Deloitte.

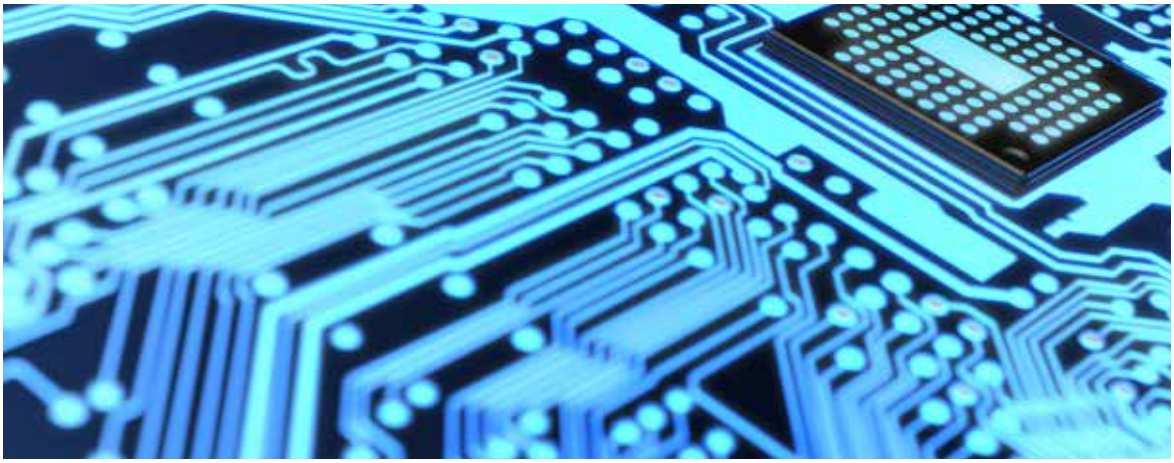
The evolution of model and algorithmic risk

A robust model risk management framework for financial institutions

Contents

Overview of model and algorithmic risk

Fundamentally, model risk management is about uncovering the assumptions that lie behind a model to understand how it contributes to risk at the organisational level.



With increasing volumes of data, and recent advances in technology and computational power, including the introduction of Artificial Intelligence (AI) and Machine Learning (ML), models are at the heart of every financial institution's operations – the backbone of every function and business line, from product design, to treasury and trading, risk management, compliance, and internal audit. But as financial institutions increasingly rely on the output of models for their decision-making, the focus on model risk – or the risk of errors in the development, implementation, or use of models – has also continued to gain momentum.

There are several reasons for this. Firstly, the evolving technological capability of these algorithms have resulted in a widespread democratisation of model development, enabling individual users to develop and deploy their own algorithmic models without relying on internal IT or traditional model development functions. While this increases the speed of innovation, it also increases the level of risk that organisations are exposed to, as these new generations of models are not subjected to the same robust testing systems and governance structures as traditional ones.

Secondly, there has been increasing stakeholder expectations related to the documentation, accountability, controls, and risk management of models. Regulators, in particular, have been intensifying their scrutiny on model risks, with a particular focus on models that include elements of AI systems and ML algorithms.

In this paper, we present a robust model risk management framework designed to help financial institutions assess and monitor their model risks. We examine the five key pillars that such an organisation-wide framework would require, and propose the use of a central model inventory to monitor models throughout their entire life cycle. Finally, we take a look at the five stages of developing a robust model risk management framework, designed to help financial institutions implement an effective risk assessment and quantification mechanism for their models.

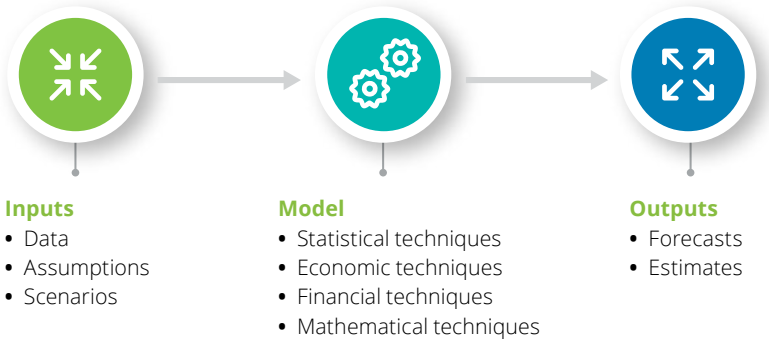
A primer on model risk

What is a model?

A model refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. It consists of three components (see Figure 1):

1. **Inputs**, including data, assumptions, and scenarios
2. **Processing**, which transforms inputs into estimates with the use of statistical, economic, financial, or mathematical tools
3. **Outputs**, including forecasts, and estimates, that translate into useful business information to support management decision-making

Figure 1: Three components of a model



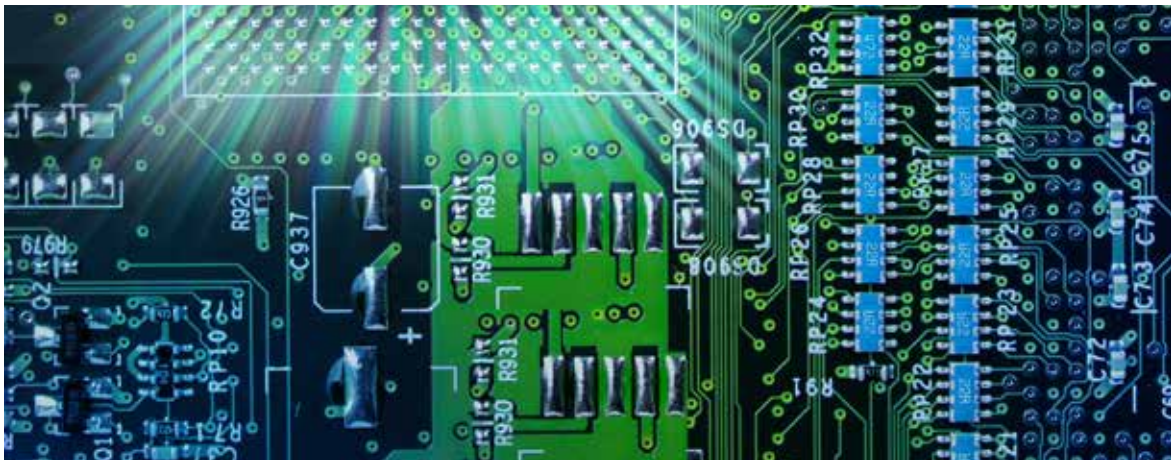
It is important that financial institutions are able to consistently define and manage models within their organisations, but this is challenging as different stakeholders tend to have different opinions about how a model should be defined. For example, while most can agree that a model exists when advanced and sophisticated techniques are used, they may disagree on whether they consider a simple arithmetic formula to be a model. The reality, however, is that even spreadsheets can be models – with the potential to present a significant amount of risk for financial institutions.

What is model risk?

According to the Capital Requirements Directive (CRD IV) in Europe, model risk is defined as the potential loss that a financial institution may incur, as a consequence of decisions that could be principally based on the output of models, due to errors in the development, implementation, or use of such models. Similarly, algorithmic risk may rise from the use of data analytics and cognitive technology-based software algorithms in various automated and semi-automated decision-making environments.

A robust model risk management framework

The focus of a robust model risk management framework goes beyond merely meeting compliance obligations, to ensuring that financial institutions put in place the appropriate risk controls for all material models and algorithms which support their decision-making processes.



Democratisation of model development

Across financial institutions, we are witnessing a decentralisation of model development within organisations. While models were traditionally developed in model development teams, the increased ease of access to IT infrastructure, such as cloud computing, open source algorithms, and visualisation tools, have resulted in the democratisation and decentralisation of model development. This results in a more agile and flexible approach to model development, where any users are able to design, develop, and deploy their own models and algorithms without the need to rely on internal IT or model development functions.

Although this phenomenon has increased the speed and ease of innovation, it also exposes financial institutions to higher levels of operational, regulatory, financial or reputational risks. Unlike traditionally developed models, which are governed by long-established policies relating to their development, validation, monitoring, and review, the new generation of complex ML algorithms are subjected to less robust testing systems and governance structures.

What this could lead to is a lack of clarity on model ownership, authority, and responsibility, for example, when changes to a model's assumptions are not documented or clearly audited. As these models form the basis of significant management decisions, their assumptions, limitations, and even usage against their intended purpose, could compromise the organisation and lead to significant increases in the level of risk.

Risk factors

Model and algorithmic risks should be considered as specific risk type to be managed in a similar way to other risks faced by financial institutions. This means that a thorough and robust framework should be put in place to identify, assess, mitigate, and monitor the evolution of model and algorithmic risks across the entire organisation, especially with increasing usage of ML and AI techniques.

Ultimately, there are several underlying factors that contribute to model risk:

- **Human biases:** The cognitive biases of model developers and users could skew outputs and yield unintended outcomes, especially when there is lack of governance or a misalignment between the organisation's values and the behaviour of individual employees.

- **Technical flaws:** A lack of technical rigour during the development, training, testing, or validation processes could result in models producing inaccurate outputs.
- **Usage flaws:** Even if the models produce accurate outputs, flaws in their implementation by end users, or integration with operations could result in inaccurate judgements during the decision-making process.
- **Security flaws:** Security breaches could enable internal or external actors to manipulate the outputs of a model to influence decision-making.

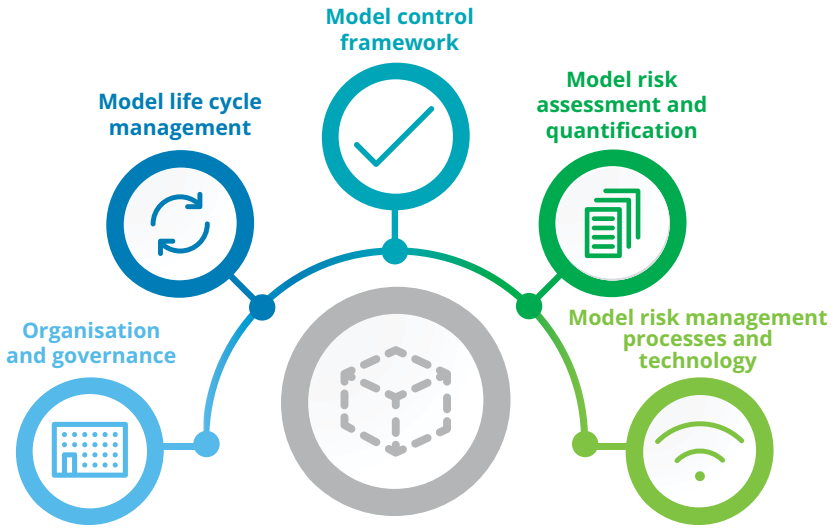
Five pillars of a model risk management framework

Regardless of the organisation's size and structure, an organisation-wide model risk management framework should consist of clearly defined roles and responsibilities across all stages of a model's life cycle, from risk identification and assessment, to measurement and mitigation, and monitoring and reporting. In addition, a sound model risk management framework should also define the level of control required for each model or algorithm within its scope, depending on the magnitude of the impact that it is expected to have on business performance and organisational reputation, and ensure clear accountability for each model and algorithm.

Overall, a robust model risk management should include five key pillars, which will need to be adapted to the level of materiality and complexity of the scope (see Figure 2):

- **Organisation and governance**: Existence of a model risk management function, approved by the board and reporting to the Chief Risk Officer, which assesses and manages model and algorithmic risks within the organisation.
- **Model life cycle management**: Monitoring of all stages in a model's life cycle, including development, documentation, classification, validation, and inventory maintenance on a continuous basis
- **Model control framework**: Initial validation before implementation and continuous review of models and algorithms that have been assigned the highest level of risk
- **Model risk assessment and quantification**: Assessment and quantification of model and algorithmic risks with the use of qualitative and quantitative techniques
- **Model risk management processes and technology**: Implementation of the appropriate processes and technology to support the management of any traditional or AI-based models

Figure 2: Five pillars of a model risk management framework

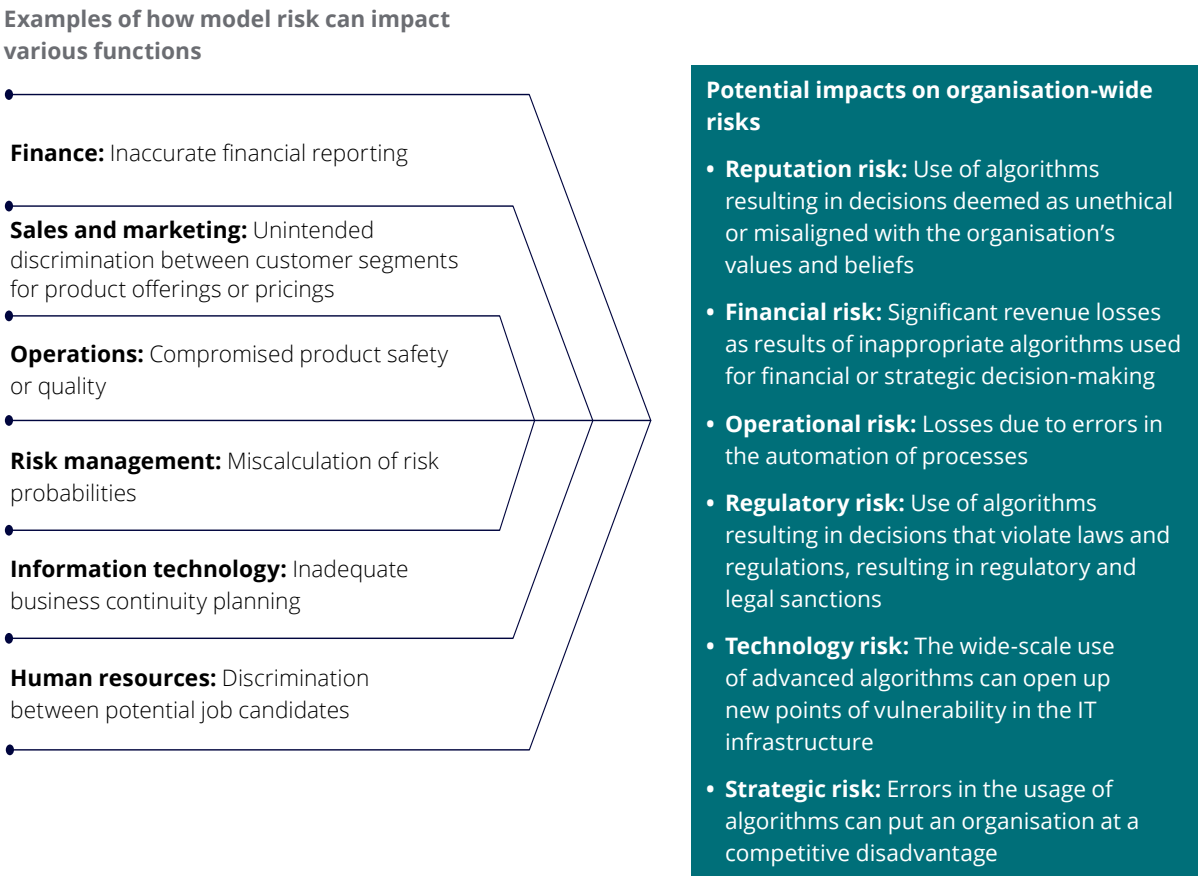


Raising awareness on model and algorithmic risk management

In order for financial institutions to assess and monitor their model risks, the appropriate metrics will need to be defined in alignment to the organisation's risk appetite statement and risk tolerance limits, and continuously monitored by the board and senior management, as they have potentially significant and costly implications for a business (see Figure 3).

The implementation of a central model inventory that encompasses all of an organisations' models, tools, and calculators can also enable stakeholders to assess the risk criticality levels for each model based on materiality, and complexity, and focus testing and validation efforts on models that are deemed to be of higher risk. Such an inventory would also enable risk mitigation actions to be documented, and improve the ability of the organisation to identify models that are not fit for purpose, or which have been used for unintended purposes.

Figure 3: Potential implications of model risk on a financial institution



Developing a robust model risk management framework

Broadly, there are five stages to implementing a robust model risk management framework to enable organisations to reap the benefits of models while mitigating the risks that they bring:

1. Designing the organisation-wide, centralised model risk management governance framework

A systematic approach towards delegating and coordinating essential risk management responsibilities consists of three main lines of defence that aim to enhance communication about model and algorithmic risks, and clarify essential roles and responsibilities:

- First line of defence, responsible for originating and owning the risk
- Second line of defence, responsible for overseeing the risk, including assessment, measurement and mitigation
- Third line of defence, responsible for providing independent assurance of the organisation's adherence to internal policies and controls, as well as external regulations

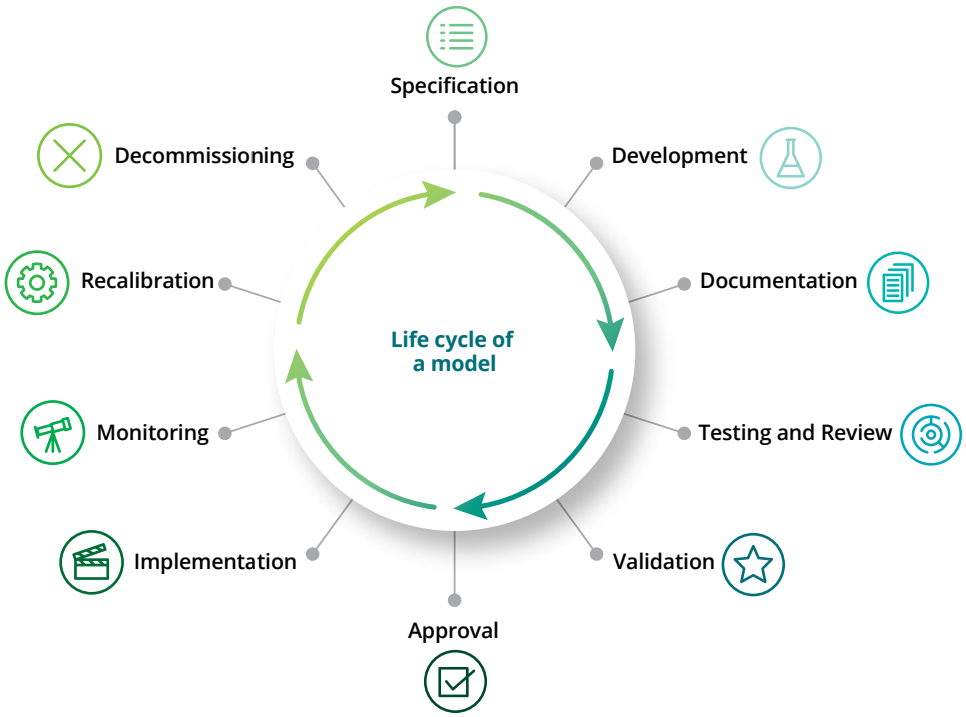
Generally, the model risk management function should be located within the second line of defence, tasked with the responsibility of setting up and maintaining the model risk management framework, and reporting directly to the Chief Risk officer. The board should also receive regular reports on the implementation of model risk management policies, and be informed of any model risks that may have a material impact on the organisation. This would enable financial institutions to develop an integrated view of its model risks, and achieve better alignment between all stakeholders.

With the increased usage of AI and ML posing a new set of challenges for the governance structure, financial institutions should also identify the stakeholders who would need to be accountable for AI-based decisions, and responsible for a model's outcomes. At the same time, stakeholders will need to develop a better awareness of any potential biases in the design, implementation, or use of AI systems, and consider putting in place a sign-off process on the potential consequences related to the fairness, ethics, and transparency of AI-based decisions.

2. Streamlining model life cycle management within the organisation
A streamlined process for managing model life cycles can enable organisations to manage their risks centrally while improving workflow efficiency. One approach that many leading financial institutions have adopted is the use of model risk management platforms to automate some of the tasks and activities related to model life cycle management.

Specifically, the model risk policy specifies the control point and role-based responsibilities in the workflow processes for each stage of a model's life cycle, from specification, development, to documentation, testing, review, validation, approval, implementation, monitoring, recalibration, and finally, decommissioning (see Figure 4).

Figure 4: Stages in the life cycle of a model



In addition to a model's life cycle, financial institutions should take into account the specificities of AI systems by updating the model monitoring processes to accommodate the continuous model monitoring and re-evaluation of the algorithms, from both technical and systems points of view. Additional AI-related metrics – based on the principles of fairness, ethics, accountability, and transparency (for more information, please refer to "Increasing regulatory scrutiny") – should also be part of the model's life cycle, and be used to determine if an algorithm remains fit for purpose.

3. Strengthening the quantitative and qualitative validation framework

To ensure that models remain fit for purpose, all models and algorithms should undergo a initial and periodic review and validation, with the depth of the review varying according to the model's materiality and level of risk. While the review for less material models may focus only on specific components, the review for more material models should be subjected to more in-depth and complex validation, including independent validations of all of their components, to ensure that the organisation's overall portfolio of models remain within acceptable risk limits. A strict, robust validation process and bias adjustment is then required to eliminate any model risk.

Given their higher levels of complexity, AI and ML models pose a unique set of challenges to model risk management and model validation. For these models, independent validation of their individual components becomes especially important. If, for example, a specific optimisation method was selected to obtain the hyperparameter corresponding to a best-performing model, this choice should be challenged by independent stakeholders during the validation process to ensure that the specificities relating to the ML algorithm has been taken into account, and the appropriate techniques have been chosen to fulfil the purpose.

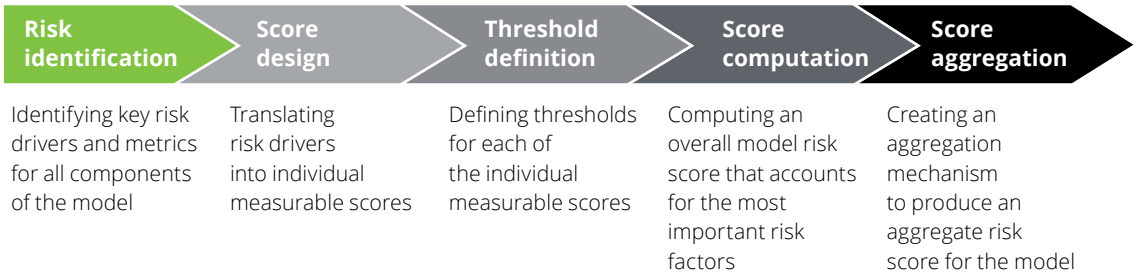
Model validation policies should also be updated to include the extensions related to the usage of ML techniques, and incorporate additional analysis to cater to AI-related complexities. As an illustration, ML validation extensions could include the following:

- Data specificities, for example, the usage of unstructured data, and fresh data bias in self-learning models
- Model soundness related to optimisation functions used for hyperparameter tuning
- Enhanced performance metrics and bias detection for model output testing, including ML interpretability, fairness, and ethics-related metrics
- AI systems in compliance with existing regulations
- Implementation challenges and controls for automated recalibration

4. Implementing an effective model risk assessment and quantification mechanism

The assessment of model risk is a crucial step that determines how models are classified and how activities are to be prioritised for model risk managers and model validation functions. It is therefore imperative that the model risk management framework be supported by an appropriate assessment and quantification mechanism that considers a range of factors, including materiality, financial impact, and model health factors such as the model's intrinsic methodologies, conceptual soundness, and performance testing. The effort required for maintenance and compliance with other internal or external bodies should also be one of the considerations during the assessment. To assess their model risks, several leading financial institutions have adopted a scorecard-based approach (see Figure 5).

Figure 5: An effective risk assessment mechanism



In terms of quantification, it is important for financial institutions to measure and quantify the amount of model risk they have taken by potentially using incorrect models. During model development, the simplification is inevitable or even intentional in order to avoid other challenges such as overfitting of the models. Models may be misspecified and their outputs differ from the reality in which case adjustments should be made to account for the "known unknowns". The quantification process should also consider estimating the risks coming from the "unknown unknowns" in data, methodologies or calibration.

Although model risk quantification methodologies are in their early stages of development, regulators and financial institutions should consider the use of additional capital requirements to account for model risk adjustments.

5. Supporting the process and workflow with a MRM platform

Model risk management framework should be enhanced by a platform to support the workflow during model lifecycle with role-based responsibilities at each control point in the workflow. The MRM platform should track any model related tasks and activities with oriented deadlines and status reporting.

Generally, a successful model risk management platform integrates the workflow and model inventory with the associated document repository to facilitate reporting and analysis requirements, and leading financial institutions have implemented centralised systems that integrate and connect all of these components.

Increasing regulatory scrutiny

As financial institutions increasingly turn towards AI and ML models as alternatives to traditional models to obtain faster, more accurate predictions for better business decisions, there has been increasing stakeholder scrutiny on the way model and algorithmic risks are managed within an organisation.

On the regulatory front, regulators are paying greater attention to model risk management frameworks, with a particular emphasis on those that relating to algorithmic risk given the raise of AI usage. Examples of such regulation include the US Federal Reserve's Supervisory Guidance on Model Risk Management (SR 11-7) and the European Central Bank's ECB guide to internal models.

In Singapore, the Monetary Authority of Singapore (MAS) recently released its set of principles to promote fairness, ethics, accountability, and transparency in the use of Artificial Intelligence and Data Analytics (AIDA) – defined as technologies that support or replace human decision-making – in Singapore's financial sector. These principles aim to guide financial institutions in their internal governance and mitigation of model and algorithmic risks as they work on the development of their AI technologies. According to MAS, firms that employ the use of AIDA should calibrate their internal governance frameworks according to their considerations of materiality (see Figure 6).

Figure 6: Key features of FEAT principles developed by MAS

Fairness

- **Justifiability:** Internal governance framework for models that provide justification for using specific factors in a decision
- **Accuracy and bias:** Internal validation and periodic review of models according to the level of materiality and complexity to minimise unintentional biases

Ethics

- **Ethics review board:** An organisation-wide ethics review board to conduct periodic reviews of decisions made with the use of AIDA systems to ensure that they are in line with the organisation's code of conduct

Accountability

- **Ownership:** Use of internally and externally sourced AIDA to be approved by an internal authority according to their materiality and complexity, and internal reporting systems to ensure awareness by both senior management and board

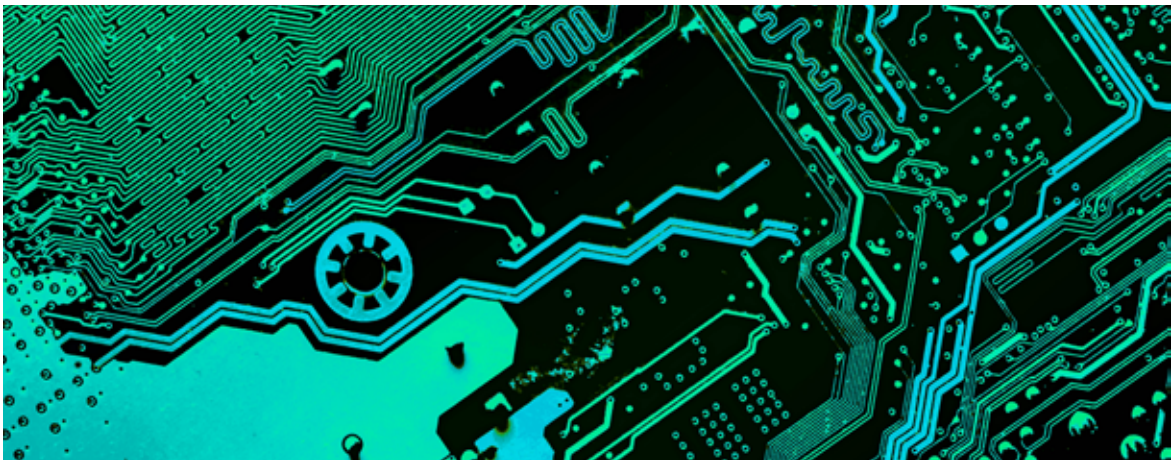
Transparency

- **Disclosure:** Clear and proactive explanations of the consequences of AIDA-driven decisions to subjects in general communications

This direction has also been reinforced by the efforts of policy makers and regulators in Singapore, such as the Personal Data Protection Commission, which released its first discussion paper presenting its Model AI Governance Framework. The objective is to articulate a common AI governance approach and a set of consistent definitions and principles relating to the responsible use of AI to promote the adoption of AI, while ensuring that regulatory requirements are met, and AI risks are assessed, measured, monitored and mitigated.

Embedding model risk management in risk culture

There is no one-size-fits all approach to model risk management. It is important for financial institutions to right-size their framework based on their unique needs.



At its core, a model risk management framework should cover model governance, modelling standards, and model validation. Beyond that, however, the robustness, standardisation, and resources used to implement the components will vary based on each organisation's needs.

A good starting point is to develop an understanding of leading practices for processes, controls, and documentation, and then to balance those practices against specific business needs to determine what level of maturity is desirable and achievable. Organisations should evaluate their desired level of model risk management against model uses, risks, overall model risk appetite, and other factors such as overall business operations, growth plans, accounting bases, regulatory oversight, and rating agency expectations.

When setting up a model risk framework, there is typically a strong focus on what rules need to be followed, with very prescriptive policies and standards. Understanding what needs to be done is important, but there is a risk of the programme becoming so rules-based that true change in the culture of the organisation regarding how models are developed, implemented, and used is sacrificed.

Ultimately, a model risk management framework should strive to embed a model governance culture within the organisation. Rather than focusing only on compliance, the framework should provide guidance, standardisation, and clear communication channels – features that could lead to long-term, improved efficiency in model development with enhanced governance.

By putting in place internal governance and structures with clear roles and responsibilities for the ethical usage of AI throughout the various stages and activities involved during the life cycle of any AI deployment, organisations can better promote the responsible use of advanced AI-based technologies. In this way, risk management can contribute to a better and sounder decision-making process, instead of being simply an oversight function.

Researched and written by

Nadège Grennepois
Partner, Risk Advisory
Deloitte France
ngrennepois@deloitte.fr

Frédéric Bertholon-Lampiris
Partner, Risk Advisory
Deloitte Southeast Asia
flampiris@deloitte.com

Contributors

Tony Wood
Partner, Risk Advisory
Deloitte Asia Pacific

Mark Woodley
Partner, Risk Advisory
Deloitte Southeast Asia

Anca Maria Alvirescu
Senior Consultant, Risk Advisory
Deloitte Southeast Asia

Contacts France

Nadège Grennepois
Partner, Risk Advisory
Deloitte France
ngrennepois@deloitte.fr

Angaman Franck Alain Affali
Senior Manager, Risk Advisory
Deloitte France
aaffali@deloitte.fr

Deloitte.