REPLY AVANTAGE

June 2017

MODEL RISK MANAGEMENT

WHITE PAPER

About **Avantage Reply**

Established in 2004, Avantage Reply (a member firm of Reply) is a pan-European specialised management consultancy delivering change initiatives in the areas of Compliance, Finance, Risk and Treasury.

Website: www.avantagereply.com

THE AUTHORS

Oscar McCarthy

Oscar McCarthy is an Associate Partner with Avantage Reply, where he is responsible for the risk management and banking advisory practices in the Netherlands. He has 20 years of professional experience in commercial and investment banking, covering all major risk types and the associated prudential regulations. His areas of expertise include both the setting of the risk governance, strategy and appetite as well as its implementation in policy, methodology and reporting. Oscar has a Ph.D. in Mathematics, and serves pro-bono as Non-Executive Director of the Professional Risk Manager's International Association (PRMIA).

Ram Ananthapadmanaban

Ram Ananthapadmanaban is Head of the Quantitative Practice at Avantage Reply. He has 13 years' experience working on critical risk and regulatory initiatives within Global financial institutions covering model risk, market risk, counterparty credit risk, derivatives pricing, wholesale credit risk, stress testing, ICAAP, Recovery planning and liquidity risk.

Ram holds an Economics degree from the London School of Economics, a Master's degree in Economics from New York University, a Master's degree in Risk Management and Financial Engineering from Imperial College London, is a PRMIA certified Professional Risk Manager (PRM) and has completed the Certificate in Quantitative Finance (CQF) qualification. He is also currently pursuing a certification in data science and machine learning in Python.

Scott Warner

Scott Warner is a consultant with an investment banking transaction execution background in New York, London and Europe. His Avantage Reply work has spanned a range of credit, market, operational and other risks, including model review and scoring. Scott has a Master of Science and two Bachelor of Science degrees in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology and a Master of Business Administration degree in Finance from the University of Chicago. He holds the PRM and FRM certifications and is a past Deputy Regional Director of the London Chapter and current member of the global Education Committee of PRMIA.

Orial Kryezu

Orial Kryezu is a senior consultant at Avantage Reply with a solid background in finance and mathematics. He has extensive experience in building, reviewing and validating models at various financial institutions covering all the major risk types.

Orial holds a Bachelor Degree and a PhD in mathematics from the University College London. Currently, he is undertaking the PRM certifications having already passed the first exam.

TABLE OF CONTENTS

REPLY AVANTAGE

1. Introduction

> ***"It is better to be roughly right than precisely wrong."***
>
> **- JOHN MAYNARD KEYNES**

Models are an integral part of modern banking. They are used inter alia to price transactions, value portfolios and optimise returns. They are also a key cornerstone of the regulatory framework, used to determine required capital and liquidity.

Models, however, require constant vigilance and scepticism. Risk measurements and financial analytics always need to be monitored for effectiveness and relevance. The simplification and assumptions that models must necessarily employ sometimes come at the cost of accuracy and structural integrity under stress. This exposes the bank to model risk: the risk of economic or reputation loss due to errors in the development, implementation or use of models.

The case for high quality model risk management may be made by reference to empirical evidence, in which anecdotes abound.

- The investment firm Long Term Capital Management ('LTCM') utilised highly profitable quantitative strategies for Fixed Income and Equity convergence trading. However, the model did not take account of investor flight-to-quality behaviour in times of stress, and the fund collapsed after the Russia default crisis.

- During the financial crisis, the trading of correlation products such as Collateralised Debt Obligations ('CDOs') and Basket Credit Default Swap products was responsible for substantial financial losses (trillions of dollars). Amongst other things, there was heavy reliance on certain model assumptions that did not account for "tail" or extreme risk appropriately. A mathematical construct known as a "Gaussian copula" was used to model obligor default dependency. The pricing model assumed zero tail dependence between obligor defaults, clearly a flawed assumption. The problems unravelled when the US subprime mortgage market collapsed with a significant number of defaults, and default correlations went through the roof. This extreme case was not captured by the Gaussian copula, and the correlation products were badly mispriced. In this case, lack of effective challenge of the assumptions and inappropriate model use led to catastrophic financial losses.

This case is strengthened by regulatory impetus. Increasingly, regulators are asking banks how they are managing model risk.

- In the United States of America, the Supervisory Guidance on Model Risk Management[1] **(SR 11-7)** is the cornerstone of local model risk regulation, and forms the basis of the Federal Reserve Board's expectations for models, such as the **Swap Margin Rule**[2] (including the exchange of initial margin for non-centrally cleared OTC derivatives).
- What the US has done via regulation, Europe is generally handling by supervision. In the European Union, model risk management is increasingly assessed as part of the governance component of the annual **Supervisory Review and Evaluation Process**[3] ('SREP') inspection. The associated standards are the subject of the European Central Bank's recently initiated **Targeted Review of Internal Models**[4] ('TRIM').

This means going beyond the historic Basel paradigm, of micro (per model) validation, to macro (i.e., portfolio level) model risk management. Key messages are therefore:

- **Model Risk is a risk like any other** and must be managed accordingly. This is increasingly the message from regulators (e.g., Fed SR 11-7, ECB TRIM).
- Hence, **the role of senior management must evolve,** from one of micro (model level) oversight and approval, to one of macro (portfolio level) risk management.
- Each request **for model approval is a model risk request**, and must therefore be justified in terms of benefits. Models with excessive complexity thus fail most risk/reward tests.

This links the model lifecycle to a programme of risk identification, assessment, monitoring and mitigation. **It enables risk-informed decision making.**

In this paper, we set out the key cornerstones of a modern model risk management framework. We start with an overview of the regulatory (i.e., mandatory) requirements, but then consider in greater detail other aspects of the framework, in particular those where some element of management discretion remains. We set out our view of the challenges and emerging best practice, illustrated where possible with anonymised anecdotes from financial institutions.

---

1 Federal Reserve, Office of the Comptroller of the Currency, Supervisory Guidance on Model Risk Management (SR 11-7).
2 US federal agencies, The Swap Margin Rule (SMR), 2015.
3 European Banking Authority, Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP), 19 December 2014.
4 European Central Bank, Guide for the Targeted Review of Internal Models, February 2017.

2. Regulatory Background

So many regulators and standard setters have issued guidance regarding some aspect of modelling over the last few years that trying to keep track of every aspect of this is a thankless, almost Herculean task. This is further complicated by the sense that different regulators have differing degrees of enthusiasm for their use, with some regulators demanding a higher standard of model, and with others seeking to minimise their dependence upon bank models. However, one may discern the following regulatory trends:

- Reduce model risk, both at a firm level and at a system level. Examples of the former include detailed supervisory guidance on model validation; examples of regulatory model risk reduction include the proposed elimination of the Advanced Measurement Approach ('AMA') and the proposed of "floors" in minimum capital determination.
- Improve the quality of the models used by raising minimum standards. This theme recurs in many recent regulatory standards, e.g., the Fundamental Review of the Trading Book ('FRTB') standard for market risk modelling. It is also central to many recent accounting standards, with increased XVA scrutiny (for pre-deal pricing) in the counterparty risk domain, and the new IFRS 9 standard for credit reserving.

2.1 View from America

The global financial crisis was exacerbated by a lack of appropriate governance around models and their use, as well as whether incumbent models were fit for purpose. The inevitable supervisory reaction has been increased scrutiny of how models are built, approved and maintained. In 2011, the Federal Reserve and the Office of the Comptroller of the Currency ('OCC') published the SR 11-7 supervisory guidance on Model Risk Management. As part of the Comprehensive Capital Analysis and Review ('CCAR'), banks are required to submit documentation on model risk management policies and practices. SR 11-7 has emerged as the de facto regulatory standard for model risk management.

According to SR 11-7, a model is defined as "*a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates*". The key focus of SR-11-7 is on ensuring that there is an "effective challenge" of models within financial institutions and strong evidencing across the end-to-end model lifecycle, from data acquisition through to reporting. A strong understanding of all sources of model risk and associated mitigations is therefore vital.

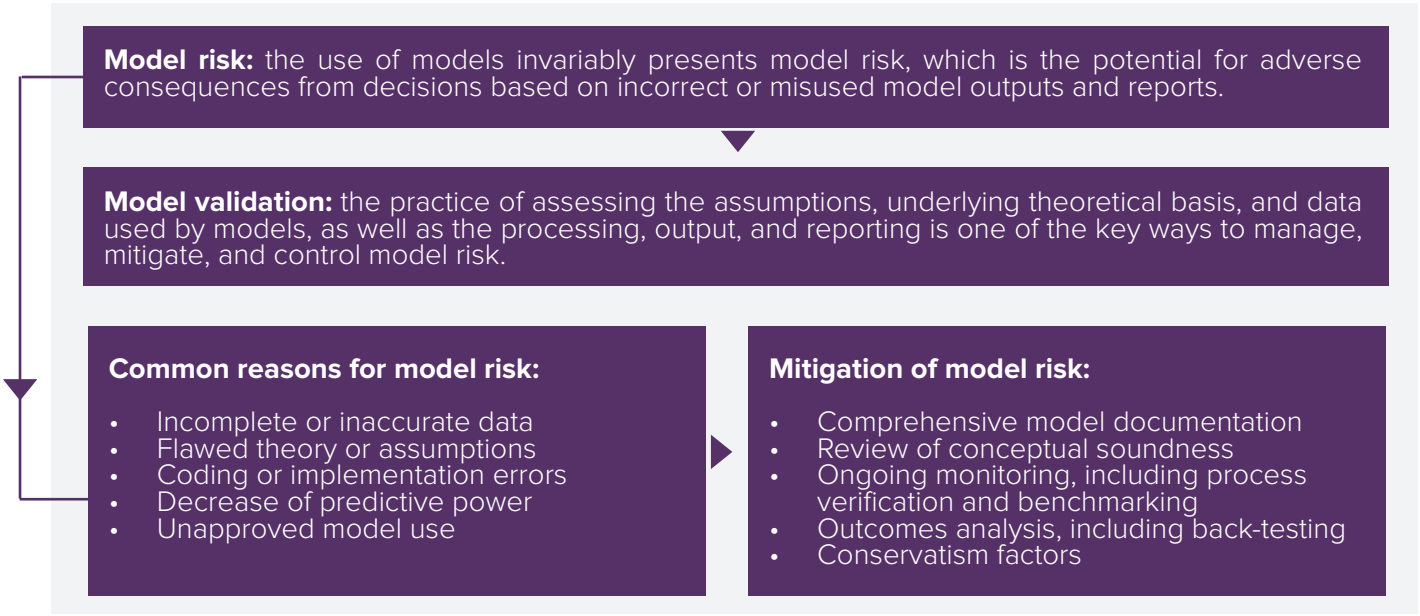


Figure 1: *SR 11 - 7: Model risk sources and mitigation*

In summary, SR 11-7 requires financial institutions to:

- Establish a strong model governance framework and infrastructure covering the end-to-end model lifecycle;
- Create a comprehensive model inventory;
- Improve and extend model review and validation processes;
- Enhance ongoing model performance monitoring;
- Ensure robust documentation exists along with clear evidence of model approval and conditions; and
- Operate an embedded control framework for effective model deployment and usage.

Many of the standards in SR 11-7, and the rigour with which they are enforced, have taken many banks, especially non-US banks, by surprise. Examples of areas which have created significant implementation headaches include:

- The broad definition of model, which goes beyond risk and valuation models and includes other models, such as trading algorithms and financial crime detection models;
- The expectation that all models are risk-assessed and recorded in an inventory;
- The formalisation of the model lifecycle as a robust process, with key controls at each step;
- The high standard of validation, with its focus on developmental evidence;
- The ongoing monitoring rules, to enable pro-active detection of model use issues; and
- The expectations of senior management pro-actively participating in model management.

Given that most banks above a certain size have an operation in New York, the influence of the SR 11-7 regulations has been felt by many banks, not just in the US, but globally.

2.2 View from the UK: Prudential Regulation Authority

The Prudential Regulation Authority ('PRA') of the Bank of England has long been at the vanguard of financial regulation. Banks operating in the City of London have been subject to a number of supervisory reviews, aimed at increasing model standards. These include:

- The Prudent Valuation rules understood that many trading book positions are illiquid and lack transparent pricing data. For such products, a conservative valuation regime was imposed, including reserves for model risk.
- The PRA was an early adopter of the "Risks not In Model" ('RNIM') regime. Such an exercise consists of identifying all risk factors used to determine the valuation of trading positions, and mapping these to those risk factors present in market and counterparty risk models. Where there are risk factors present in valuation but not in risk measurement, the PRA requires banks to prudently estimate the implied capital shortfall and propose appropriate remedial model actions. Common examples of gaps include absent and illiquid risk factors such as cross-risks, basis risks, higher-order risks and calibration parameters.
- The PRA now requires firms to annually (re-) certify their compliance with the requirements of approval for using internal capital models. Specifically, the PRA expects an appropriate individual in a Significant Influence Function ('SIF') role to provide to them on an annual basis written attestation that:
    - The firm's internal credit Internal Ratings Based ('IRB'), market, operational and Counterparty Credit Risk ('CCR') approaches for which it has received a permission comply with the CRR requirements and any applicable PRA supervisory statements; and
    - Where a model has been found not to be compliant, a credible plan for a return to compliance is in place and being completed.

A recent example of the PRA's thinking on model management came in their recent Note on Stress Testing[5], in which it identified the standards it expects to be applied to (stress testing) models.

2.3 View from Europe: ECB

To advance a consistent implementation of Pillar I minimum capital requirements models and the harmonisation of supervisory approaches, the ECB has begun efforts on a Targeted Review of Internal Models ('TRIM'). It has recently issued guidance[6] in which it states that, while the focus of TRIM is internal (capital) models, it nevertheless expects all regulated Eurozone banks to have a well-developed model risk management framework in place, and to apply this to all models used for business decision making.

The framework should permit a bank to identify, assess, monitor and manage its model risk. It should include a model inventory that facilitates a comprehensive understanding of the models; model risk assessment procedures, which enable risk-sensitive resource allocation; monitoring mechanisms to pro-actively describe model errors; and a robust governance which ensures that pro-active management of model risk is practised throughout the organisation. This should all be succinctly documented in a Model Risk

5 Bank of England, Stress Test Model Management, March 2017, available at: www.bankofengland.co.uk/pra/Documents/about/letter270317.pdf.
6 European Central Bank, Banking Supervision, Guide for the Targeted Review of Internal Models (TRIM), February 2017.

Management Policy, which describes inter alia the differing mandates, roles and responsibilities throughout the bank, and defines key reporting procedures to ensure that key issues are rapidly escalated and that the Bank's model risk appetite is respected.

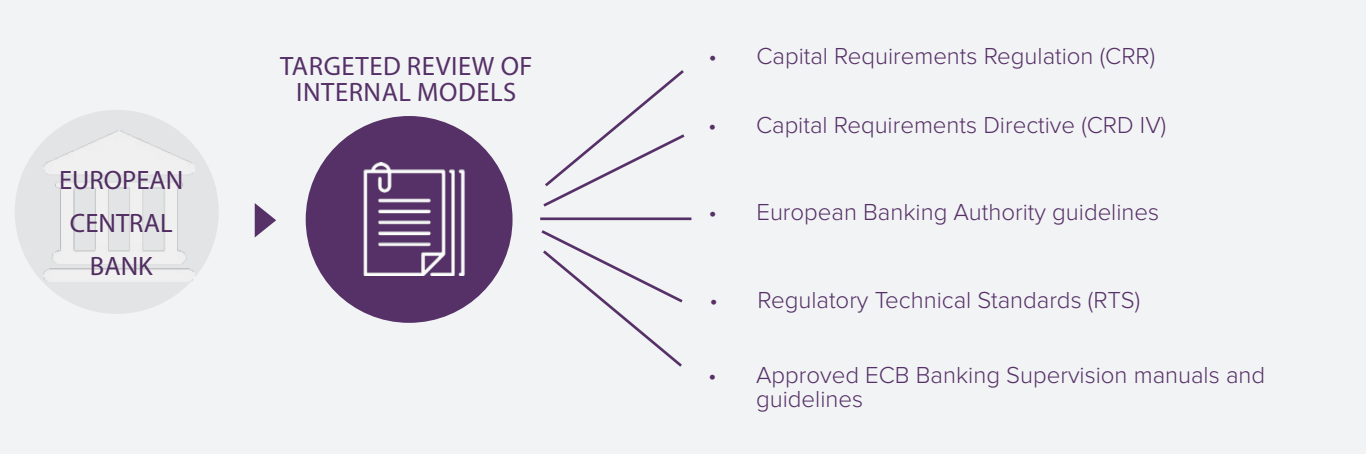


Figure 2: *TRIM*

The guide[7] to TRIM, published in February 2017 by the ECB, gives an interpretation of the existing legal framework (CCR, CRD IV, ECB guidelines, other references) related to internal models for credit, market and counterparty credit risks and on general model governance topics. It aims to harmonise interpretations and best practices to ensure that internal models are used appropriately across the industry. The guide gives appropriate supervisory practices that cover key elements of internal models including principles on the model risk management framework and its components: Governance, validation, internal audit, model use, management of model changes, data quality and external involvement.

"An institution should have a model risk management framework in place that allows it to identify, understand and manage its model risk as it relates to internal models across the group (institutions are expected to implement an effective model management framework for all models)"[8].

It also includes substantial details regarding the expected standards which banks are expected to achieve for their internal credit, counterparty and market risk models.

TRIM is an ongoing project that will be further refined based on feedback received from the institutions concerned, on-site assessments, SME analyses on peer groups, and regulatory developments. It will establish supervision standards comparable to those of the US; therefore, all Pillar I, Pillar II, and stress testing models must adopt higher standards. This implicitly requires the same of downstream models, such as valuation and behavioural models. TRIM is expected to be finalised in 2019.

7 Guide for the Targeted Review of Internal Models (TRIM), available at: https://www.bankingsupervision.europa.eu/ecb/pub/pdf/trim_guide.en.pdf.
8 TRIM Guide, Article 7.

3. Model Risk Management Framework

Model risk cannot be completely eliminated; however, measures can be taken to manage it. How can model risk be mitigated? Best practices from regulatory guidelines (Fed/OCC, TRIM) encourage institutions to design and have in place a Model Risk Management Framework ('MRMF'). This consists of a number of elements which allow for model risk to be identified, escalated and remediated. The aim is to establish a framework capable of closing model risk gaps through feasible allocation of risk control functions, such that resources are deployed effectively. The well-established 'Three Lines of Defence' approach deployed in managing other financial risk types is a good starting point to enhance the ability of an institution to mitigate model risk. The figure overleaf shows the key components of the MRMF.

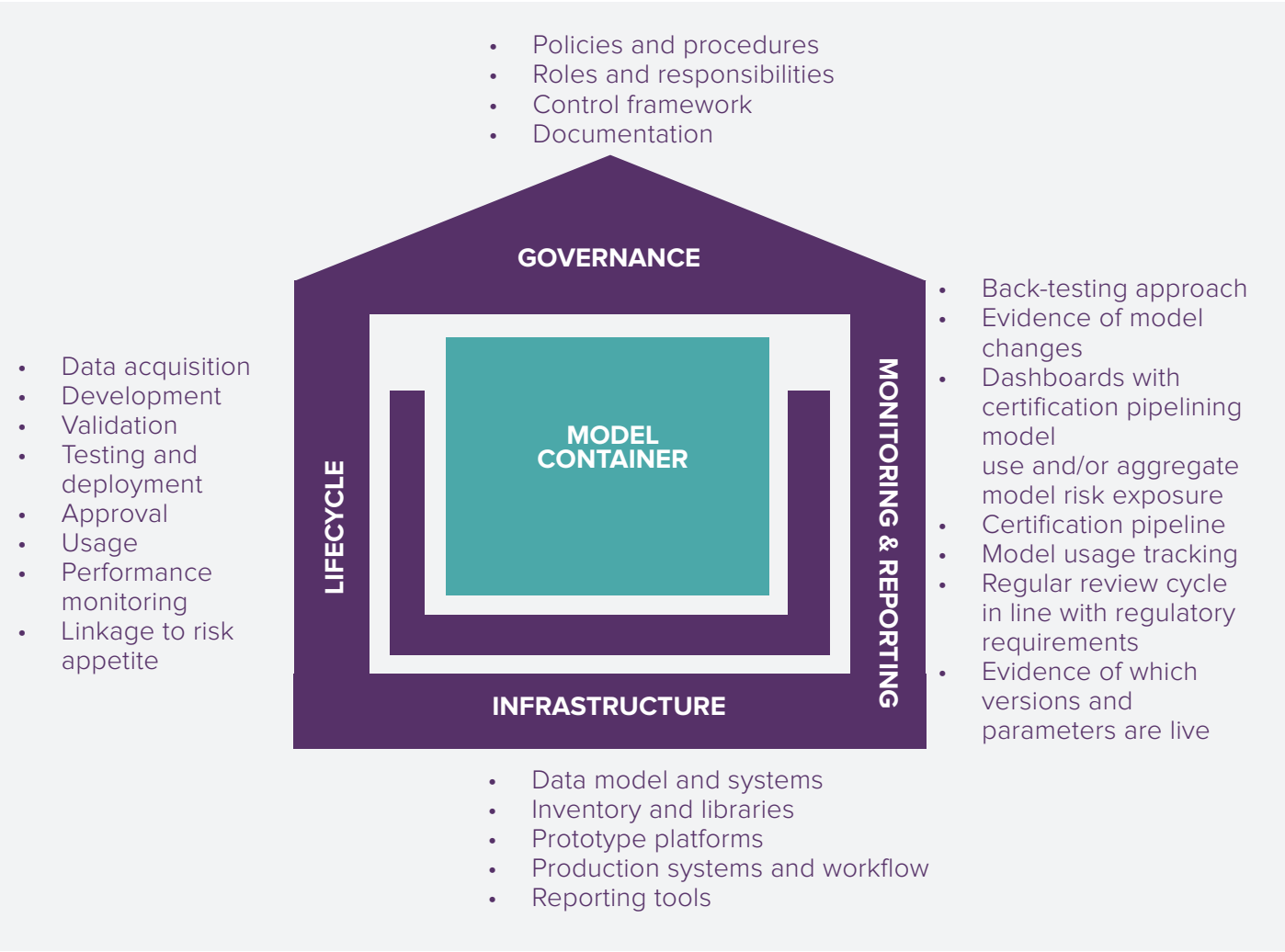


Figure 3: *Model Risk Management Framework*

3.1 Governance

Governance involves setting out the roles and responsibilities of the stakeholders in the model risk management process, accompanied by a set of principles, policies and procedures necessary to mitigate the impact of model error or incorrect model use.

"*Developing and maintaining strong governance, policies, and controls over the model risk management framework is fundamentally important to its effectiveness. Even if model development, implementation, use, and validation are satisfactory, a weak governance function will reduce the effectiveness of overall model risk management.*" (Fed/OCC)

A key governance question each firm needs to ask itself is this: **Is senior management actively engaged in model risk management, or does it merely rubber-stamp?**

The challenge for members of the Management Body and Senior Management is often to understand the highly technical nature of the models which they are asked to approve. Without the appropriate technical knowledge, some senior managers may fall back on managing the process rather than the outcome, by seeking confirmation that all the correct stakeholders have been consulted and that correct procedure has been followed.

This alas does not suffice, as the extract from the below speech by Andrew Bailey, previous Head of the PRA, makes clear:

"*Let me give an illustration of this in a highly topical area for banks and insurers, internal risk models. What does a Board need to understand? Try the following:*

- *Key elements of model design;*
- *Significant assumptions and expert judgements;*
- *Key sensitivities; and*
- *Significant limitations and uncertainty in the model.*

To restate, the challenge is to reduce complexity to simplicity, so that Board members feel that they understand:

- *Where is the model expected to work well;*
- *In what circumstances is it likely to break down;*
- *Is the overall model output credible;*
- *What "moves the dial" in terms of key assumptions or judgements; and*
- *Are those assumptions and judgements reasonable?"*[9]

Similarly, the Head of Capital Modelling at a medium sized Wholesale and Retail Bank said:

> "It is important that the Board and Senior Management understand the nature of the risk captured by the capital model, the approach taken to calculate capital, the key assumptions and limitations of the model, the capital allocation methodology and more importantly the strategic levers they can pull to influence capital allocations."

A key implication of these expectations is that high quality documentation and communication throughout the modelling process is vital, to enable both senior management and the management body to make informed decisions. This in turn requires us to think carefully about the different aspects of the governance, with particular reference to Roles & Responsibilities, and to Policies & Procedures.

9 Governance and the role of Boards, Westminster Business Forum, 3 November 2015.

3.1.1 Roles and responsibilities

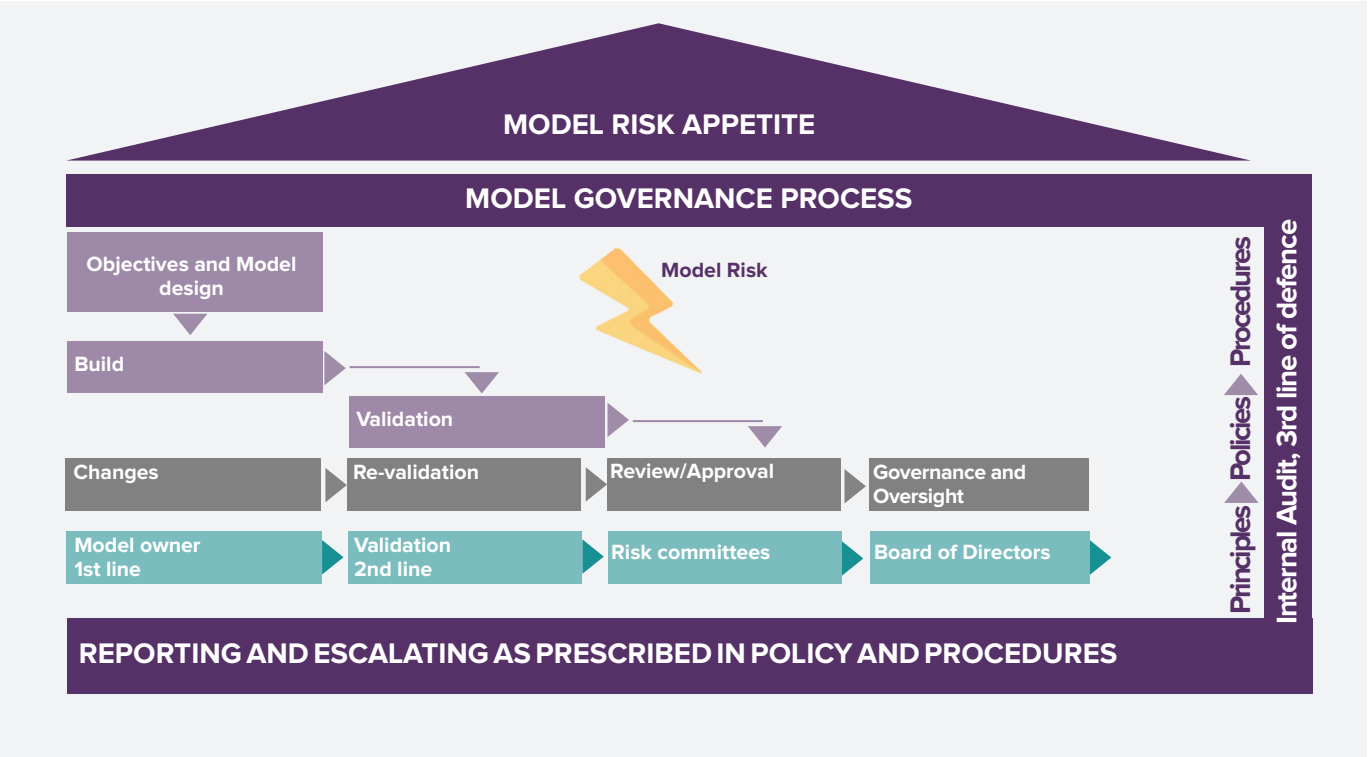


Figure 4: *Model risk governance for new models and model changes*

As model risk can arise due to both Quantitative and Qualitative factors such as model misuse, proper model risk management requires engagement of teams with a diverse set of skills. Roles and responsibilities can be grouped into a number of layers of functions:

Model owners – the individual responsible for developing and using the model provides the first line of defence. They must also develop the relevant model documentation describing all of its technical specifications, restrictions on model use, and strengths and limitations which, clearly, requires the function to have complete understanding of the model. A risk source that may arise in this function is over-reliance on the specialty of a key team member. All tasks have to be executed in accordance with the approved governance and procedures (e.g., key operating procedures, documentation templates - see figure 5), provided by the model risk management framework.

Centralised risk functions – include functions such as framework owner, model validation (both 2nd line of defence) and internal audit (3rd line of defence). A fundamental requirement is that model validation, and in particular internal audit, are performed independently from other functions in order to avoid any conflict of interest that may arise when framework breaches occur. Responsibilities of the centralised functions range from highly technical assessment of model assumptions, methodology and performance, to a qualitative assessment of the execution of policies and procedures embedded in the model risk management framework. In addition models can vary in complexity and type, can cross business lines, and risk categories. The board of directors, which is ultimately responsible for the effectiveness of the management framework, needs to ensure that the centralised functions have the required resources and skills.

Role	Responsibilities
Functional roles Responsible for executing policies and producers prescribed in the model risk management framework.	
Model owner (1st line of defence) 1	• Ensures the model complies with business requirements and framework requirements. • Responsible for the end-to-end model lifecycle: design, build, use and performance monitoring. • Produces and maintains documentation. • Implements controls and responds to breaches identified by model validation.
Control functions (2nd line of defence) 2	• Own the framework. • Ensure adequate controls are in place. • Manage conflict of interest, e.g., between model owner and model validator. • Approve use of independent external validation.
Independent validation (2nd line of defence) 2	• Performs independent validation of documentation provided by model owner, model assumptions and implementation, model use and limitations on use, model inter-dependencies; can the model be reproduced by a third party using existing documentation? • Monitors remediation of breaches performed by the model owner and corresponding documentation. • Monitors production results against expected results. • Ensures that any external independent validation required has the expertise and skill to perform the validation.
Internal Audit (3rd line of defence) 3	• Assesses the performance of the model risk management framework: governance, risk management and internal controls. • Evaluates existing policies and procedures to determine whether they are adequate and comply with regulatory requirements and with industry best practices.
Governance bodies Review, challenge and manage the scope of the model risk framework in accordance with the risk appetite tolerance of the organisation.	
Model risk committees	• Review all model validation reports, approve remediation plans and monitor their implementation. • Advise the board of directors on significant changes required to the model risk management framework. • Review new models, significant model changes and new model pipeline, and advise the board.
Board of Directors	• Ensures that there are sufficient resources available, appropriate training and guidance. • Specifies the model risk appetite to be embedded into the framework through principles, policies and technical specifications. • Approves models or significant changes based on materiality, e.g., new, high materiality models. • Drives change towards a more robust and effective framework by reviewing and amending model risk management policies.

Figure 5: *Roles and responsibilities within different functions of the model risk management framework*

The key question which each firm should therefore ask is thus: **How are the three lines of defence demarcated within the firm?**

A question which starts with consideration of the risk committee structure and risk organisation, and the degree of centralisation therein, and then considers the different controls in place throughout the organisation to ensure their correct operation. These decisions are then documented in a detailed set of policy and procedure documents.

3.1.2 From principles to procedures

Model risk governance also contains the principles, standards and procedures related to model risk which are embedded into the framework.

"*To have a holistic understanding of risks and risk measurement, it is expected that institutions will either develop group-wide principles and guidelines relating to the development and maintenance of internal models, or ensure that each relevant entity has an appropriate, independent audited framework in place*". (TRIM)

Financial institutions should develop a set of high level minimum standards around the modelling process that guarantee compliance with the minimum regulatory requirement and best practices expected. Additional standards could be applied based on a number of factors, such as differences in regional regulatory requirements, financial model categorisation and materiality of the model.

High level standards and principles	**A set of high level standards to enforce compliance with minimum regulatory requirements and a commitment to industry best practices throughout the modelling process.**		
	Subsidiary level principles and standards	**Regional policy, e.g EMEA model risk policy**	**Policy and principles based on financial model classification, e.g. credit models or pricing models**
Model documentation template	**Validation guidelines**	**Model Inventory guidelines**	**Data quality governance**
Ensures consistent documentation of models across end-to-end model lifecycle.	Guidelines to ensure that the model meets prescribed objectives, minimum regulatory requirements and best practices.	Provides guidelines on details of the model to be recorded.	Governance around the quality of the data to be used as input data, e.g. validation of input data.
Model changes governance	**On-going monitoring**	**Use of external models**	**Model development and use**
Guidelines on the approval process of model changes, extent of changes and assessment of impact.	Governance around the extent and frequency of testing and monitoring necessary to ensure consistent model performance.	Governance required for using external models: Service Level Agreements.	Governance process for designing, building, validating, approving and using new models.

Figure 6: *Key components of the Model Risk Management Framework*

The main purpose of a policy is to define a risk-sensitive model governance approach. A guiding principle for managing model risk is "effective challenge" of models, that is, critical analysis by objective, informed parties who can identify model limitations and assumptions, and produce appropriate change. Effective challenge depends on a combination of incentives, competence

and influence. Incentives to provide effective challenge to models are stronger when there is greater separation of that challenge from the model development process. Competence is a key to effectiveness, since technical knowledge and modelling skills are necessary to conduct appropriate analysis and critique. Finally, in order to be effective, challenge must have the influence to ensure that actions are taken to address model issues, through a combination of explicit authority, stature within the organisation, and commitment and support from higher levels of management.

3.2 Model lifecycle

The model risk governance framework should provide end-to-end coverage of the model lifecycle. A robust policy defines a best-practice model lifecycle, which describes the different stages of production of a model, such as development, implementation, validation, approval and use. See the diagram below for details. Defined processes assure that the model design and implementation is aligned to objectives, and that the model is used accordingly. Robust standards on internal validation are established, facilitating the risk assessment and findings, with key risk issues tracked and reported to senior management.

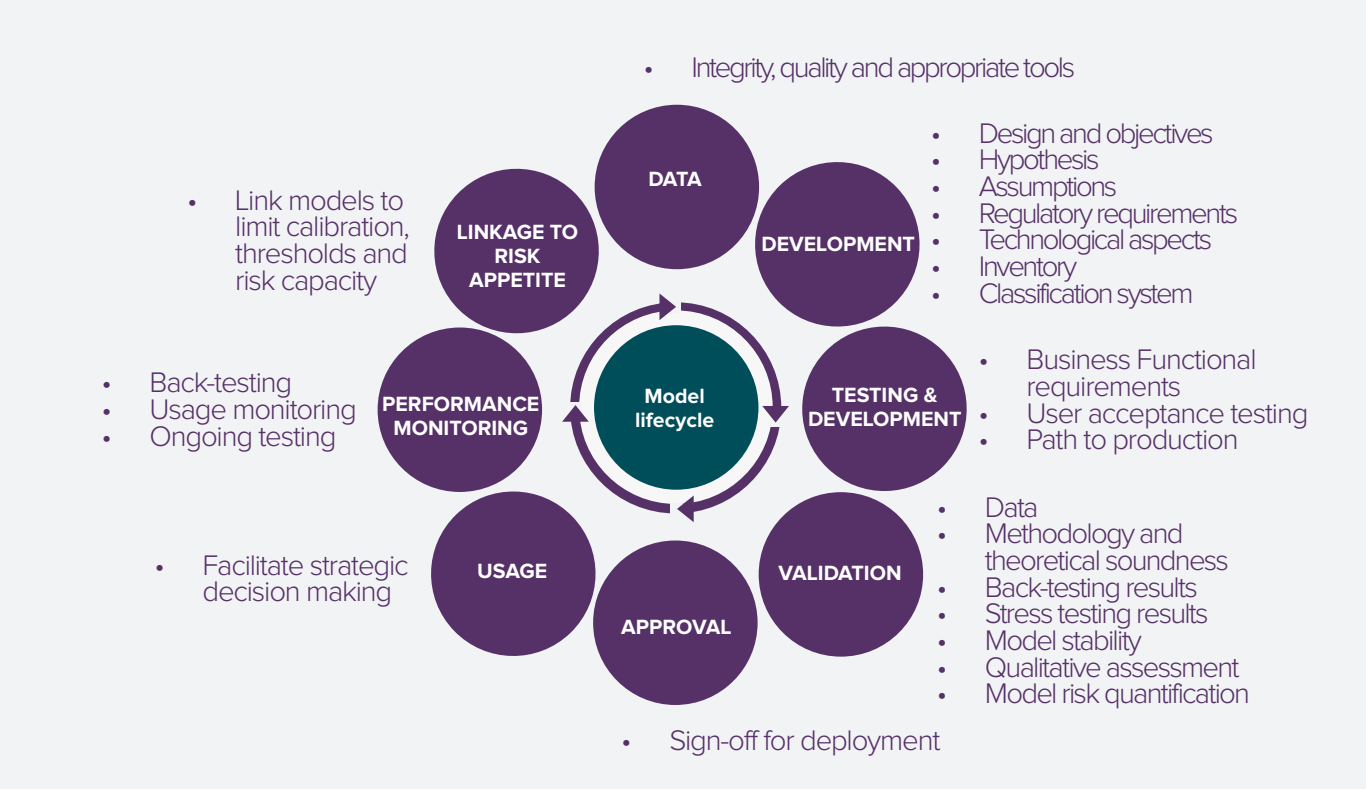


Figure 7: *Model lifecycle stages*

Origination, design and development	The model owner needs a clear understating of the purpose of the model – why the business needs it. Clearly documented business requirements enable the model builder to construct a model that is aligned with business needs.
Implementation	Implementation requires the infrastructure to develop, test and run the model. The model owner, in liaison with IT, ensures that platforms and tools are in place to support the model throughout its end-to-end lifecycle. Technical and functional specification documents specify the implementation of the model. Testing should expose model strength, limitations and constraints beyond which model performance deteriorates significantly. If models are provided by a third party, their documentation needs to be reviewed and results examined to ensure the model works as intended, and that the model owner has full understanding of its limitations.
Validation	Independent validation provides assurance that the model performs as expected, meets business needs and satisfies regulatory requirements. Some of the elements covered by validation are: • Model purpose; • Model design, assumptions and development; • Performance; • Use; and • End-to-end model lifecycle documentation, i.e. can the model be reconstructed independently using the documentation? Crucially no conflict of interest should arise when carrying out the validation.
Approval	All models are reviewed and approved by the relevant committee(s) before being approved, and the board of directors informed. The committees may also advise and refer the final decision to the board of directors. The materiality of the models is a significant factor when determining the approval process. The decision uses the reports from the model owner, which include adequate information to support the review. Reports provide concise remediation actions and plans in response to validation reports and issues identified. Similarly the committees receive and review all validation reports.
Use	Only when the model has been approved can it be deployed in a production environment. The model owner documents the scope of and concise restrictions on model use. Controls to ensure intended model use can also be put in place.
Ongoing monitoring	Ongoing monitoring of all models ensures that the model performance is within agreed parameters and enables identifications of model limitations and weaknesses. It is an important source of insight into the operational implementation of a model, e.g., data issues, methodology complexity and technological considerations.

Figure 8: *Core components of the model lifecycle*

The general concept of a model lifecycle is broadly understood, with varying degrees of detail, by most firms. The challenge in implementing this is to map to each key stage of the lifecycle the appropriate controls, to ensure that errors are detected and can thus be corrected.

What are the key controls used at each stage of the model lifecycle to manage model risk?

Examples of how errors may arise at different stages of the model lifecycle and how the lines of defence may "intercept" these errors are:

	Error	Risk Mitigation	Role/Line of Defence
Input data	Raw data extracted from the database are incorrect	Model owner implements a series of data quality checks: completeness checks, statistical tests. Checks against data governance policy	Model owner/ 1st line of defence
	Model metrics selected as inputs (no correlation tests performed)	Independent model validation request that model owners include additional tests	Model validator/ 2nd line of defence
Model design and build	a) Model relies on large number of assumptions b) Model calibrated using data from a stable period when expecting environment to be influenced by extreme (e.g. political) events	a) Model owner, responsible for methodology, builds model prototype and tests its performance to identify areas of weakness before build stage b) Independent review of model methodology by Model Validator before full commitment	Model owner and Independent Validation/ 1st and 2nd line of defence
Model output use	Models are applied outside their approved scope	a) Internal audit performs independent assessment of the effectiveness of the model use policy and finds gaps b) Model owner approves key reports based on model output c) Backtesting provides statistical evidence of model output reliability	Internal audit/ 3rd line of defence 1st and 2nd line of defence

Figure 9: *Examples of key model controls*

3.3 Model Infrastructure

The technology infrastructure is an important component of the model risk management framework. The interconnectivity between source data systems, analytical engines and reporting platforms needs to be well documented, with the rationale for platform choices clearly articulated.

For underlying systems, the completeness, accuracy and timeliness of data that feed models needs to be a top priority, with a clear segregation between input data, model data and output data. A well-defined data model will ensure traceability from inputs through to outputs. The choice between internal vs. vendor systems needs to be clearly articulated. There needs to be a robust vendor selection process undertaken by an independent body if possible, so that the financial institution is able to consider how the vendor systems fit within the current infrastructure. The same controls need to be applied to vendor systems as internal models.

For analytics, there needs to be a detailed inventory of model libraries, with clear documentation of those used for prototyping vs. production clearly identified. Doing so will ensure that errors can be picked up quickly and remediated. It also enables model usage to be tracked more effectively. However, if possible, it is important to consider whether single modelling platforms can be used for both prototyping and production. This will mitigate the likelihood of errors in implementation and vastly improve delivery time. In fact, prototypes should be used in the requirements gathering phase to demonstrate the model as a "proof of concept", and then productionised using the same language. Any changes made need to be correctly versioned, documented and implemented. For example, a derivatives pricing model can be developed and productionised in the same language, so that there is clear propagation from R&D through to production.

A number of financial institutions are shifting from vendor solutions to open-source modelling platforms, such as Python, Julia and R, in areas such as machine learning, derivatives pricing, capital modelling and stress testing. Key drivers have been transparency, speed, cost, flexibility and auditability. Models need to stand the test of regulatory scrutiny and enable strategic decision making. The head of quantitative analytics at a large insurance company, who shifted the firm's Solvency 2 capital modelling onto an open-source platform, said:

> "Why do we have different tools for prototyping vs. production? Surely, using a single open source modelling platform reduces the likelihood of implementation errors, especially when the tool in question is fast, cost effective, robust, flexible, transparent and auditable."

For reporting, model outputs need to be presented in a logical structure to aid strategic decisions. Appropriate platforms need to be chosen that enable drilldown from outputs through to underlying inputs to explain changes. Advancements in data science and visualisation need to be used to aid the dynamic management of model risk, so that clusters of model risks can be identified and mitigated. The issues may be systematic, with multiple models depending on the same datasets, or systemic, in that the failure of one model can have a "domino effect" and cause the failure of multiple others. For example, the failure of a single credit scorecard model can impact a capital calculation model and an IFRS 9 credit impairment model.

Many financial institutions have layers of technology built up through time, with many legacy platforms. It is difficult to disentangle the "spaghetti" or introduce changes to the existing architecture. There are different tools used for the same purpose and across the model lifecycle, with data coming in from several sources. Financial institutions need to think strategically about the end-to-end model lifecycle when making infrastructure choices. Here, the key question is:

In determining the optimal technology infrastructure, covering the full model lifecycle, have you considered key factors such as speed, cost, vendor vs. internal systems, simplicity, robustness, flexibility, transparency and auditability?

Most Banks have an IT strategy that enables rapid prototype development and promotion. And yet, so many of the fundamental problems which arise in development and implementation are, in effect, a consequence of this lack of common infrastructure.

3.4 Monitoring and reporting

Once a model has been validated and approved, it then enters official use within the bank for internal reporting purposes. At this stage, there is the danger of complacency: after all, what could possibly go wrong, given all the meticulous control work applied to date?

There are a number of possible errors which can (and do) occur after validation and approval:

- The model reaches its theoretical limitations, e.g., certain types of stressed markets. One should be able to identify these scenarios in advance from validation work, and thus be forewarned of stormy waters.
- The model ceases to function correctly, due to errors in the live environment, e.g., due to poor data feeds or to system changes. Often, such environmental errors produce egregious errors, which makes identification straightforward, however this is by no means given.
- The model is used incorrectly. Models are often developed with a particular business need in mind, but as the underlying portfolio grows, so does the need for evolving model sophistication. This is often the hardest production error to detect, and thus can only be mitigated by strict controls around model use.

Monitoring and reporting thus refer to those periodic activities which occur once a model has

been approved for use, in order to verify that it is being used and functioning correctly. Often, the most visible consequence of model use is the reports which are generated by the model. The management information associated with a live model should be monitored for correctness, with appropriate heuristics in place to enable rapid identification of potential errors or issues.

The ongoing monitoring continues throughout the life of the model, to track known model limitations and to identify any new ones. Model outputs may also be verified through the use of appropriate benchmarks, which enable rapid identification of divergence. Discrepancies between the model output and benchmarks should trigger investigation into the sources and degree of the differences.

Where available, ongoing model monitoring should also utilise management reports, e.g., portfolio reviews, reconciliation reporting and back-testing reports. It should include the analysis of any overrides which have been made in the reporting and production process, evaluating the reasons and tracking their performance. Many of the tests employed as part of model development and implementation should be included in the ongoing monitoring and be conducted periodically. If outcomes analysis produces evidence of poor performance, the model owner should take action to address those issues.

The fundamental question that a firm should ask is thus: **Are you able to efficiently detect model errors or issues?**

For example:

- How will I know if the model is working?
- How will I know if it isn't working?
- What are the warning signs we need to adapt in daily work?

Such questions should, in principle, be answered as part of the model validation process. However, there is no substitute for constant vigilance in model use.

3.5 Model container

An increasingly familiar, real-world problem: your regulator requires you, at short notice, to send a complete model file. Can you assemble all the required documents, evidence and reports at short notice? Often, the required components are distributed across the firm, with for example methodology papers held by the model owner, data and systems documentation held in IT archives, and output reports held in various corners of risk and finance.

Do you have a central repository to capture all evidence pertaining to model changes (such as documentation, model prototypes, code and reports) across the full lifecycle?

A model container is a repository that links all aspects of a model: model lifecycle, governance monitoring and reporting, and infrastructure. It covers all models within an organisation and provides a microcosmic view of the model risk framework. Key characteristics captured include:

- Who developed the model?
- When was it last validated?

- How is the model performing?
- Do we have enough oversight of the model?
- What are the documentation gaps?
- What are the bottlenecks in the documentation gaps?

The container has key information but also actual items such as documentation and code approval emails. It can facilitate a group-wide evaluation of aggregate model risk. In addition to information included in a model inventory, it may also contain validation reports, model owner reports, internal audit reports, on-going monitoring results, etc..

Best practice model risk management increasingly requires a central tool which serves a number of functions. It acts as the official Model Inventory, where all models are registered and scored; it acts as the repository for all required documentation; it acts as an Action Management tool, to enable all stakeholders to keep track of all forthcoming tasks such as Re-validation, or Audit gap closure. Such a tool thus becomes the basis for all model risk reporting, both internal and external. We will explore some of these themes in the next chapter.

4. Model Risk Assessment

4.1 Model risk appetite

The Financial Stability Board (FSB) defines risk appetite as "*The aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan*". Specifically, model risk appetite is the extent to which the organisation is willing to accept the inherent risk that arises from the application of models in order to achieve its objectives. By nature, the broad applicability of models which crosses business lines and risk types requires model risk appetite to be considered within the context of the risk appetite framework of the organisation.

Model risk appetite is translated through statements, quantitative and qualitative, to more precise risk appetite metrics and thresholds, as shown in the figure below.

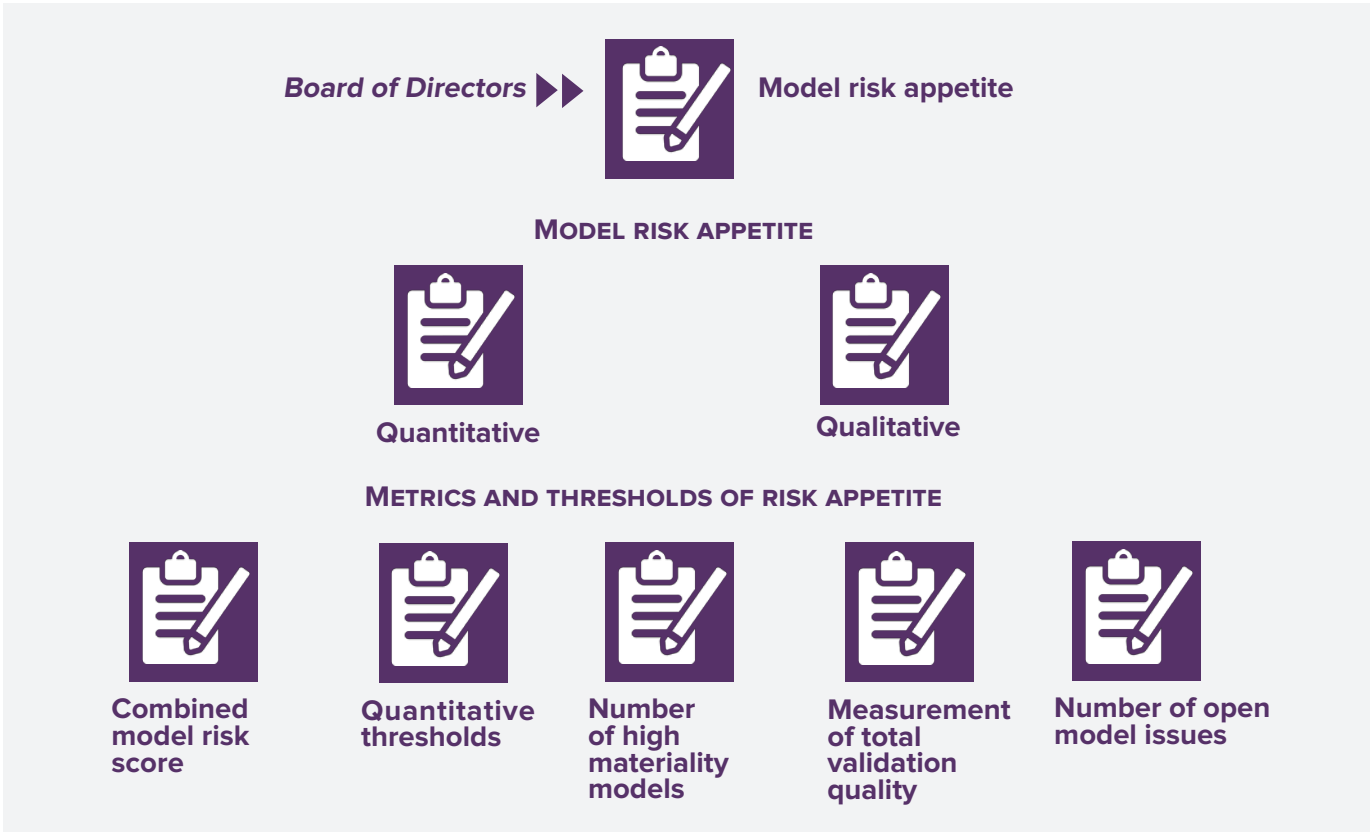


Figure 10: *Risk appetite setting*

The criteria used to determine which models are material to the organisation should be aligned with its risk appetite. Materiality is the impact or consequences that model error has on the financial institution. This impact is typically not directly proportional to the model error. For example, depending on the risk appetite, the organisation may deem a model to be material or important depending on whether the model results are the primary factor affecting decisions relating to capital calculations or liquidity, or if the model has many downstream dependencies. These criteria may be independent, regardless of the complexity of the model and the actual quantitative model error. Materiality can also be set based on criteria related to the model in question such as:

- Model complexity;
- Number of assumptions;
- Data inputs; and
- Number of identified model weaknesses.

In addition, risk appetite limits may be set based on appetite metrics which aggregate model risk to business line, entity and group wide levels, for example, limits on the number of high materiality models, the combined quality of the validation, or internal audit results. Whilst financial institutions specify their own model risk appetite as a reflection of business needs and objectives, it also has to be within the risk capacity of the organisation given its resources. The FSB defines risk capacity as "*The maximum level of risk the financial institution can assume given its current level of resources before breaching constraints determined by regulatory capital and liquidity needs, the operational environment (e.g. technical infrastructure, risk management capabilities, expertise) and obligations, also from a conduct perspective, to depositors, policyholders, shareholders, fixed income investors, as well as other customers and stakeholders*".

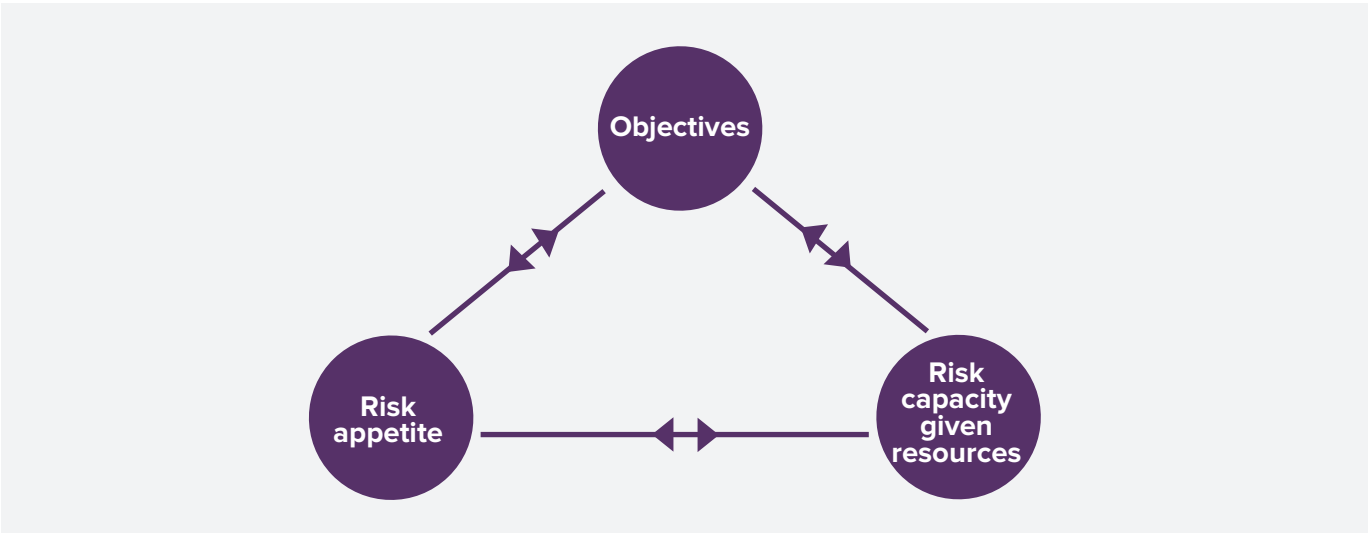


Figure 11: *Risk appetite definition*

In assessing the adequacy of model risk appetite, the key question which each firm should ask is thus: **How does your Risk Appetite compare to your model performance indicators?**

Key challenges related to model risk appetite are:

- In addition to important factors such as business objectives, risk capacity and resources, available model risk appetite is also influenced by:

a. The varied complexity of models across the institution. Some comparability of model risk measures utilised across the model landscape would allow the board to better assess and understand the risk they are willing to accept.
b. A fundamental understanding of limitations and restrictions of models.
c. The aggregated model risk, which may be complex or poorly understood. For example:

i. Inclusion in the aggregation of external, black-box models, and
ii. Correlations used to aggregate risk which are not based on solid scientific grounds.

d. Communication, comprising:

i. Top-down communication of model risk appetite to all stakeholders. Model risk appetite must be consistent and understood by all stakeholders; and
ii. Bottom-up communication of the materiality of model risk to the board through the governance framework.

> "The risk appetite statement should be easy to communicate and therefore easy for all stakeholders to understand. It should be directly linked to the financial institution's strategy, address the institution's material risks under both normal and stressed market and macroeconomic conditions, and set clear boundaries and expectations by establishing quantitative limits and qualitative statements."
>
> **- Financial Stability Board**

> "...an impoverished conception of 'risk appetite' is part of the 'intellectual failure' at the heart of the financial crisis. Regulators, senior management and boards must understand risk appetite more as the consequence of a dynamic organisational process involving values as much as metrics."
>
> **- (Accounting, Organizations and Society 34 (2009) 849–855)**

> "Relevant staff at all levels should know and understand the core values of the institution, its risk appetite and risk capacity. They should be capable of performing their roles and be aware that they are held accountable for their actions in relation to the institution's risk-taking behaviour."
>
> **- (Page 30, Draft Guidelines on Internal Governance - EBA/CP/2016/16)**

- Embedding model risk appetite in a model risk management framework, which enables effective communication and monitoring of model risk.
- Establishing a framework which allows model risk appetite to be managed against changing business environments, objectives and regulations, i.e., the ability of the organisation to adapt and set model risk appetite appropriately.

4.2 Scope

A key decision which each bank must take when establishing a model risk management framework concerns the exact scope of application: **Which models are in scope, and which models (if any) are out of scope?**

Many European commercial banks have traditionally elected minimal coverage, restricting the scope to regulatory models (e.g., those used to determine Pillar I capital, ICAAP and ILAAP, stress testing and IFRS 9). A medium sized bank might have on the order of 50 to 100 models in such a portfolio.

However, many of these models make use of multiple modelled inputs. For example:

- Financial market risk models such as VaR and CVA use valuation models as inputs. And these valuation models themselves are often dependent on modelled parameters, such as those extracted from volatility surfaces.
- ALM models for the measurement of interest rate and liquidity risk similarly require economic valuation models, which in turn require as inputs behavioural maturity models and a selection of yield curves.

In short, one has a model hierarchy which links capital to data over several intermediate steps. This model hierarchy has led many banks to adopt a broader scope definition, which is based on the above hierarchy principle: models which, directly or indirectly, act as inputs to capital models are, themselves, within the scope of model risk management. This typically increases the number of models in scope by an order of magnitude, to somewhere between 500 and 2,000.

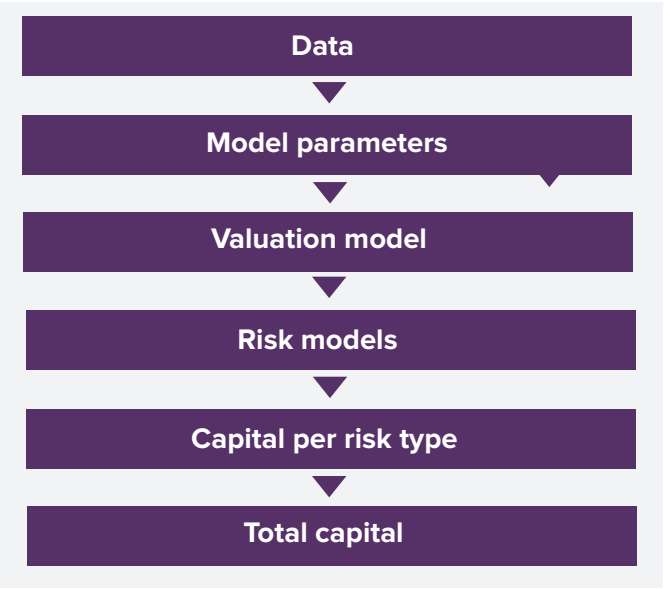


Figure 12: *Model hierarchy*

In contrast, all US banks have – in line with SR 11-7 requirements – officially adopted a universal scope definition: if it's a model, then it's in the scope of model risk management. This means that models outside the above perimeter, such as trading algorithms, financial crime detection models, marketing selection designs, and interest rate management methods, all enter the scope of the policy. Such a scope massively increases the number of models to be registered, from a few hundred to over a thousand. The massive increase in workload implied by such a scope increase requires the application of a risk-sensitive model governance, which prioritises resources towards the higher risk models.

A non-US bank could in theory elect to adopt a two-pronged approach, with an SR 11-7 based scope

definition for US operations and a narrower scope definition for other operations. However, for any US operation above a certain size, this rapidly becomes cumbersome. Many of the models used directly or indirectly by the US operation will in fact be global models, used elsewhere in the bank; hence, one rapidly finds that a very large number of models which have been developed at head office enter the scope of SR 11-7. Therefore, there comes a point at which the demarcation becomes arbitrary, with certain high risk models out of scope, but many low risk models in scope. As a consequence, many firms are increasingly adopting as best practice the principle that all models should be subject to model risk management. Time will tell whether this approach is sustainable over the long term.

Adopting this approach moves model risk management away from being purely an exercise in compliance, and enables some element of pro-active risk management to take place.

4.3 Model risk measurement

The essential starting point for a model risk management framework is the mandatory registration and risk assessment of all models within the agreed scope. This implies some notion of risk scoring, which prompts the question: **How do you determine the level of risk in a model?**

The measurement of model risk should be a combination of expert input and empirical evidence with both qualitative and quantitative assessment. The models listed on the inventory should be scored consistently through construction of a scorecard, so that the degree of model risk can be compared on a like-for-like basis. One key objective of scoring is to ensure that that one can discriminate between models and rank them in terms of high, medium and low model risk. The precise scoring mechanism can be as granular as required, as long as one can discriminate between the models. What is key for senior management is to understand key sources and clusters of model risk to help guide mitigating actions. The information should be collected first through a self-assessment exercise completed by the model owners and key users, if applicable, and checked for completeness and consistency, ideally by a centralised model risk team who has a separate reporting line to model owners or validators.

Each model should be scored based on impact and severity dimensions. Impact relates to the materiality of the model. For example, what balance sheet size does it account for, how much regulatory capital is attributed to it, and how many other models depend on it. For example a Value at Risk (VaR) model would have a higher impact score than a single derivatives pricing model.

Severity relates to the degree of complexity of the model. The metrics used to assess this should go beyond pure quantitative measures to include qualitative assessment as well. The assessment should cover the full model lifecycle with respect to:

- Data quality;
- Documentation quality;
- Quality of model development;
- Completeness/quality of validations performed;
- Quality of user acceptance testing;
- Quality of model deployment;
- Approvals obtained;
- Model use;
- Ongoing performance monitoring; and
- Degree of embedding into the business.

The assessment then provides a heatmap of key sources of model risk. The scoring data should be visually represented, so that gaps can be highlighted to help drive remedial actions, and also highlight

how far an organisation is from a target state. For example, in the following diagram, on a scale of 1 to 5 (with 1 being the lowest and 5 the highest), the model in question is assessed along several dimensions across the model lifecycle. The key sources of model risk are documentation quality, completeness/quality of validation, model use and ongoing model performance. This tells senior management that actions need to be taken to improve documentation, improve validation processes and ongoing monitoring of performance (e.g., backtesting), and ensure that model outputs are used appropriately (i.e., an appropriate control framework exists, and the right people are using the outputs to drive strategic decisions). However, the above should be viewed alongside the materiality of the model. If the model is highly material and has the weaknesses mentioned above, it would merit more management attention than a model with low materiality.

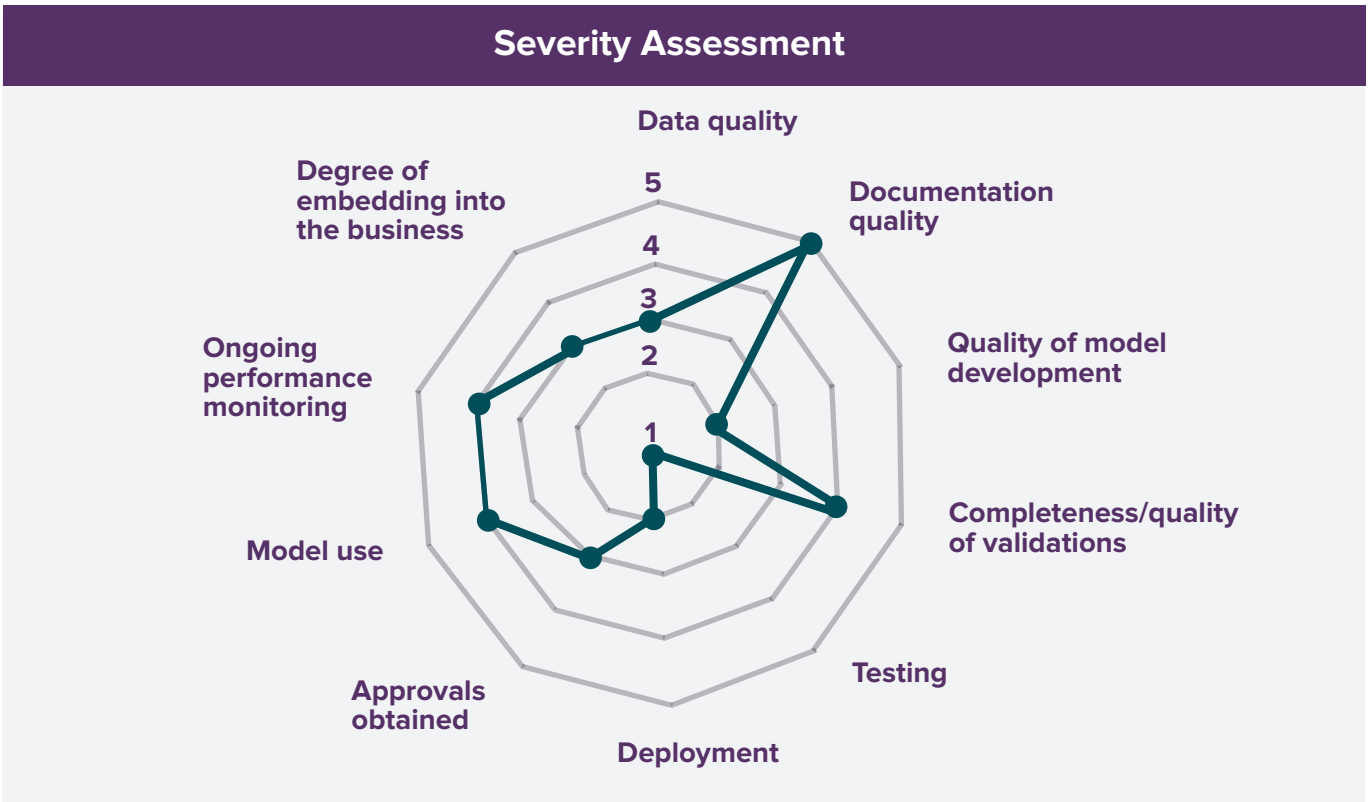


Figure 13: *Model risk scorecard: severity assessment*

The scoring exercises should be repeated periodically, so that the impact of management actions can be ascertained. Through time, one can understand model risk trends and emergent clusters that require senior management attention.

On top of model scoring, at the micro level the degree of model risk should be ascertained through model validation exercises. This can be done, for example, through identification and quantification of errors.

	Identification of error sources	Quantification of error
Data	• Insufficient data and data errors • Predictive power	• Output sensitivity to data error • Sensitivity to absence of variables
Model design	• Incorrect assumptions • Technological difficulties	• Sensitivity of results to scenario testing • Using alternative/external models to compare results
Model use	• Model not updated regularly • Inconsistent with model	• Simulate predictive power of a model over time • Impact of model misuse

Figure 14: *Examples of model risk quantification*

4.4 Model risk aggregation and reporting

The final question we pose in respect of a firm's Model Risk Management framework is the following: **Are senior management and the management body appropriately informed about the level of model risk in the firm?**

Development of comprehensive model risk reporting for senior management and risk committees becomes an essential part of model risk management. This requires having both some notion of individual risks, with the critical ones individually highlighted, and some notion of aggregate risk.

Once models are consistently scored, aggregation of model risk can be performed along multiple severity dimensions. Firms may want to think about how they weigh the scores based upon the impact score of a model. There may be a few dimensions across which organisations choose to aggregate their model risk, such as:

- Severity dimensions including:
  - Data quality;
  - Documentation quality;
  - Quality of model development;
  - Completeness/quality of validations performed;
  - Quality of user acceptance testing;
  - Quality of model deployment;
  - Approvals obtained;
  - Model use;
  - Ongoing performance monitoring;
  - Degree of embedding into the business;
  - Business unit;
  - Legal entity; and
  - Trading desk.

One can create a model risk hierarchy, so that the degree of model risk can be assessed at different levels of granularity (perhaps even from group level down to the level of an individual model). At the end of the day, the aggregation should be informative and help drive the right sorts of behaviours in the organisation, so that clusters of model risk can be mitigated in an effective and timely manner.

5. Industry Challenges

The key challenges for the industry and responses in building a model risk framework are summarised below. The goal for a firm is to:

- Know what types of models it has;
- Know how these models are performing;
- Know whether there is robust governance in place; and
- Ensure there is transparency and effective challenge of models.

KEY INDUSTRY CHALLENGES	
Establishing a framework that is adaptable to emergent risks and market changes	Balancing model complexity and operational necessities
Establishing a strong model infrastructure across the model lifecycle	Effectively challenging model design, development and use
Enhancing model risk assessment to support decision making	Improving and extending model review and validation processes
Establishing a strong model governance framework covering end to end model life cycle	Addressing insufficient input data
Operating an embedded control framework for model deployment and usage	Enhancing model performance monitoring
Ensuring robust evidencing across the model lifecycle	Creating a comprehensive model inventory

INDUSTRY RESPONSE

1. Perform a current state assessment of the model risk framework to identify gaps against best practice;
2. Enhance the model governance framework including policies and procedures, roles and responsibilities and committee structures;
3. Improve processes across the full model lifecycle including governance, documentation, monitoring and reporting;
4. Define methodologies for the consistent scoring of model across multiple dimensions that facilitate risk assessment, comparison and prioritisation;
5. Create a model container that encapsulates all model management components and facilitates the dynamic management of model risk;
6. Conduct independent model review, benchmarking and remediation to ensure that models withstand regulatory scrutiny;
7. Provide enterprise wide training on model risk.

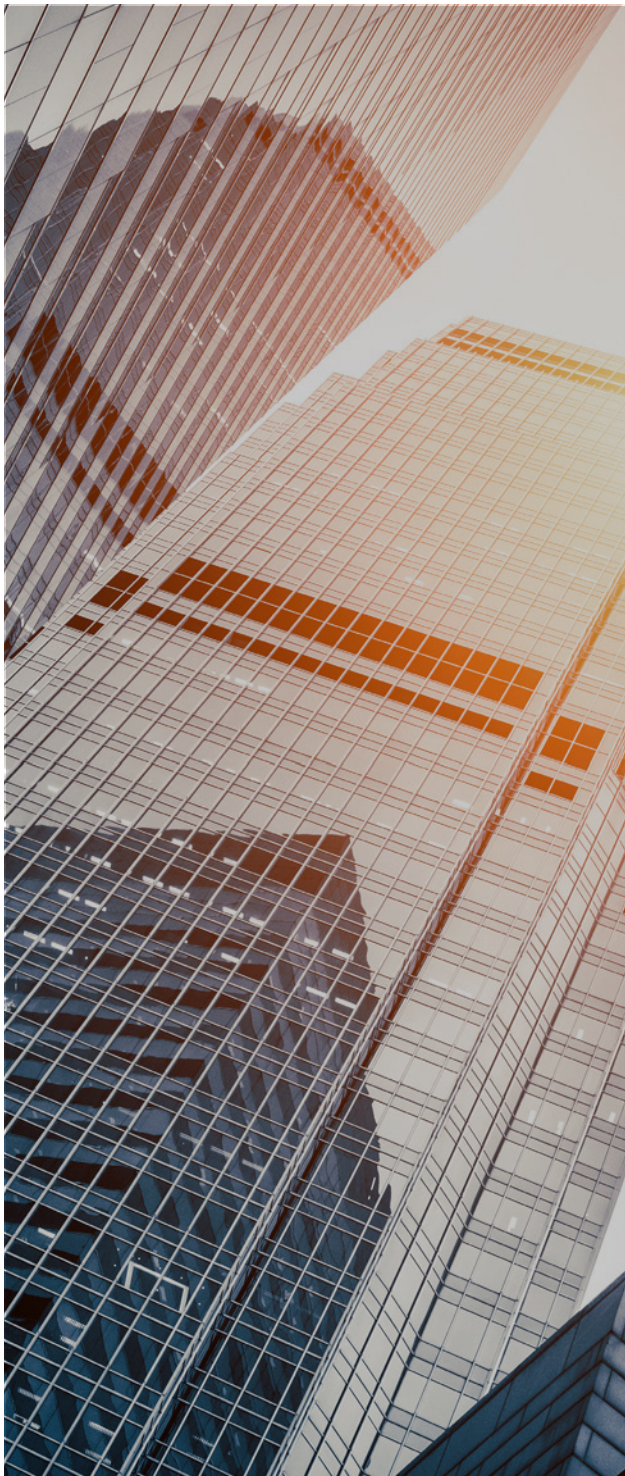
Figure 15: *Key industry challenges and responses*

6. Conclusion

Many high-profile cases of model failure, such as LTCM and the use of “Gaussian copulas” in the run up to the financial crisis, led to significant losses and reputational damage for financial institutions. The SR 11-7 regulatory guidance on model risk management has emerged as the de facto regulatory standard. Although banks in Europe have been slow to adopt SR 11-7, the Targeted Review of Internal Models (TRIM) has now put heightened focus on model risk management in the Eurozone.

Given the increasing impact of models on bank activities and the increasing weight of regulatory and supervisory scrutiny on model risk, banks will need to strengthen the robustness of their model risk management framework. The key components of a model risk management framework are governance, lifecycle, infrastructure, monitoring and reporting, and a container that links together all segments of a model.

In establishing a model risk management framework, banks have several choices to make. What is important is to get the right balance between sophistication vs. embeddedness that is commensurate with the bank’s business model. In terms of best practice, financial institutions should aim to have a complete model inventory, a centralised model risk function with the appropriate skills and expertise, a consistent scoring mechanism for models in their inventory, a strong control framework for model use, a view of risks across the full model lifecycle, a strong understanding of model performance, a clear articulation for technology choices – whether internal or vendor solutions -- and effective challenge of model assumptions. At the end of the day, the model risk management framework will need to stand the test of regulatory scrutiny and safeguard financial institutions from future losses and reputational damage.



CONTACTS

Avantage Reply (Amsterdam)

The Atrium | Strawinskylaan 3051
1077 ZX Amsterdam
Netherlands
Tel: +31 (0) 20 301 2123
E-mail: avantage@reply.com

Avantage Reply (Brussels)

5, rue du Congrès/Congresstraat
1000 Brussels
Belgium
Tel: +32 (0) 2 88 00 32 0
E-mail: avantage@reply.com

Avantage Reply (London)

38 Grosvenor Gardens
London SW1W 0EB
United Kingdom
Tel: +44 (0) 207 730 6000
E-mail: avantage@reply.com

Avantage Reply (Luxembourg)

22-24 Allée Scheffer
2570 Luxembourg
Luxembourg
E-mail: avantage@reply.com

Avantage Reply (Milan)

Via Castellanza, 11
20151 Milano
Italy
Tel: +39 02 535761
E-mail: avantage@reply.it

Avantage Reply (Paris)

Rue du Faubourg Sainte Honoré, 3
75008 Paris
France
Tel: +33 (0) 1 71 24 12 25
E-mail: avantage@reply.com

Avantage Reply (Rome)

Via Regina Margherita, 8
00198 Roma
Italy
Tel: +39 06 844341
E-mail: avantage@reply.it

Avantage Reply (Turin)

Via Cardinale Massaia, 83
10147 Torino
Italy
Tel: +39 011 29101
E-mail: avantage@reply.it

Avantage Reply (Lisbon)

Avenida da Liberdade, 110
1269-046 Lisbon
Portugal
Tel: +351 21 340 4500
E-mail: avantage@reply.com

Xuccess Reply (Frankfurt)

Hahnstrasse 68-70
60528 Frankfurt am Main
Germany
Tel: +49 (0) 69 669 643-25
E-mail: xuccess@reply.de

Xuccess Reply (Hamburg)

Griegstraße 75
22763 Hamburg
Germany
Tel: +49 (40) 890 0988-0
E-mail: xuccess@reply.de

Xuccess Reply (Munich)

Arnulfstrasse 27
80335 München
Germany
Tel: +49 (0) 89 - 411142-0
E-mail: xuccess@reply.de


REPLY
AVANTAGE