Every Model Matters –

How AI Adoption is Reshaping the role of Model Risk Management

Table of Contents

01

Introduction

Introduction

Artificial Intelligence (AI) is rapidly reshaping European banking. From credit processing and risk assessment to customer interaction and process automation, AI models and systems are becoming embedded across virtually every business function. Yet this transformation is unfolding against a regulatory backdrop that is both ambitious and fragmented. The EU AI Act, the world's first comprehensive AI law, introduces a risk-based classification framework that applies to developers and deployers alike, while existing model risk management (MRM) requirements under MaRisk, the ECB's Guide to Internal Models, and national supervisory expectations continue to evolve in parallel. Beyond Europe, the United States and the United Kingdom rely on existing guidance and principles-based oversight rather than prescriptive AI-specific legislation, and jurisdictions across the Asia-Pacific region are charting their own diverse paths. For banks operating internationally but also banks only focused on Europe, this patchwork of regulatory regimes creates a compliance landscape of considerable complexity, one where definitions of what constitutes an "AI system," an "AI model," and a "model" in the AI and MRM sense do not always align.

This paper examines how banks are navigating that complexity in practice. Drawing on detailed case studies from three leading German financial institutions, Commerzbank, Deka, and KfW, it captures a spectrum of approaches to AI governance and model risk management. These institutions differ in size, business model, systemic importance, and regulatory exposure, and their strategies reflect that diversity. Some have pursued fully integrated governance frameworks that bring AI models under a unified MRM umbrella.

Others have adopted more pragmatic architectures, recognizing synergies between AI governance and MRM where they exist but keeping the two domains separate where practical considerations demand it. Common to all, however, is a set of shared challenges: the rapid increase of AI use cases beyond traditional model teams, the heightened demands around explainability and fairness, the opacity of third-party and general-purpose AI models, the speed at which techniques such as Generative AI and agentic systems are evolving, and the fundamental tension between the pace of innovation and the pace of regulation. Historically, the 2nd line risk function, particularly MRM, has been viewed as a bottleneck in the model lifecycle. But in the context of AI's rapid and disruptive adoption, this perception risks not only slowing down progress but also missing opportunities for strategic alignment between control functions and the business. The contributing banks demonstrate that MRM needs to evolve from a reactive gatekeeper into a proactive enabler of responsible innovation offering early-stage advisory, challenge, and guidance that can accelerate rather than impede AI deployment.

What emerges from comparing these institutions is a clear and converging message to regulators. Banks are calling for greater harmonization, not only across jurisdictions but also between AI-specific regulation and established MRM requirements. Two paths are on the table: either the financial services industry receives dedicated supervisory guidance on how to interpret and implement the AI Act alongside existing model governance obligations, or financial services are carved out from the AI Act's model governance scope entirely, creating the opportunity for a single, comprehensive EU-level MRM framework that covers both AI and non-AI models. Regardless of which path prevails, the contributing institutions agree that rigid, highly detailed rules cannot keep pace with exponential technological change. What is needed instead is a flexible, principles-based framework that provides clarity on AI risk classification, validation dimensions for novel model types, the treatment of third-party AI, and the role of proportionality in governance, while leaving room for the industry and its supervisors to adapt as the technology continues to evolve.

This paper aims to contribute to exactly that dialogue. It maps the regulatory landscape, surfaces the practical realities of AI governance inside European banks, and distils a set of open questions intended as a starting point for structured engagement between the financial services industry and its regulators, an engagement that is urgently needed if Europe is to avoid falling behind in AI adoption and, ultimately, in global competitiveness.

The paper is structured as follows. Section 2 surveys the global regulatory landscape for AI in banking, contrasting the approaches of the EU, the US, the UK, and selected APAC jurisdictions. Section 3 presents detailed case studies from the three contributing banks, examining how each has adapted its governance and model risk management frameworks to accommodate AI. Section 4 synthesizes these perspectives into a cross-institutional comparison, identifies key open questions facing the industry, and concludes with a call for dialogue between the industry and regulators.

02

Regulatory landscape for AI in banking

Regulatory landscape for AI in banking

AI regulation is rapidly evolving, with major regions adopting distinct approaches that impact compliance strategies and business operations. Understanding these frameworks is essential for multinational organizations seeking to innovate responsibly and maintain market access. When developing and deploying AI models, European Banks must therefore navigate a complex and dynamically evolving regulatory landscape. On the one hand, they are required to comply with AI-specific regulations, but on the other hand they must also satisfy existing requirements and supervisory expectations for financial institutions such as MRM. This complexity further increases for banks operating internationally, as they must also deal with varying regulatory regimes in both domains across different jurisdictions.

The global regulatory landscape for AI is largely shaped by two different approaches:

1. Prioritizing the safe and responsible use of AI,
2. Promoting AI innovation and competitiveness.

In the first category are the countries that already have or are about to introduce comprehensive AI regulations such as the EU. Those jurisdictions do not oppose AI innovation but want to reduce the risk of harmful AI usage. In the second category are countries that see AI as a competitive advantage and are therefore cautious to introduce AI regulation to avoid slowing down AI development such as the UK or the US. This does not mean that those jurisdictions are not wary of harmful AI usage, but they prefer to closely monitor AI advancements and intervene with specific AI regulation only when deemed necessary.

Regulatory landscape in the European Union

The EU AI Act, effective August 1, 2024, is the world's first comprehensive law regulating AI. It establishes a risk-based framework for evaluating AI systems used across the EU economy, targeting both developers (creators or major modifiers of AI) and deployers (users of AI in real-world settings). Financial institutions, as significant AI users, could fill both roles.

The Act categorizes AI systems by risk (1), (2):

- Unacceptable: Banned systems that threaten safety, livelihood, or rights.
- High: Systems with significant impact, subject to strict oversight and conformity assessments on data quality, human oversight, transparency, documentation, accuracy, robustness, cybersecurity, and quality management (1), (2).
- Limited: Require transparency so users know they are interacting with AI.
- Minimal: Negligible risk; few requirements.

For financial services, Annex III lists AI used in credit scoring, risk assessment, and insurance pricing for individuals as high-risk, triggering extra reporting and review requirements (1). Oversight is conducted by national financial supervisors and the European Supervisory Authorities (EBA, ESMA, EIOPA), with support from the European AI Office (1), (2), (3).

The Act regulates AI systems but not AI models directly, except for General Purpose AI (GPAI) models, which are defined and subject to specific requirements (1). Recital 97 clarifies that AI models are essential components of AI systems but are not standalone systems (1).

Model risk management (MRM) regulation for financial institutions in the European Union is fragmented. The ECB Guide to Internal Models (EGIM) is a European regulation providing overarching guidance for model risk management, for instance regarding machine learning risks in internal models, with a focus on explainability, governance, skill requirements, validation, and robust IT/data infrastructure (4). However, the EGIM is limited to pillar 1 models and no unified EU-wide binding MRM regulation exists. As a result, the regulatory landscape relies heavily on national frameworks to address gaps, with for instance Poland's "Recommendation W" setting standards for bank model risk management, but lacking explicit AI sections (5), and Germany's revised MaRisk (2024) introducing requirements for model explainability and data quality, especially for innovative AI models used for risk management (6).

Regulatory landscape in the United States and the United Kingdom

As of late 2025, neither the US nor the UK has comprehensive, binding, cross sector AI legislation. Both rely mainly on existing laws and sectoral supervisors, with a principles-based MRM regulatory framework.

In the US, federal supervisory authorities emphasize innovation while managing risks with existing statutes. Agencies like the Consumer Financial Protection Bureau apply longstanding laws, such as the Equal Credit Opportunity Act, to ensure fairness and prevent discrimination in AI-driven credit decisions. Officials such as the Comptroller of the Currency advocate technology-neutral, risk-based oversight, which is already integrated into banking supervision (7), (8), (9), (10). Until recently, model risk management for AI had been handled under established regulation such as SR 11-7, requiring robust model development, implementation, and validation, without imposing extra legislative burdens on banks (11), (7), (8), (9), (10). However, in its *"Revised Guidance on Model Risk Management"* (SR 26-2), Footnote 3 of the guidance explicitly excludes agentic and generative AI systems from the newly released MRM requirements. Nevertheless, non-agentic and non-generative AI models remain within the scope of SR 26-2 and banks are still expected to apply their broader risk management and governance frameworks for any systems, processes or tools out-of-scope of the updated MRM guidance (12).

Likewise, the UK takes a principle-based approach to AI. The National AI Strategy and the 2023 White Paper set out five guiding principles, namely safety, transparency, fairness, accountability, and contestability, administered by sectoral regulators like the Financial Conduct Authority (FCA) and Bank of England (BoE) (13), (14). The Supervisory Statement SS1/23 defines general model risk management standards, encompassing interpretability and transparency for AI models (15). Oversight is conducted through existing statutory powers, allowing regulators to enforce requirements around consumer protection and operational resilience as needed (14), (16).

Additional regulatory initiatives

Countries in the APAC region have adopted diverse AI regulatory approaches, with some aligning more closely with the EU model and others resembling the US/UK frameworks. For example, Japan uses a principle based, pro innovation AI framework, complemented by principles for model risk management (17). Japan's AI Promotion Act and AI Business Guidelines emphasize fairness, safety, human centricity and innovation, while FSA principles treat AI as general models under strong governance and validation (18), (19). On the other hand, South Korea's AI Basic Act is an overarching, risk-based law that promotes ethical and innovative AI, requiring high-impact systems to undergo assessment, risk management, explainability, and human oversight, but stopping short of requiring EU-style bans and with relatively low fines (20).

Global AI Regulatory Landscape

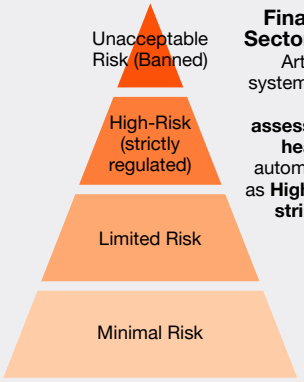
Risk focused

Innovation focused

EU: Risk-based approach

AI regulation
- **Cross-sectoral, risk-based** AI regulatory framework
- Focus on safe and responsible AI use
- **Bans** models classified as **unacceptable risks**

Model Risk Management:
- Union-wide regulation does not exist
- EU-level guidance **(ECB's EGIM)** and national frameworks (e.g., Germany's **MaRisk**) explicitly **address AI/ML deployment in quantitative risk models**
- Particular **focus** lies on **explainability**, though binding requirements remain fragmented across member states



Financial Services Sector Implications: Artificial Intelligence systems used for **credit scoring** and **risk assessment** in **life and health insurance** is automatically classified as **High-Risk, requiring stringent oversight**.

US: Innovation through deregulation

AI regulation
- **No federal AI legislation**; regulation limited to state-level laws (e.g., Colorado AI Act)
- **AI governed** through **existing agencies** rather than a dedicated regulator
- Emphasis on innovation and understanding AI use cases over prescriptive regulation

Model Risk Management (SR 26-2):
- **SR 26-2**: Supervisory **guidance** on **MRM** issued by the Fed and OCC, setting expectations for model development, validation, and governance
- **Non-agentic and non-generative AI models** governed under this framework

Dedicated AI regulation only — **Consolidated AI & MRM Regulation** — **Dedicated MRM regulation only**

Risk-based standards without outright bans

AI regulation
- AI Basic Act establishes **risk-based standards**; high-risk AI requires assessments and human oversight but **avoids outright bans**

Model Risk Management:
- **No unified MRM framework** or clear AI model definition; updated FSC guidelines expected

Balanced approach

AI regulation
- **AI Promotion Act sets broad principles**; primarily a framework for future legislation

Model Risk Management:
- FSA MRM Principles emphasize **three-lines-of-defense governance**
- AI/ML models expected to fall under **existing "Principles for Model Risk Management" framework**

Sector-specific approach

AI regulation
- **Sectoral governance approach** with voluntary AI Governance Framework (2019, updated 2024) covering transparency, fairness, and accountability

Model Risk Management:
- **No unified MRM framework; AI-specific MRM guidance** (2024) and MAS Guidelines (2025) introduce first formal AI model deployment guidelines for the **financial services sector**

UK: Flexible, principles-based approach

AI regulation
- **No overarching AI legislation**; principles-based approach via existing sector-specific regulations (White Paper, 2023)
- **Outcomes focused** rather than prescriptive rules

Model Risk Management:
- **SS1/23**: PRA guidance defining **five core MRM** principles (identification, governance, development, validation, risk mitigants) for banks using internal models
- SS1/23 **considers key risk factors** associated with AI models, including **interpretability, explainability, and potential bias**

Figure 1: Global AI Regulatory Landscape

03

Model Risk Management for AI models

Model Risk Management for AI models

Artificial Intelligence (ML, Gen AI and Agentic AI) is becoming deeply embedded in the operating fabric of European banks, reshaping processes, decision-making, and customer interaction. As AI adoption accelerates, financial institutions face a dual challenge: implementing AI systems safely and responsibly while aligning with a fragmented and rapidly evolving regulatory landscape. In this section the focus is on practical insights from three leading German banks, Commerzbank, Deka, and KfW, on how to adapt MRM frameworks for AI at scale.

Across all business models, a dominant theme emerges: AI is not simply another model type, but a class of systems with unique operational, ethical, and governance implications. Yet, inconsistent definitions across supervisory standards create ambiguity over when AI systems fall under classical model governance and when they require new oversight mechanisms. This definitional uncertainty is compounded by overlapping regulatory requirements and diverging international approaches, forcing banks to navigate a complex compliance landscape. Against this backdrop, AI literacy gaps and decentralized development are rapidly expanding usage risk beyond traditional model users, while the pace of AI innovation increasingly outstrips traditional MRM processes.

Interviews with the three contributing banks reveal that, despite differing starting points, they face a consistent set of practical challenges:

- **Defining and scoping AI**: Divergent regulatory definitions of "AI system," "AI model," and "model" force each institution to develop its own approach to delineating what falls under AI governance, MRM, or both.
- **Designing governance and the role of the Three Lines of Defence**: The wide range and cross-functional nature of AI demands new governance structures that rethink how responsibilities are allocated across the three lines.
- **Applying proportionality and tiering**: The volume and diversity of AI use cases require risk-based classification frameworks that calibrate oversight depth to potential impact and complexity.
- **Managing third-party and Model-as-a-Service (MaaS) risks**: Growing reliance on external AI providers introduces supply-chain risks around transparency, controllability, and documentation that challenge conventional validation practices.
- **Establishing AI-specific validation approaches**: Transparency, explainability, fairness, and the dynamic behaviour of techniques such as Generative AI and LLMs demand validation methods well beyond those used for traditional statistical models.

Despite these challenges, the banks converge on a shared direction: adopting risk-based and proportional oversight, evolving (not only) MRM from a reactive control function into a proactive enabler of responsible innovation, and leveraging technology to keep up with the speed of AI adoption. The following case studies reflect each institution's individual perspective and priorities, shaped by its size, business model, systemic classification, and regulatory exposure. They are intentionally not written to a uniform template and the diversity of approaches is itself a finding of this paper. However, several recurring themes connect the contributions which are summarized in Table 1.

	Commerzbank	Deka	KfW
Business model	International commercial bank	Large securities services provider	German development bank
AI / model definition approach	• Dual approach: broader scope currently (full AI inventory including regression models per ML Guideline) • Narrower definition going forward aligned with ECB (e.g., regressions excluded from AI)	• Clear distinction between MaRisk model definition and EU AI Act definition of AI system • Not every AI system should automatically be identified as a model	• An AI model is recognized as a model in the MRM sense if it fulfills the MaRsik-driven model definition
MRM and AI governance integration	• Fully integrated: AI governance, ML policy, and MRM framework operate as a unified system under the 3LoD	• Deliberately parallel: AI governance and MRM governance run as independent but interacting control loops • Exchange between the two systems advised	• Separate guidelines for AI usage and model usage • Both guidelines cross-reference each other
AI Risk categorization	• AI risk is handled as a horizontal driver within existing risk categories • Four damage potentials: Human Oversight, Fairness, Transparency, Reliability; risk classification per ML Guideline	• No new (internal) risk category for AI risk. • Risk categorization for AI system follows EU AI Act	• It has not been assessed as a new risk category, instead it is treated as potential risk drivers for already established risk categories
Third-party / vendor AI models	• Diversifying cloud partnerships to mitigate concentration risk • Assesses open source to retain flexibility and avoid lock-in	• Hybrid cloud setting for the implementation of vendor models wherever possible to mitigate risks	• Currently under discussion
Tiering for AI systems / models	• Classified proportionally by potential impact and complexity, considering function, degree of autonomy, business criticality, and consequences of malfunction or misuse	• Classification of each AI system following the EU AI Act categories	• AI systems are classified following the EU AI Act categories
Validation approach	• Conceptual assessment: ML Guideline compliance, materiality, complexity, intended use • Documented test strategy covering relevant risk scenarios, and ongoing monitoring with clear go-live and model change governance	• Due to the distinction between model and AI system, AI system validation is part of the software development process whereas for models, established validation roles are effective (also, where AI systems might be models)	• Coexistence of validation approach for models and AI system challenge along the software development process

Table 1: Key dimensions and each banks approach

Detailed Case Studies

Insights from an International Commercial Bank – Ratul Ahmed, Commerzbank AG

The real value from AI comes from clear problem framing rather than tools-first adoption. AI in banking will be an orchestrated stack; statistical models, machine learning systems, large generative models, and rule-based logic, deployed where each is most effective. Success depends on intent clarity plus human judgment, with trust, explainability, and control as foundations ensuring that use of AI remains aligned to values, regulation, and societal expectations.

Commerzbank aims to be an AI driven bank, using AI and GenAI to improve decisions, streamline processes, and spur innovation across all divisions. The AI strategy is integrated with IT, Data, and Digital Operational Resilience strategies and organized around three pillars:

- Empowered AI (decentral, cross unit delivery embedded in business workflows)
- AI Foundation (scalable, secure platforms, tools, and data)
- AI Culture (literacy, trust, empowerment for responsible adoption)

Operationalization includes AI Hubs in business units and AI Partners to drive adoption and exchange. Progress is measured via KPIs spanning AI education, scalable services, hub maturity, data readiness, platform adoption, trustworthy AI practices, and value impact. Bank-wide literacy is advanced through training, newsletters, video series, and hackathons. Ethical principles cover transparency, non discrimination, human oversight, data protection, inclusivity, and fairness, reinforced by 3LoD, a machine learning policy and guideline, and an AI inventory integrated in the model risk management tool for traceability across use cases, models, and systems. Alignment with the EU AI Act guides risk based obligations and GPAI requirements. The bank diversifies cloud partnerships to mitigate concentration risk and assesses open source to retain flexibility and avoid lock in.

Nevertheless, implementation challenges remain. EU AI Act definitions are broad, blurring lines between traditional risk/pricing models and AI systems, creating scope ambiguity. Oversight spans multiple bodies, risking plural interpretations and contradictions. There is overlap with product safety, DORA, GDPR, and MaRisk, requiring careful harmonization. Uncertainties persist around filters. Transitional feasibility is strained by delays in CEN/CENELEC standards and interplay with sector standards. The GenAI supply chain raises questions on sovereignty, competitiveness, and compliance as many foundational models originate outside Europe.

Frameworks for AI model validation

Commerzbank is identified by BaFin as O-SII, and therefore variations in regulatory regime across geography will impact Commerzbank's AI implementation. The bank does benefit from a close working relationship between GRM Model Risk Management and the Centre of Competence for AI in GS Data. As a bank, the decision was taken that AI risk is handled as a horizontal driver within existing risk categories rather than a standalone material risk, aligning with supervisors, leveraging current governance, and avoiding fragmentation. This allows proportionate controls across operational, compliance, and model risk domains.

Tiering approach

AI systems and models are classified proportionally by potential impact and complexity, considering function, degree of autonomy, business criticality, and consequences of malfunction or misuse. Higher tiers (e.g., high-stakes decisions or regulatory relevance) trigger more extensive validation, documentation, monitoring, and governance; lower tiers follow streamlined controls under common principles. This ensures efficiency and consistency with the EU AI Act and internal governance standards.

Dynamic adaptation

As regulation and technology evolve, both 1st and 2nd LoD review the classification and governance setup. A consistent AI definition underpins proportional oversight and inventory completeness. Commerzbank applies a dual approach: a broader scope for currently prohibited practices (full AI inventory entry, including regression models, per machine Learning Guideline) and, going forward, a narrower definition aligned with the ECB (e.g., regressions excluded from AI). This balances innovation with control and maintains regulatory conformity. In 2025, Commerzbank published the AI Governance Policy, extending the governance framework with the ML Guideline and Model Risk Governance Policy for Machine Learning, all executed via the 3LoD.

Commerzbank decided early on to establish an AI Governance Mesh and assign roles and responsibilities:

- First Line (GS-Data under the CDAIO): Owns AI strategy; operationalizes 2nd LoD policies through harmonized procedures; advises teams on definitions, eligibility, and restrictions; maintains the ML Guideline; advances literacy; ensures AI inventory data quality and completeness.
- Second Line (GRM-MRM): Owns the AI Governance Policy and MRM framework; sets standards for AI model risk; conducts independent validations; determines final classifications; calibrates assurance; coordinates cross disciplinary controls (e.g., third party risk, data protection); offers early advisory and validates high impact initiatives.
- Third Line (GM Audit): Independently assesses governance effectiveness and control operation, adapting frequency by risk.

Practical validation techniques focus on

- Conceptual assessment: Ensuring ML Guideline requirements are addressed according to risk classification; determining materiality, complexity, resilience, intended use, and potential impact; applying tiering for proportionate oversight.
- Testing: Documented test strategy for model risk topics; results showing sufficient reliability; coverage of relevant risk scenarios.
- Monitoring & follow-up: Clear go live strategy and approval processes; established model change governance; ongoing monitoring.
- Risk assessment: Coverage of all model risk relevant scenarios with transparent assumptions and expert aligned quantification of probability and severity.

If every model matters – how does an MRM team manage this going forward?

During the update of its model risk framework and inventory, Commerzbank addressed GenAI inventory questions by listing system, model, and use case so that models and systems can be classified independently per the ML guideline. The inventory aims to:

- Provide in house transparency on implementation in business context, enabling scalability and avoiding duplication.
- Enable early advisory from 1st and 2nd LoD to product owners.
- Record risk classification for the four damage potentials (Human Oversight, Fairness, Transparency, Reliability) per the ML Guideline.
- Assess regulatory impact to anticipate upcoming European and other jurisdictional obligations and exploring potential language testing services.

The bank is also advancing model lifecycle management via a data science platform to support compliant development, operation, and validation for both central and decentralized units. This promotes continuous evolution, robustness, and scalability, embedding ML lifecycle best practices across the framework.

Insights from a Large Securities Service Provider - Dr. Carsten Wehn & Dr. Cäcilia Zirn, Deka Group

Introduction to the specific setting

Deka's approach to AI governance is shaped by a distinctive institutional context and insight: that AI governance and model risk management governance can, and in many cases should, operate as parallel control loops, each tailored to its respective regulatory objectives, with defined interaction points between them. As a large securities services provider, Deka operates under CRR, KWG, MaRisk on its banking side but not universally across its asset management activities, that operate under asset management specific regulations like among others KaMaRisk, KAGB and Derivatives Regulation. With AI developers distributed across IT and business departments rather than concentrated in dedicated model teams, the bank has adopted a pragmatic governance framework that addresses both the EU AI Act, MaRisk requirements and requirements from the ECB supervision without forcing them into a single structure.

When introducing AI, two factors are particularly important to consider regarding the framework conditions.

The first factor is AI literacy. Traditional models are typically developed by a limited number of experts familiar with the relevant regulations and are used for clearly defined applications. AI, by contrast, is developed by numerous employees across IT and other departments, individuals who might have had little prior exposure to regulatory requirements. The regulations themselves are new to AI, with their specific forms and consequences only gradually becoming apparent. This creates an inherent tension between promoting the adoption of AI and raising awareness of the associated regulatory and internal requirements.

The second is the software-driven nature of AI. AI systems are fundamentally software applications, and therefore subject to existing internal and regulatory requirements for software development, documentation, and the handling of sensitive data. Importantly, the EU AI Act does not base its regulations on AI models, but rather the specific application or use case of AI.

Considering the two factors, extending an already well-established approach for software development is particularly suitable for a financial institution like Deka. Since every form of AI ultimately involves individual data processing or an application, such an approach can be centered around software development and its existing requirements. The following subsections examine to what extent this approach satisfies regulatory requirements (mainly MaRisk and the EU AI Act) and what its advantages and disadvantages are.

MaRisk, the EU AI Act and their implication for model risk management at Deka

MaRisk as systemic regulation for banks (focus models)

The regulatory requirements for MRM vary considerably across jurisdictions, see section 2. International guidelines like SR11-7 were adopted in the ECB-regulated area much later and remain relatively high-level, with the EBA and ECB guidelines specifically targeting individual regulatory areas, such as the normative perspective of Pillar 1. In Germany, the 7th amendment to the MaRisk introduced more comprehensive requirements for the use of models in section AT 4.3.5 applicable to all financial institutions regulated in Germany and supplementing ECB and EBA requirements for ECB-regulated institutions. Notably, there are different rules for asset managers: MaRisk is applicable for Deka on the banking side, but not necessarily across the asset management side where other regulations are relevant.

The inclusion of section AT 4.3.5 in 2024 marks a significant step in regulating the fundamental principles for model governance, while also addressing rapid technological advancements such as machine learning and AI. German supervisory authorities, including BaFin and the Deutsche Bundesbank, have adopted a progressive stance: rather than imposing restrictions on specific algorithms or methods, they focus on explainability of model results; see BaFin (2021) and Deutsche Bundesbank & BaFin (2021) (21), (22).

Under the amended MaRisk, model governance has become increasingly important, requiring institutions to consciously implement and monitor models used in risk management. The extent of these requirements depends on the complexity, purpose, and uncertainties associated with each model. Section AT 4.3.5 expands the scope of MRM requirements to include all models used in processes regulated under MaRisk, going beyond the earlier definition provided in section AT 4.1. For a detailed discussion of the individual requirements of AT 4.3.5, please refer to Wehn (2024) (23).

Under MaRisk, a model is defined as a quantitative method, system, or approach that employs statistical or mathematical theories to process input data into quantitative estimates. This definition encompasses both internally developed and third-party models used in decision-making processes. The guidelines provide methodological flexibility and explicitly acknowledge models with AI characteristics, emphasizing that AI applications and traditional models can represent fundamentally different concepts.

The MaRisk guidelines also specifically mention models that exhibit characteristics of artificial intelligence. This last point further illustrates that applications of artificial intelligence and models are, or at least can be, two fundamentally different topics.

EU AI Act as a regulation to protect consumers and citizens

While banking regulation in general, and regulations on the use and deployment of models in the MaRisk sense in particular, serve to prevent undue losses for an individual bank and ultimately systemic stability, the aim of the EU AI Act is to protect the rights of (EU) citizens.

The fundamental difference, therefore, lies in the dimension of regulation: the EU AI Act always considers an AI system in direct relation to its **intended use**. The definition of artificial intelligence in the EU AI Act, on the other hand, is deliberately broad in order to cover a wide range of AI technologies and applications.

The term ‘Artificial intelligence system’ is defined in the EU AI Act in Article 3(1) and relies on a ‘software developed using one or more of the techniques and approaches listed in Annex I and capable of producing results such as content, predictions, recommendations, or decisions that influence interaction with the environment for a specific set of objectives.’ Thus, the EU AI Act explicitly defines AI systems **as software, not models**, which is a crucial point for implementing appropriate governance.

An AI system may involve the use of a model, but this is not mandatory. It is important to note that, under the EU AI Act, AI systems are not inherently considered models as defined in MaRisk AT 4.3.5. They are the products of the respective machine learning algorithm, but no explicit definition is provided. There are no explicit requirements for these models per se, but rather, as mentioned, for AI applications[1].

The EU AI Act therefore focuses on protecting citizens and considers the specific purpose of AI applications which are categorized into four risk classes (see section 2).

Furthermore, a distinction is made between the provider and deployer of an AI application. According to Article 3(3) of the AI Act, a provider is ”a natural or legal person, public authority, agency or other body which develops or commissions the development of an AI system or AI model with a general purpose and places it on the market or puts the AI system into operation under its own name or trademark, whether for consideration or free of charge”. According to Article 3 (4) of the AI Act, a deployer is “a natural or legal person, public authority, agency or other body which uses an AI system under its own responsibility, unless the AI system is used in the course of a personal and non-professional activity.”

The requirements stipulated by the EU AI Act for each AI application arise from the constellation of roles and risk classes.

[1] The AI Act introduces specific regulations for so-called “General Purpose AI models” (referred to as GPAI). GPAI models, which include large generative AI models and in particular large language models (LLMs) such as GPT-4, can be used for a wide variety of tasks. If a GPAI model is integrated into or forms part of an AI system, that system should be considered a general purpose AI system provided that the integration enables it to serve a wide range of purposes. However, the AI Act only imposes requirements on the providers of GPAI models. In practice, Deka is therefore unlikely to be affected by these additional requirements, as it does not act as a provider of GPAI models.

Implications for appropriate governance

These differing definitions and regulatory objectives have direct implications for governance design for both AI systems and models. The central principle, that an institution not subject to SR11-7 and where banking regulation does not apply universally (such as Deka's asset management activities) can follow, is **that governance for both topics can be established independently**. There is no requirement to manage both from a single source. Rather, each subject can be addressed in its own control loop, focused on its distinct aspects. This separation also accommodates a practical reality: changes to models can be very lengthy depending on their impact (e.g., requiring supervisory approval) and demand significant management attention (up to the board level), whereas innovation cycles for AI systems must be very rapid to remain competitive. Keeping the two governance streams distinct allows each to operate at its own pace, which is elaborated in the next sub-section.

In summary, the following relationships can be derived:

- Models are data processing systems that affect MaRisk processes or need to comply to ECB / EBA requirements.
- Artificial intelligence refers to systems that operate using specific techniques.
- Both are, with the exception of a few edge cases, software applications.

Most importantly, not every AI system should automatically be identified as a model.

Integration of AI into appropriate governance

As shown above, models and AI systems are distinct entities governed by regulations with different objectives. MaRisk (and, where applicable, EBA and ECB guidelines) regulates models to ensure sound MRM. The EU AI Act regulates AI systems to protect citizens and consumers. Where the comprehensive requirements of SR11-7 do not apply, it is possible to establish a dedicated governance framework for models and a dedicated governance framework for AI systems, each meeting the relevant requirements and regulations. This separation ensures proportionate attention to each domain. The design question for financial institutions is: how can AI governance coexist effectively with established MRM requirements?

Despite their differences, governance for models and AI systems share several similarities:

- Inventory: Both models and AI systems must be recorded in an inventory, though the requirements differ. A model inventory must track core model aspects, latest validations results and processing status. An AI inventory must especially document the risk class of an AI system (relative to its use case) under the EU AI Act as well as the role (provider or deployer) the bank has regarding the system.
- Lifecycle: There are different roles within each life cycle.
- MRM assigns clear responsibilities and decision-making authority through five defined roles (24): model owners, model developers, model users, model operators, and model validators. These roles interact across the model lifecycle, as illustrated in Figure 2.

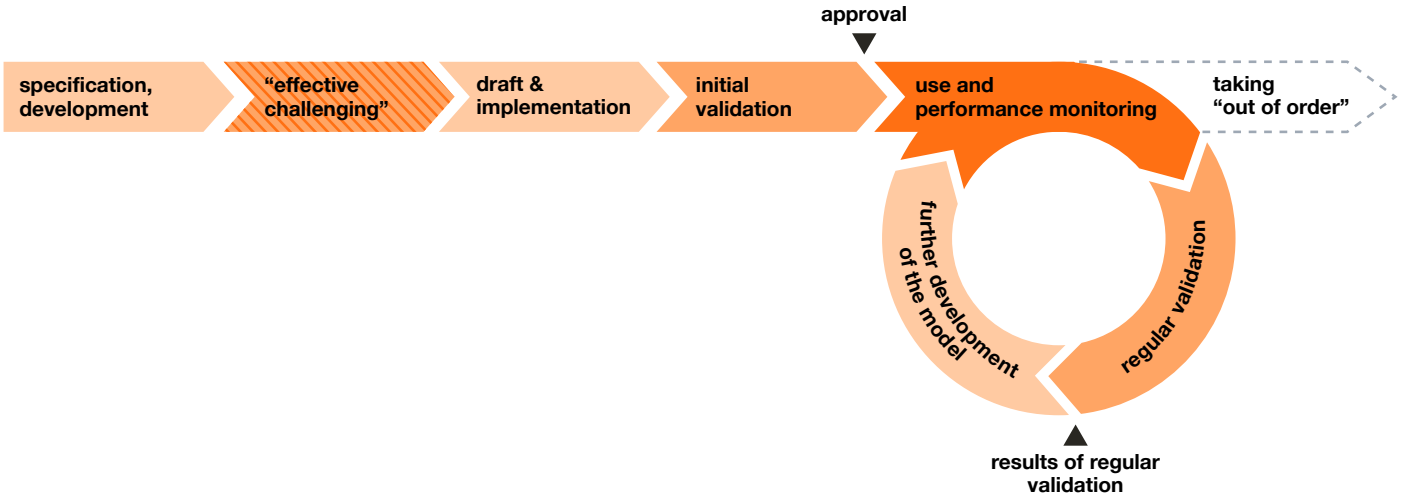


Figure 2: Stylized model lifecycle cf. (24)

Based on its objectives and the lessons learned from the financial crisis, the supervisory authority assigns top-level responsibility for the use of models, particularly in the management of financial institutions. Executive management is expected to be aware of the strengths, weaknesses, and limitations of the models.

Similarly, governance for artificial intelligence systems must consider several requirements. Since AI applications are IT applications, requirements for software development and implementation apply. Specific requirements arising from the respective risk class and provider/deployer role under the EU AI Act, and which go beyond existing requirements, can be incorporated into existing guidelines.

Unlike models, which are typically considered within their specific context and rarely subject to an overarching “model strategy”, AI requires a dedicated strategy. Such a strategy should address the business policy implications and perspectives, as well as discuss strategic use cases. It can also be predefined which risk classes of the EU AI Act AI systems are acceptable, for example, whether high-risk systems are acceptable, excluded by default, or subject to additional requirements.

Since AI applications are typically developed jointly by business departments and IT, roles are distributed across multiple units:

- Business departments design the functions and technical content of the AI application and assess its economic benefits.
- Business and IT jointly ensure compliance with the requirements for AI systems.
- IT handles compliance with technical specifications (development, testing, operation, etc.) and provides infrastructure and technology standards.
- Information security requires particular attention given the associated cyber risks, ensured by cooperation between the respective department and central IT security departments.

Practically, an AI inventory can be set up efficiently based on the existing software inventory, for example, an enterprise architecture system already maintained. Only the additional properties arising from the EU AI Act (risk class, role) need to be included in the inventory.

As shown above, it is possible to establish AI governance alongside MRM governance, tailored to the specific requirements and to the high dynamism of AI. This allows for precise compliance without creating significant redundancies between the two control loops. Nevertheless, an exchange between the two systems is both advisable and, in certain cases, essential because an AI system can also be a model and vice versa.

AI applications differ from traditional software applications due to the associated risks: in addition to the risk classes defined in the AI Act, AI applications can, for example, pose reputational or cyber risks. Two implications follow:

- The risk class definition for AI applications should be adapted accordingly and must be centrally coordinated within existing risk monitoring units. For instance, an application classified as low-risk under the AI Act could still represent high reputational risks and should therefore be treated internally as a higher-risk application requiring stricter standards.
- Special attention should be given to validation. For critical AI applications particularly, model validation expertise should be leveraged for evaluations that go beyond system tests.

AI as an opportunity

In summary, while the challenges of implementing AI systems in medium-sized financial institutions and banks are multifaceted, AI should overall be considered positively. Aligning the governance framework for AI with the guidelines used for implementing software applications is a pragmatic path since potential AI developers may be distributed across the entire process chain rather than concentrated in a single team.

This AI governance can differ from model governance, as long as only the requirements of MaRisk are relevant to models. In this case, models are limited to those procedures whose processes fall within the scope of MaRisk which is generally much narrower than the potential scope of AI systems. For AI systems, the requirements of the EU AI Act apply, necessitating extensions to the existing software governance and additions to the inventory.

Both control loops can then be appropriately integrated, either by comparing the associated risks (e.g., non-financial risks) or by a systemic comparison.

Looking ahead, further challenges remain. The regulation of AI systems will continue to evolve and the pace of technological development remains very rapid. Reflecting both dynamics in a timely manner within governance frameworks is a non-trivial task. The authors therefore recommend pragmatic implementations of the respective requirements, so that future developments can be addressed as flexibly as possible.

The authors thank Fabian Müller (statworx) for inspiring discussions about setting up a practical AI governance.

Insights from a German Development Bank – Hans Elbracht, KfW

The initiation and implementation of AI (-driven) use cases is a rapidly growing field inside KfW, which covers process optimization, supportive information for decision-making and interaction approaches across almost all business areas. As a consequence, providers and users of AI use cases are increasingly distributed across the entire bank (and beyond), demonstrating both the transformative potential and the challenge of consistently managing the (known & unknown) opportunities and risks.

The nature and variety of AI use cases increases not only the number of potential users but also the range of stakeholders and disciplines that are involved. Apart from the use case devising departments, at least IT, data and information security, third-party management, legal and risk (non-financial & financial) should be consulted.

AI use cases can be seen as specific applications of AI technologies (i.e. ML, NLP, GenAI). The EU AI Act defines an AI system as a "machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (25). This definition shares a certain similarity with the (banking regulation) definition of a model 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" (see SR 11-7 or MaRisk).

For an efficient and sustainable introduction of AI use cases the institution should therefore, amongst other topics, identify similarities across already established approaches for systems and models. This is key to finding appropriate compromises in adhering to both consumer and banking regulation. However, KfW's guiding principle is to place specific use cases at the centre of attention and efforts.

Current approach and features of AI and model governance

One of the key challenges in designing and implementing AI use cases is balancing the speed and innovative power of AI with the need for sustainable trustworthiness. Given the broad spectrum of AI use cases, KfW has not yet allocated bank-wide responsibility for managing AI use cases to a specific department or role, reflecting the view that premature centralization could constrain an evolving landscape. To prevent redundancies and inefficiencies, we believe that process integration across software development, procurement and risk management is essential.

Thus, KfW follows a more collaborative approach of coexistence of responsibilities, consulting the different disciplines across the institution especially for managing systems and models. Based on the bank-wide increasing demand to implement AI use cases, KfW's current governance to identify and manage corresponding risks is structured as follows:

- Strategic treatment: The development and usage of AI use cases is part of the IT strategy, as every AI use case is to some degree embedded in IT processes, technologies, and applications. The non-financial risk unit is responsible for ensuring (consumer) regulatory compliance especially with the EU AI Act. The financial risk control unit is responsible for the strategic development of (all) models and the adherence with (banking) regulation, making MRM part of the risk strategy. Furthermore, AI risk has not been assessed as a new risk category, instead AI risks are treated as potential risk drivers for already established risk categories for both financial and non-financial risks. Therefore, established risk management processes also cover AI risk.
- Guidelines: KfW has established internal guidelines for AI usage and model usage. The AI usage guidelines adopt the EU AI act definitions of AI systems and general-purpose AI models, covering general principles for responsible usage, roles, risk classification, third-party applications and AI literacy. Adherence is ensured by a checklist per AI use case, supported by an AI community. The model risk guideline defines models using the MaRisk-driven definition (thereby also covering AI models) and sets out specific requirements regarding model risk, roles, processes (development, validation, approval) and reporting. Importantly, both guidelines (AI usage and model usage) cross-reference each other.
- Inventories: AI use cases are recorded in the application inventory, whereas models are maintained in a separate model inventory. The latter also facilitates key workflows to manage the go-live, usage and deregistration of models. KfW has deliberately chosen not to consolidate both inventories until now, instead running regular comparisons to keep a coherent overview across both domains.

- Roles: Different roles are used and have been implemented to manage AI use cases and models across their lifecycles. For AI use cases these roles are users of the AI applications, technical roles (development, implementation, care), and control responsibilities. For models in general, these roles are users, (model) owners, developers, validators and other established roles, that are in place for a longer time due to the (regulatory driven) maturity of the model management domain. There are natural similarities between the responsibilities of those roles for AI and models. However, the roles for challenging models (development, monitoring, validation) are evolving rapidly because of the pace of technological change, the difficulty of distinguishing clearly between systems and models and the increasing reliance on third-party solutions and their knowledge.
- Classification: KfW has established different assessments to evaluate risk and prioritizes efforts for AI use cases and models. AI systems are classified following the EU AI Act categories (see Section 2). Prioritization of implementation is an outcome of a broader voting across IT use cases (not limited to AI). For prioritization of efforts to maintain (risk) models, KfW uses a tiering approach based on materiality and steering impact of those models for the institution. The risk of using these models is primarily identified by ongoing monitoring and validation activities, where potential permissions are discussed along the approval process.

In summary, KfW observes clusters where dealing with AI systems and models is comparable, making it reasonable to consolidate the existing approaches to merge knowledge and resources.

Consequently, KfW has established two initiatives. An AI accelerator role has been established, a dedicated role tasked to identify and resolve bank-wide obstacles regarding the initiation and implementation of AI use cases while keeping the established 3 Lines of Defence model. Its objectives include transparency over all AI use cases and coordination of comparable ones, overall performance monitoring, legal and regulatory topics and institution-wide upskilling and training. In parallel to this coordination role, an Agile Release Train structured AI factory has been established (SAFe), designed to streamline and scale AI development resources, with the strategic objective of building a centralized AI platform. Together, both initiatives aim to accelerate the implementation and maintenance of AI use cases while improving the overall AI governance.

In parallel, the already existing governance function is encouraged to accompany existing and new AI use cases with particular attention to key characteristics of this new class of systems and models, including traceability, autonomy and adaptability. This also encompasses the identification and mitigation of AI-specific phenomena like model drift, concept drift and hallucination.

Diversity as an opportunity

The challenge of appropriately balancing innovation with oversight is not new, but the wide range of applications and the large number of (upcoming) users differs from previous changes. However, the diversity of both AI use cases (business context and technical solution) and disciplines involved is an opportunity to renew existing roles and optimize collaboration across the institution, a process that extends well beyond the model risk function.

A key driver to improve collaboration is advanced lifecycle management. Current lifecycle periods, characterized by sequential working and documentation needs, risk impeding innovation in AI use cases by design. KfW aims to accelerate fit-for-purpose assessments and the corresponding approval processes, but this clearly starts with a shift in mindset and behaviour across all stakeholders. It also calls for greater flexibility in regulatory expectations as sequential processes and documentation are no longer state of the art in terms of contemporary model management. Joint platforms which enable concurrent development, testing, and documentation are essential.

A second driver is rethinking the image of control units. Given the speed of innovation and characteristics of AI models (self-learning, unknown causality), it is important to renew the roles to have a more proactive or preventive character, which requires different thinking and acting. Guideline-based validation and approval needs to be extended by situational challenge, especially due to the increasing absence of internal solutions (for AI use cases).

A third driver is the strategic consolidation of systems and models. Currently, the focus of model renewal and maintenance including their use cases often falls on individual models. However, many upcoming automation and AI use cases will serve a broader audience and are designed to deliver efficiency gains at scale. Bank-wide transparency over upcoming use cases and comparable applications is therefore essential to manage the (AI) system and model landscape appropriately.

Finally, the diversity of AI use cases presents an opportunity to bring business and control units closer together across all divisions and that should be seen as a chance when running future AI use cases.

04

Proportional, Practical, Principled: Considerations for an effective regulatory AI Framework for Banks

Proportional, Practical, Principled: Considerations for an effective regulatory AI Framework for Banks

This whitepaper provides key insights into the implementation of model risk management requirements and emerging obligations under the EU AI Act within large German banks.

Our comparison highlights that, given the unique characteristics of each institution, there is currently no universal blueprint for compliance or risk management strategy. Instead, the approaches adopted differ significantly, reflecting both the specific internal conditions of each bank and the rapid pace of innovation inherent to artificial intelligence. These variances manifest in organizational structures, governance models, and the integration of AI systems into existing risk frameworks. Institutions are adapting their model risk management strategies not only to satisfy regulatory demands, but also to ensure agility and responsiveness in an environment where technological advances are continuous. For banks and financial institutions seeking inspiration and practical solutions in this evolving field, our aim is to provide a selection of key considerations and potential approaches. By sharing current practices and highlighting the challenges faced by industry peers, we hope to support others in developing robust, future-oriented strategies for the governance and oversight of AI and model-related risks.

Depending on their view, banks have chosen to implement or are planning to implement fully integrated management of AI models (including model governance and development platforms) or have adopted rather pragmatic approaches, recognizing synergies between MRM and AI governance and management where possible and sensible but keeping them separate where more practical. However, all banks agree that (model) governance should be proportional to the inherent risk, regardless of whether AI is employed or not and so should be the regulatory practice as well.

A key result from comparing views and statuses of different banks in the previous sections is that depending on the level of exposure towards international regulation and the level of aspiration towards AI, banks are advocating for more harmonized regulation for AI - across jurisdictions but also with MRM requirements.

The EU follows a hybrid approach with expected sectoral guidelines for the financial sector. Some parts of the EU AI Act have been identified as redundant, given that they are already fully covered by existing banking regulation. However, other parts of the EU AI Act will require specific interpretation alongside existing regulation or represent new regulation to the financial sector.

Regardless of the approach taken, the rapid pace of AI innovation is fundamentally incompatible with rigid, highly detailed rules and regulations and instead calls for a more flexible, principles-based framework. For instance, ChatGPT was launched only about three years ago, and today AI agents and agentic systems are at the forefront of AI development, illustrating just how exponential this progress has become. Based on the findings of this paper, such principles should, at a minimum, provide guidance on the following areas:

- **According to which criteria should AI models, AI systems, and use cases be differentiated?** The classification as a model leads to the application of FS-specific MRM and validation requirements. This should also consider proportionality, not necessarily in the sense of complexity and size of the institution, but rather of the specific use case.
- **Should AI be categorized either as a standalone (sub-) risk type or as an overarching risk driver?** Categorization as a standalone (sub-) risk type results in additional pressure on standard setters and 2nd line oversight, reaffirming the traditional 3LoD setup. Categorization as an overarching risk driver allows for pragmatism and can be used to create autonomy through the organization and flex the 3LoD. While the latter will allow for adoption faster than the former, risk acceptance will generally have to be higher.
- **How should AI models by third parties be considered?** This issue underscores the need for clear, sector-specific guidelines on the use of third-party general-purpose AI (GPAI) models in financial services. Without them, institutions face challenges in managing transparency gaps, especially around vendor practices on data, models, and cybersecurity, while also contending with over-reliance on key providers and insufficient contingency planning. Therefore, the EU AI Act introduced distinct obligations for providers and deployers, but the lines between these roles can blur: deployers who significantly modify or integrate GPAI models into their systems may themselves become providers. This dual role brings heightened regulatory responsibilities, including transparency, documentation, and risk mitigation duties.
- **How can an effective risk-based assessment of AI risk be established and how can a corresponding risk appetite in the sense of a use case coverage be determined?** Due to the plethora of use cases of an AI model, not all uses cases can be thoroughly considered in the validation in due time.
- **What AI-specific validation dimensions are needed?** Dimensions such as fairness and explainability are of particular importance in the assessment of AI models, yet their evaluation is not homogenous across model types. Novel approaches like GenAI and agentic AI warrant a battery of innovative validation approaches. For instance, GenAI models could be divided into use-case based arch etypes with specific validation procedures for each category.

This set of aspects should be seen as a starting point for a dialogue between regulators and the financial services industry, rather than a comprehensive list.

05

References

References

1 **European Parliament**. EU AI Act: first regulation on artificial intelligence. [Online] 08 June 2023. https://artificialintelligenceact.eu/.

2 **White & Case**. AI Watch: Global regulatory tracker - European Union. [Online] 21 July 2025. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-european-union.

3 **European Commission**. European AI Office. [Online] https://digital-strategy.ec.europa.eu/en/policies/ai-office.

4 **European Central Bank**. ECB guide to internal models. [Online] 2028 July 2025. https://www.bankingsupervision.europa.eu/press/pr/date/2025/html/ssm.pr250728~2b36305822.en.html.

5 **Polish Financial Supervision Authority**. Recommendation W on model risk management in banks. [Online] 2015 July 2015. https://www.knf.gov.pl/knf/pl/komponenty/img/knf_161644_Recommendation%20W_english_48340.pdf.

6 **Bundesanstalt für Finanzdienstleistungsaufsicht**. Mindestanforderungen an das Risikomanagement - MaRisk. [Online] 29 May 2024. https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_06_2024_MaRisk_pdf_BA.html.

7 **Christopher J. Waller**. Innovation at the Speed of AI. Board of Governors of the Federal Reserve System. [Online] 15 October 2025. https://www.federalreserve.gov/newsevents/speech/waller20251015a.htm.

8 **Janet Yellen**. CFPB Comment on Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector. Consumer Financial Protection Bureau. [Online] 12 Aug 2024. https://www.consumerfinance.gov/about-us/newsroom/cfpb-comment-on-request-for-information-on-uses-opportunities-and-risks-of-artificial-intelligence-in-the-financial-services-sector/.

9 **Michelle w. Bowman**. Artificial Intelligence in the Financial System. Board of Governors of the Federal Reserve System. [Online] 22 November 2025. https://www.federalreserve.gov/newsevents/speech/bowman20241122a.htm.

10 **Rodney E. Hood**. AI in Financial Services. Office of the Comptroller of the Currency. [Online] 29 April 2025. https://www.occ.treas.gov/news-issuances/speeches/2025/pub-speech-2025-38.pdf.

11 **Board of Governors of the Federal Reserve System**. SR 11-7: Guidance on Model Risk Management. [Online] 04 April 2011. https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm.

12 **Board of Governors of the Federal Reserve System**. SR 26-2: Revised Guidance on Model Risk Management. [Online] 17 April 2026. https://www.federalreserve.gov/supervisionreg/srletters/SR2602.htm.

13 **Department for Science, Innovation and Technology, Office for Artificial Intelligence, Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy**. National AI Strategy. [Online] 22 September 2021. https://www.gov.uk/government/publications/national-ai-strategy.

14 **Department for Science, Innovation and Technology**. AI regulation: a pro-innovation approach – policy proposals. Uk Government. [Online] 29 March 2023. https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals.

15 **Bank Of England**. SS1/23 – Model risk management principles for banks. [Online] 17 May 2023. https://www.bankofengland.co.uk/prudential-regulation/publication/2023/may/model-risk-management-principles-for-banks-ss.

16 **White & Case**. AI Watch: Global regulatory tracker - United Kingdom. [Online] 25 November 2025. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-kingdom.

17 **Financial Services Agency of Japan**. Principles for Model Risk Management. [Online] 12 November 2021. https://www.fsa.go.jp/common/law/ginkou/pdf_03.pdf.

18 **Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry**. AI Guidelines for Business. [Online] 4 April 2025. https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_14.pdf.

19 **Cabinet Office**. Act on Promotion of Research and Development, and Utilization of Artificial Intelligence-related Technology Now. [Online] 28 May 2025. https://www.cao.go.jp/houan/pdf/217/217anbun_2.pdf.

20 **Ministry of Science and ICT**. A New Chapter in the Age of AI: Basic Act on AI Passed at the National Assembly‘s Plenary Session. [Online] 2024 December 2026. https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=1071&searchOpt=ALL&searchTxt=.

21 **Bundesanstalt für Finanzdienstleistungsaufsicht**. Big Data und künstliche Intelligenz: Prinzipien für den Einsatz von Algorithmen in Entscheidungsprozessen. [Online] 15 June 2021. https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_Prinzipienpapier_BDAI_en.html.

22 **Deutsche Bundesbank, Bundesanstalt für Finanzdienstleistungsaufsicht**. Machine learning in risk models - Characteristics and supervisory priorities. [Online] 21 July 2021. https://www.bundesbank.de/resource/blob/793670/61532e24c3298d8b24d4d15a34f503a8/mL/2021-07-15-ml-konsultationspapier-data.pdf.

23 **Wehn, Carsten S.** AT 4.3.5. T. Krebs and P. Stegner. Bearbeitungs- und Prüfungsleitfaden: Neue MaRIsk, 6. Auflage. Heidelberg : Verlag Finanzkolloquium, 2024.

24 **Hoffmann, Jan-Philipp.** Übergreifendes Modellrisikomanagement. P. Quell, C.S. Wehn and M.R.W. Martin. Modellrisiko und Validierung von Risikomodellen. Köln : Bank-Verlag, 2016.

25 **European Commission.** Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 20241689 (AI Act) (English). [Online] 06 February 2025. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application.

Authors

Ratul Ahmed
Group Head of Model Risk Management
and Validation at Commerzbank
ratul.ahmed@commerzbank.com

Dr. Carsten Wehn
Head of Model Risk Management
and Validation at Deka
carsten.wehn@deka.de

Dr. Cäcilia Zirn
AI Strategy Lead at Deka
caecilia.zirn@deka.de

Hans Christian Elbracht
Head of Model Risk Management at KfW
hans_christian.elbracht@kfw.de

Dr. Philipp Schröder
Partner at PwC Germany
p.schroeder@pwc.com

Dr. Janis Müller
Senior Manager at PwC Germany
janis.mueller@pwc.com