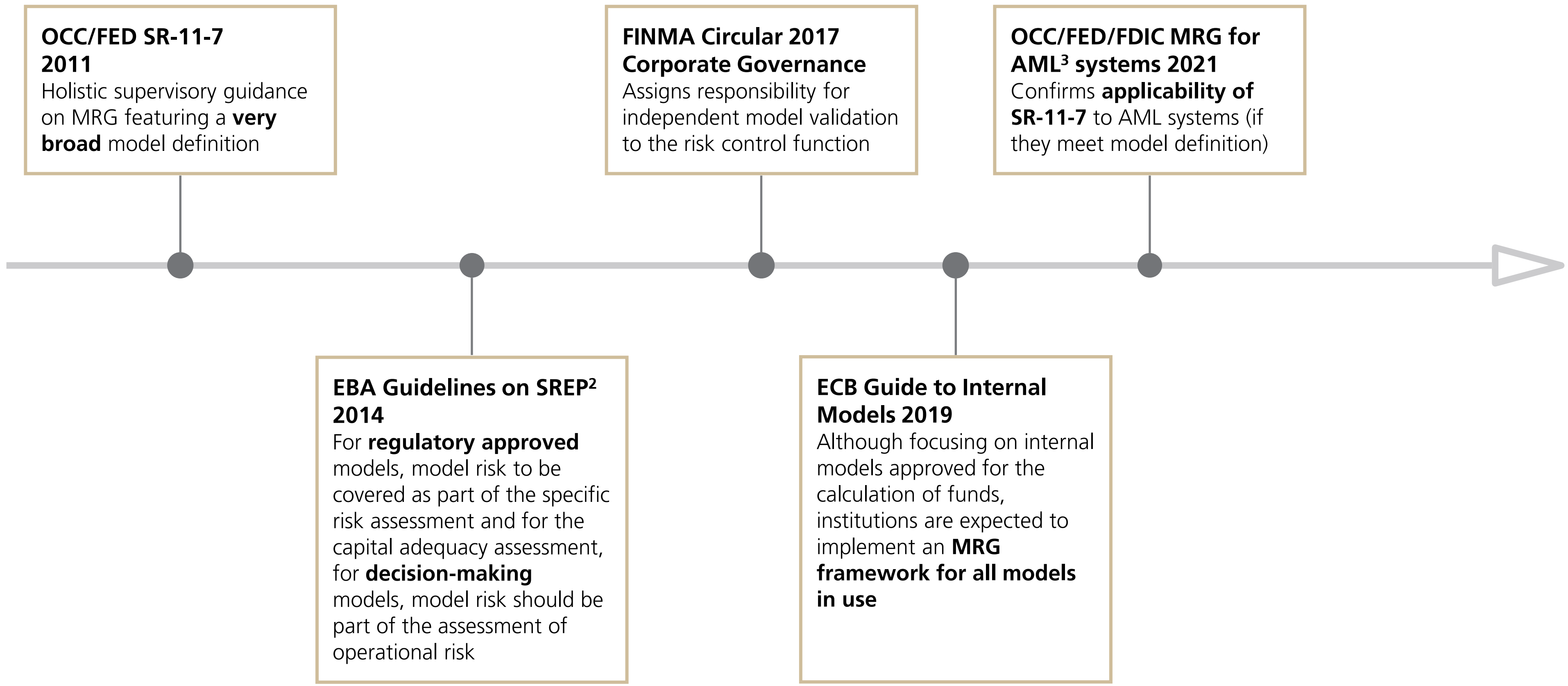
Relevance: Inadequate testing before production release of a trading algorithm. "It was a software bug [...]. It happened to be a very large software bug." Knight Capital CEO Thomas Joyce.

Impact: One defect in a trading algorithm caused Knight Capital to lose $ 440m in about 30 minutes.

***Model risk** is the risk of adverse consequences resulting from decisions based on incorrect or misused model outputs and reports.*

Some MRG[1] Regulatory Milestones

Over the past years, regulatory bodies confirmed that global banks need to implement a comprehensive MRG framework with coverage beyond the traditional models (minimum and economic capital, stress testing, liquidity, valuation).



OCC/FED SR-11-7 2011
Holistic supervisory guidance on MRG featuring a **very broad** model definition

EBA Guidelines on SREP[2] 2014
For **regulatory approved** models, model risk to be covered as part of the specific risk assessment and for the capital adequacy assessment, for **decision-making** models, model risk should be part of the assessment of operational risk

FINMA Circular 2017 Corporate Governance
Assigns responsibility for independent model validation to the risk control function

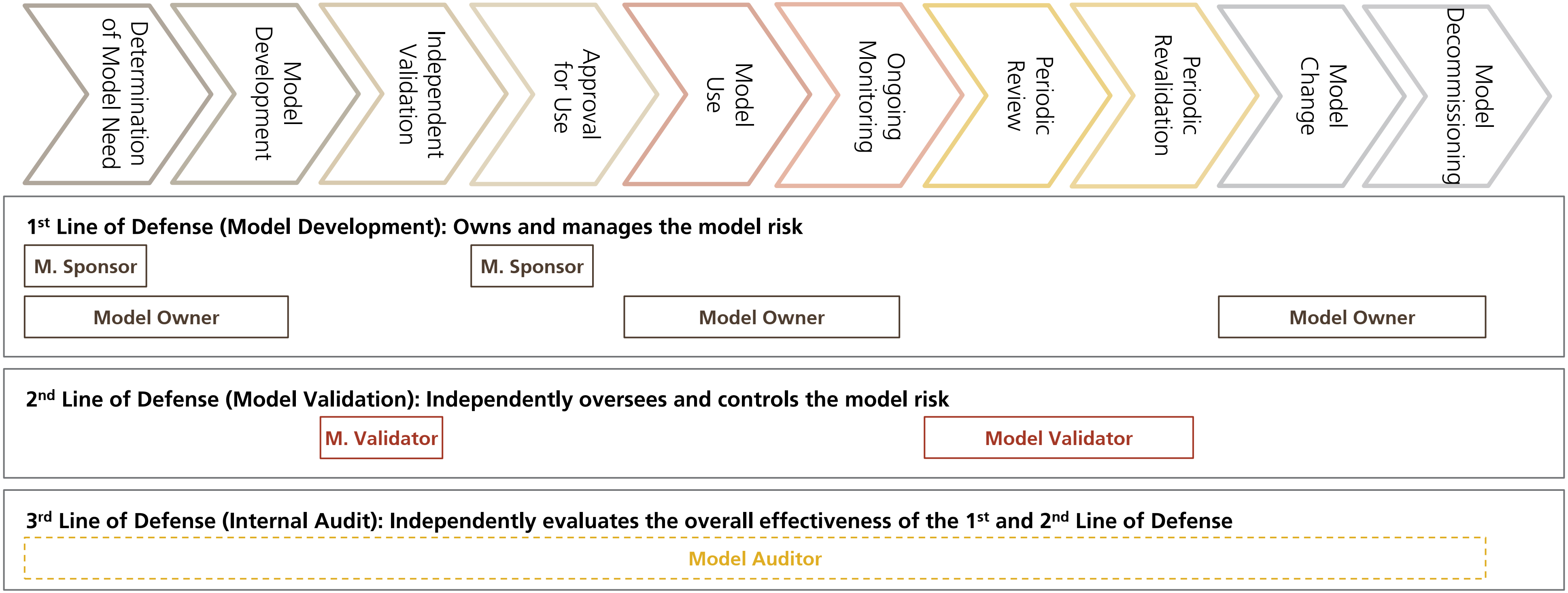
ECB Guide to Internal Models 2019
Although focusing on internal models approved for the calculation of funds, institutions are expected to implement an **MRG framework for all models in use**

OCC/FED/FDIC MRG for AML[3] systems 2021
Confirms **applicability of SR-11-7** to AML systems (if they meet model definition)

[1] MRG: Model Risk Governance
[2] SREP: Supervisory Review and Evaluation Process
[3] AML: Anti-Money Laundering

MRG Processes, Roles and Responsibilities in a Nutshell

Like any other risk, model risk should be managed via three lines of defense over the model's lifecycle.



1st Line of Defense (Model Development): Owns and manages the model risk

2nd Line of Defense (Model Validation): Independently oversees and controls the model risk

3rd Line of Defense (Internal Audit): Independently evaluates the overall effectiveness of the 1st and 2nd Line of Defense

Model Sponsor

- Has budget authority to commission models for development to meet business needs
- Has approval for use authority for models approved by the 2nd Line of Defense

Model Owner

- Responsible for model risk and its management throughout the model's lifecycle
- Ensures that model development (including documentation and implementation), use and ongoing monitoring is performed in line with policies
- Remediates issues identified by the 2nd Line of Defense

Model Validator

- Provides independent assessment and effective challenge of model risk along a model's lifecycle
- Performs independent model reviews and raises issues (if applicable) in line with policies

UBS

Key Aspects of the MRG Enhancement

Extension to new areas, holistic model risk coverage including risk appetite setting and enhanced reporting capacity.

Onboarding existing systems to MRG
Extension of MRG framework to existing, non-traditional models, used for example in the context of Monitoring & Surveillance of Operational Risks and Algorithmic Trading

Artificial Intelligence and Machine Learning
Increasing adoption of Artificial Intelligence and Machine Learning across the bank, especially also in areas not using models previously

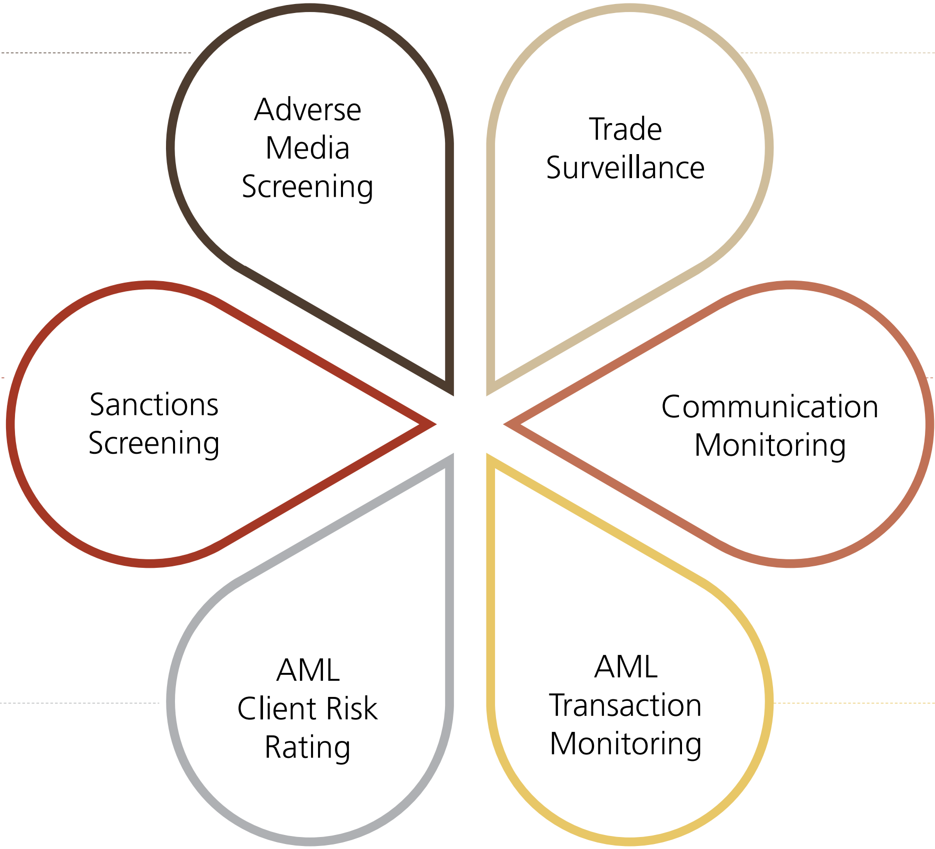
Holistic coverage of model risks at individual model level
Development and independent reviews moved away from a methodology-centric approach to holistic coverage of input, methodology, implementation and use including ongoing performance monitoring

Model Risk Measurement and Appetite
Model Risk Measurement and formulation of Model Risk Appetite not only on an individual model level but also in the aggregate

Reporting & Monitoring
Reporting & monitoring of the governance status of individual models as well as in the aggregate for senior management, auditors and regulators

Onboarding Existing Systems: M&S[1] Models – Model Landscape

M&S models are typically alert generators to identify various types of suspicious activities and patterns. Alerts are reviewed by experts for potential escalation.



Identify financial crime relevant news articles from various media sources concerning UBS clients or prospects

Identify references to sanctioned entities, individuals or regions within payment messages in order to prevent the transaction

Produce AML risk ratings which drive the frequency/depth of periodic client reviews as well as the level of alerting thresholds in downstream transaction monitoring systems (not alert generating)

Detect potential cases of market misconduct (e.g., insider trading, front running and trades away from the market price)

Detect potential compliance breaches in electronic messages (chats, e-mails, etc.) and audio communication (landline, mobile, Skype) of targeted UBS employees

Detect suspicious client transactions relating to money laundering (e.g., changes in transaction behavior, transactions involving high risk jurisdictions, flow through)

[1] M&S: Monitoring & Surveillance

Onboarding of Existing Systems: M&S Models – Characteristics & Model Risk

Use

- Many models monitor key operational risks (Financial Crime, Market Conduct)
- Alerts go through an expert review process and might ultimately lead to a regulatory filing

Input data

- Large amounts of data (trades, orders, text, audio, transactions, payments, client data), typically sourced from core systems
- Processing is usually automated

Methodology

- Monthly, daily or event based execution of the alerting logic
- Many submodels based on rules with many tunable parameters, statistical anomaly detection and/or Machine Learning

Implementation

- Inhouse built systems as well as on- and off-premise vendor solutions
- Implementation under resposibility of the IT department

⚠ Key model risk are false negatives (Type II error)

The model does not produce an alert when it should have (false alerts “only” lead to extra effort and are well controlled through alert review)

✓ Key testing / controls

Regular reviews of non-alerting cases / Below-the-Line testing
Regular testing with synthetic data
Regular coverage assessments (regulatory/internal requirements)

UBS

Artificial Intelligence and Machine Learning: Newly Emerging Use Cases - Challenges

There are challenges to adapt the framework to AI/ML[1] as it enables applications in formerly MRG-remote areas rather than introducing fundamentally new model risks[2].

MRG Awareness

Increase awareness and understanding of the model governance process, the roles it defines, the model lifecycle requirements and its benefits in AI/ML development teams of solution owners

Model Identification

Identify AI/ML models in areas of the bank that have no standing collaboration with Model Risk Governance & Control units

Delineation to risks controlled by other functions (Compliance, Legal, Information Security)

Are the below model risks?

- Logic embedded in a trading algorithm places disadvantage to certain clients or manipulates the market
- Predictions of employee misconduct resulting in investigations prior to any wrong-doing
- Deployment of self-adapting software whose behavior changes without a release
- Algorithmic support in job candidate screening tools resulting in a preference for a particular nationality/gender/ethnicity

[1] AI/ML: Artificial Intelligence / Machine Learning

[2] AI/ML clearly amplifies risks in the areas of fairness & bias, explainability & interpretability, ethics and control of model outcomes (self-learning)

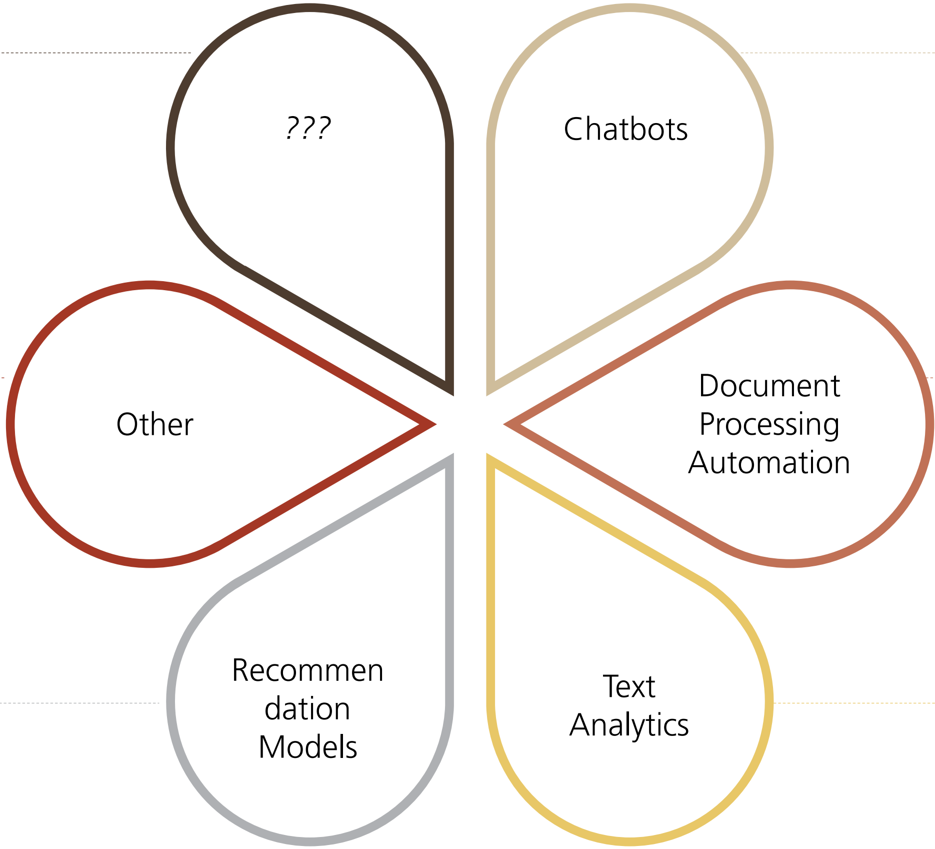
Artificial Intelligence and Machine Learning: Newly Emerging Use Cases – Model Landscape

Many new AI models currently used in production present minimal model risks due to their business use.

The AI/ML area is in its infancy and further use cases are investigated

Various models utilizing AI for forecasting, classification, or anomaly detection (e.g., predict work volumes for Group Operations, identify abnormal behavior in log patterns)

Suggest to a client advisor products that might be of interest to their clients based on client attributes, portfolio characteristics, market information, and other sources



Consume user input and trigger actions based on a prediction of the user's intent (retrieve pre-defined text answers or create tickets for the relevant response team).

Scan documents to determine whether and where specific information is located therein (e.g., ISIN of a security or the name of the counterparty that a contract refers to)

Use natural language processing for classification and prediction (e.g., e-mail prioritization, HR general request triage)

Holistic Coverage of Model Risks

Model risks should be assessed consistently in all model areas and holistically along various model risk factors (see an example of a model risk taxonomy below).

Dimensions	Factors		Risk Description
Inputs	1.1	**Input Automation**	Input data preparation/collection not automated hence posing significant operational risks
	1.2	**Input Data Quality**	Use of unreliable, unrepresentative or poor-quality data sources, high risk or non-validated feeder models
	1.3	**Input Data Appropriateness**	Use of data which is unsuitable for the model's intended purpose, reliance on questionable proxies
	1.4	**Documentation and Governance**	Missing key information on model inputs, insufficient oversight and controls of input data
Methodology	2.1	**Analytical Assumptions**	Use of analytical assumptions which are inappropriate with respect to the model purpose
	2.2	**Expert Assumptions**	High dependency of model outcome on expert judgment
	2.3	**Conceptual Framework**	Ineffective or flawed model design (including input, processing and output)
	2.4	**Calibration and Parametrization**	Inappropriate, unstable or insufficiently justified calibration
	2.5	**Complexity**	High or inappropriate model complexity leading to increased potential for undetected issues
	2.6	**Documentation and Governance**	Missing key information (e.g., assumptions) or unclear responsibilities regarding model development and design
Implementation	3.1	**Implementation Soundness**	Implementation or coding errors in the production environment
	3.2	**Operational Stability**	Unauthorized changes, insufficient level of access control, insufficient information on how to operate model
	3.3	**Documentation and Governance**	Missing key information or unclear responsibilities for model implementation
Model Use	4.1	**Alignment with Purpose**	Model inappropriately used outside its intended purpose and/or validated scope of applicability
	4.2	**Performance Monitoring**	Poor model performance
	4.3	**Ongoing Monitoring**	Inappropriate design of ongoing performance monitoring
	4.4	**Reporting**	Inaccurate, unreliable or unintuitive reporting of model outputs
	4.5	**Documentation and Governance**	Missing key information (e.g., limitations, restrictions) or unclear responsibilities regarding model use

Model Risk Measurement & Appetite: Individual Model Level

Inherent Risk Rating (IRR)

Drives frequency and depth of regular independent reviews

Combines

- Model Materiality, the impact of model failure
- Model Complexity, the likelihood of model failure induced through complexity of inputs, methodology and implementation

		Complexity		
		High	Medium	Low
Materiality	High	High	High	Medium
	Med	High	Medium	Low
	Low	Medium	Low	Low
	Imm	Immaterial		

Independent Review

Systematic identification of issues along various model risk factors, including issue severity ratings

Risk dimensions	Risk factors
Input	Input Automation Input Data Quality Input Data Appropriateness Documentation and Governance
Methodology	Analytical Assumptions Expert Assumptions Conceptual Framework Calibration and Parametrization Complexity Documentation and Governance
Implementation	Implementation Soundness Operation Stability Documentation and Governance
Use	Alignment with Purpose Performance Monitoring Ongoing Monitoring Reporting Documentation and Governance

Residual Risk Rating (RRR)

Factors in the outcome of independent reviews and mitigating controls, starting from the IRR as baseline

Risk reducing factors may be:

- Independent reviews are performed in line with prescribed cycles
- Issues are mitigated by compensating controls
- Assumptions, limitations and weaknesses of the model are transparently communicated
- Overarching controls (ongoing performance monitoring, output reviews and sign-offs)

Risk Appetite is formulated in terms of issue severity

■ Fundamental issues or conceptual flaws lead to a rejection of the model

▮▮ Severe issues need to be remediated timely and mitigated by compensating controls, or remediated before go-live

▶ Moderate issues can be accepted for a longer time horizon

UBS

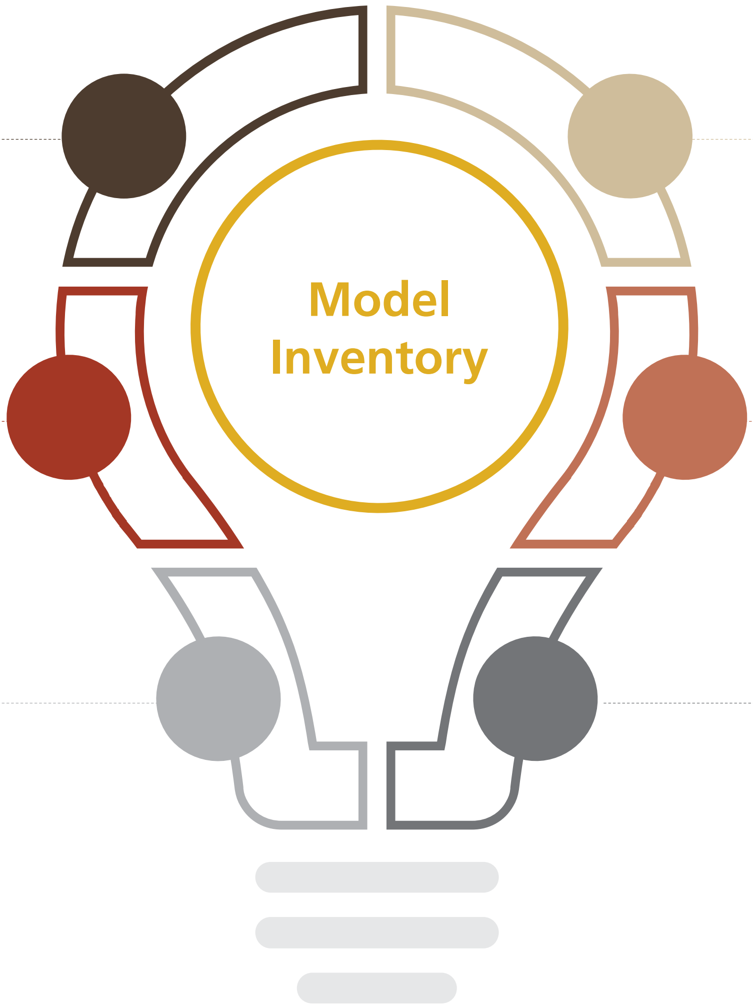
Model Risk Measurement & Appetite: Model Portfolio Level

There are various metrics that could be used to monitor the aggregated model risk. Trigger breaches should be investigated, escalated and addressed.

Metric class	Examples
Model Riskiness	Percentage of models in use with a high Residual Risk Rating
	Percentage of models in use with a high Inherent Risk Rating
	Percentage of models in use with open severe issues
	Percentage of not yet validated models in use
	…
Regulatory Matters	Number of regulatory matters related to Model Risk
	…
Model Risk Control Framework	Percentage of models in use with significantly overdue revalidation
	Percentage of models with overdue remediation of validation issues
	Percentage of models in use with material model inventory data quality issues
	…
Model Risk Concentrations	Percentage of models with severe issues in a particular model risk dimension
	Percentage of models in a particular model area with severe issues
	…

Reporting & Monitoring

Central model inventory should provide high quality model data for key reports.



Model Risk Report

Provides senior management, auditors and regulators with all relevant model portfolio information, supplemented by corresponding narratives

Risk Appetite Monitoring

Daily monitoring of model risk appetite metrics

Model Type Reports

Dedicated model type reports are available to management, sliced and diced by model type, regulatory purpose and/or legal entity

Data Quality Monitoring

Various online reports allow to monitor inventory data quality, including a case manager for issue resolution

Model Reports

Single-model specific reporting providing an overview of the current model status

Stakeholder Dashboards

Online dashboards allow stakeholders to oversee his/her portfolio and to ensure that warning flags are adequately managed

How to Cope with the Enhanced Expectations?

Various measures were implemented to remain effective and efficient.

People & Talent	Significant personnel increase in core locations Campus recruiting at India's top universities
IT Infrastructure	Common platform for development, independent validation & production for classical risk models Central model inventory supporting process workflows and storage all model data and documents Enhanced reporting capabilities
Validation Report Structuring & Automation	Reports are built automatically from standardized blocks (supplemented with narratives where needed): *Analysis*: risk factor, objective, design, results, conclusion, identified model risk *Issues*: risk factor, description, criticality & justification, opened on, closed on, reason for closure *Assumptions, Limitations & Weaknesses* Establishment of analysis menus for well known model groups
Model Tiering	Depth of (independent) testing and revalidation frequency depends on Inherent Risk Rating Immaterial use cases are not independently reviewed
Simplification of Model Landscape	Unify inputs, methodology and implementation for similar use cases Merge similar models

Questions?

Please don’t hesitate to ask