Jedes Modell zählt –

Wie der Einsatz von KI die Rolle des Modellrisikomanagements transfomiert

Inhaltsverzeichnis

01

Einleitung

Einleitung

Künstliche Intelligenz (KI) verändert das europäische Bankwesen rasant. Von der Kreditbearbeitung und Risikobewertung bis hin zur Kundeninteraktion und Prozessautomatisierung – KI-Modelle und -Systeme halten Einzug in nahezu alle Geschäftsbereiche. Diese Transformation vollzieht sich jedoch vor einem regulatorischen Hintergrund, der sowohl ehrgeizig als auch fragmentiert ist. Der EU AI Act, das weltweit erste umfassende KI-Gesetz, führt einen risikobasierten Klassifizierungsrahmen ein, der sowohl für Entwickler als auch für Anwender gilt, während sich die bestehenden Anforderungen an das Modellrisikomanagement (MRM) gemäß MaRisk, dem Leitfaden der EZB für interne Modelle, und die nationalen aufsichtsrechtlichen Erwartungen parallel dazu weiterentwickeln. Außerhalb Europas stützen sich die Vereinigten Staaten und das Vereinigte Königreich eher auf bestehende Leitlinien und eine prinzipienbasierte Aufsicht als auf präskriptive KI-spezifische Gesetzgebung, und die Rechtsordnungen im asiatisch-pazifischen Raum beschreiten ihre eigenen, vielfältigen Wege. Für international tätige Banken, aber auch für Banken, die sich ausschließlich auf Europa konzentrieren, schafft dieses Flickwerk aus Regulierungssystemen eine Compliance-Landschaft von beträchtlicher Komplexität, in der die Definitionen dessen, was ein „KI-System“, ein „KI-Modell“ und ein „Modell“ im Sinne von KI und MRM ausmacht, nicht immer übereinstimmen.

In diesem Beitrag wird untersucht, wie Banken in der Praxis mit dieser Komplexität umgehen. Anhand detaillierter Fallstudien zu drei führenden deutschen Finanzinstituten – der Commerzbank, der Deka und der KfW – wird ein Spektrum an Ansätzen für die KI-Governance und das Modellrisikomanagement aufgezeigt. Diese Institute unterscheiden sich hinsichtlich ihrer Größe, ihres Geschäftsmodells, ihrer systemischen Bedeutung und ihrer regulatorischen Anforderungen, und ihre Strategien spiegeln diese Vielfalt wider. Einige haben vollständig integrierte Governance-Rahmenwerke eingeführt, die KI-Modelle unter einem einheitlichen MRM-Dach zusammenfassen.

Andere haben pragmatischere Architekturen gewählt, wobei sie Synergien zwischen KI-Governance und MRM dort anerkennen, wo sie bestehen, die beiden Bereiche jedoch getrennt halten, wenn praktische Erwägungen dies erfordern. Allen gemeinsam ist jedoch eine Reihe gemeinsamer Herausforderungen: die rasante Zunahme von KI-Anwendungsfällen über traditionelle Modellteams hinaus, die gestiegenen Anforderungen an Erklärbarkeit und Fairness, die Undurchsichtigkeit von KI-Modellen von Drittanbietern und Allzweckmodellen, die Geschwindigkeit, mit der sich Techniken wie generative KI und agentische Systeme weiterentwickeln, sowie das grundlegende Spannungsfeld zwischen dem Tempo der Innovation und dem Tempo der Regulierung. Historisch gesehen wurde die Risikofunktion der zweiten Linie, insbesondere das MRM, als Engpass im Modelllebenszyklus angesehen. Vor dem Hintergrund der raschen und disruptiven Einführung von KI birgt diese Sichtweise jedoch die Gefahr, dass nicht nur der Fortschritt verlangsamt wird, sondern auch Chancen für eine strategische Abstimmung zwischen Kontrollfunktionen und dem Geschäft verpasst werden. Die beteiligten Banken zeigen, dass sich das MRM von einem reaktiven Gatekeeper zu einem proaktiven Wegbereiter für verantwortungsvolle Innovation entwickeln muss, der Beratung, Kritik und Anleitung in der Frühphase bietet, um den Einsatz von KI zu beschleunigen statt zu behindern.

Aus dem Vergleich dieser Institutionen ergibt sich eine klare und übereinstimmende Botschaft an die Regulierungsbehörden. Die Banken fordern eine stärkere Harmonisierung, nicht nur zwischen den verschiedenen Rechtsordnungen, sondern auch zwischen KI-spezifischen Vorschriften und den bestehenden Anforderungen an das Modellrisikomanagement. Zwei Wege stehen zur Debatte: Entweder erhält die Finanzdienstleistungsbranche spezifische aufsichtsrechtliche Leitlinien dazu, wie der EU AI Act neben den bestehenden Modell-Governance-Verpflichtungen auszulegen und umzusetzen ist, oder Finanzdienstleistungen werden vollständig aus dem Anwendungsbereich der Modell-Governance des EU AI Act ausgenommen, was die Möglichkeit für einen einzigen, umfassenden MRM-Rahmen auf EU-Ebene schafft, der sowohl KI- als auch Nicht-KI-Modelle abdeckt. Unabhängig davon, welcher Weg sich durchsetzt, sind sich die beteiligten Institutionen einig, dass starre, hochdetaillierte Vorschriften mit dem exponentiellen technologischen Wandel nicht Schritt halten können. Stattdessen ist ein flexibler, prinzipienbasierter Rahmen erforderlich, der Klarheit hinsichtlich der KI-Risikoklassifizierung, der Validationsdimensionen für neuartige Modelltypen, der Behandlung von KI-Modellen von Drittanbietern und der Rolle der Verhältnismäßigkeit in der Governance schafft, während er der Branche und ihren Aufsichtsbehörden Spielraum lässt, sich an die fortschreitende technologische Entwicklung anzupassen.

Dieser Beitrag soll genau zu diesem Dialog beitragen. Er gibt einen Überblick über das regulatorische Umfeld, beleuchtet die praktischen Realitäten der KI-Governance in europäischen Banken und fasst eine Reihe offener Fragen zusammen, die als Ausgangspunkt für einen strukturierten Dialog zwischen der Finanzdienstleistungsbranche und ihren Regulierungsbehörden dienen sollen – ein Dialog, der dringend erforderlich ist, wenn Europa vermeiden will, bei der Einführung von KI und letztlich auch bei der globalen Wettbewerbsfähigkeit ins Hintertreffen zu geraten.

Der Beitrag ist wie folgt aufgebaut: In Abschnitt 2 wird ein Überblick über die globale Regulierungslandschaft für KI im Bankwesen gegeben, wobei die Ansätze der EU, der USA, des Vereinigten Königreichs und ausgewählter Länder im asiatisch-pazifischen Raum gegenübergestellt werden. In Abschnitt 3 werden detaillierte Fallstudien der drei beteiligten Banken vorgestellt, in denen untersucht wird, wie jede einzelne ihre Governance- und Modellrisikomanagement-Rahmenwerke an den Einsatz von KI angepasst hat. Abschnitt 4 fasst diese Perspektiven in einem institutionsübergreifenden Vergleich zusammen, identifiziert zentrale offene Fragen, mit denen die Branche konfrontiert ist, und schließt mit einem Aufruf zum Dialog zwischen der Branche und den Regulierungsbehörden.

02

Regulatorisches Umfeld für KI im Bankwesen

Regulatorisches Umfeld für KI im Bankwesen

Die Regulierung im Bereich der KI entwickelt sich rasant weiter, wobei bedeutende Regionen unterschiedliche Ansätze verfolgen, die sich auf Compliance-Strategien und den Geschäftsbetrieb auswirken. Das Verständnis dieser Rahmenbedingungen ist für multinationale Unternehmen, die verantwortungsbewusst innovativ sein und ihren Marktzugang sichern wollen, von entscheidender Bedeutung. Bei der Entwicklung und dem Einsatz von KI-Modellen müssen sich europäische Banken daher in einem komplexen und sich dynamisch wandelnden regulatorischen Umfeld zurechtfinden. Einerseits sind sie verpflichtet, KI-spezifische Vorschriften einzuhalten, andererseits müssen sie aber auch bestehende Anforderungen und aufsichtsrechtliche Erwartungen an Finanzinstitute wie MRM erfüllen. Diese Komplexität nimmt für international tätige Banken noch weiter zu, da sie sich zudem mit unterschiedlichen Regulierungssystemen in beiden Bereichen in verschiedenen Rechtsordnungen auseinandersetzen müssen.

Die weltweite Regulierungslandschaft im Bereich der KI wird weitgehend von zwei unterschiedlichen Ansätzen geprägt:

1. Priorisierung der sicheren und verantwortungsvollen Nutzung von KI,
2. Förderung von Innovationen und Wettbewerbsfähigkeit im Bereich der KI.

Zur ersten Kategorie gehören Länder, die bereits umfassende KI-Vorschriften haben oder kurz vor deren Einführung stehen, wie beispielsweise die EU. Diese Länder lehnen KI-Innovationen nicht ab, wollen aber das Risiko einer schädlichen Nutzung von KI verringern. Zur zweiten Kategorie gehören Länder, die KI als Wettbewerbsvorteil betrachten und daher bei der Einführung von KI-Vorschriften zurückhaltend sind, um eine Verlangsamung der KI-Entwicklung zu vermeiden, wie beispielsweise das Vereinigte Königreich oder die USA. Das bedeutet nicht, dass diese Länder keine Bedenken hinsichtlich einer schädlichen Nutzung von KI haben, sondern sie ziehen es vor, die Fortschritte im KI-Bereich genau zu beobachten und nur dann mit spezifischen KI-Vorschriften einzugreifen, wenn dies als notwendig erachtet wird.

Regulatorisches Umfeld in der Europäischen Union

Der EU AI Act, der am 1. August 2024 in Kraft getreten ist, ist das weltweit erste umfassende Gesetz zur Regulierung künstlicher Intelligenz. Er schafft einen risikobasierten Rahmen für die Bewertung von KI-Systemen, die in der gesamten EU-Wirtschaft zum Einsatz kommen, und richtet sich sowohl an Entwickler (Urheber oder wesentliche Modifikatoren von KI) als auch an Anwender (Nutzer von KI in der Praxis). Finanzinstitute könnten als bedeutende Nutzer von KI beide Rollen einnehmen.

Der EU AI Act stuft KI-Systeme nach ihrem Risiko ein (1), (2):

- Unzulässig: Verbotene Systeme, die die Sicherheit, den Lebensunterhalt oder die Rechte gefährden.
- Hoch: Systeme mit erheblichen Auswirkungen, die einer strengen Überwachung und Eignungsbewertung in Bezug auf Datenqualität, menschliche Kontrolle, Transparenz, Dokumentation, Genauigkeit, Robustheit, Cybersicherheit und Qualitätsmanagement unterliegen (1), (2).
- Begrenzt: Es muss Transparenz herrschen, damit die Nutzer wissen, dass sie mit einer KI interagieren.
- Minimal: Vernachlässigbares Risiko; wenige Anforderungen.

Im Bereich der Finanzdienstleistungen werden in Anhang III KI-Anwendungen, die bei der Bonitätsbewertung, der Risikobewertung und der Preisgestaltung von Versicherungen für Privatpersonen zum Einsatz kommen, als Hochrisiko eingestuft, was zusätzliche Melde- und Überprüfungsanforderungen nach sich zieht (1). Die Aufsicht wird von den nationalen Finanzaufsichtsbehörden und den Europäischen Aufsichtsbehörden (EBA, ESMA, EIOPA) wahrgenommen, unterstützt durch das Europäische KI-Büro (1), (2), (3).

Der EU AI Act regelt KI-Systeme, jedoch nicht direkt KI-Modelle, mit Ausnahme von Modellen für allgemeine KI (GPAI), die definiert sind und besonderen Anforderungen unterliegen (1). In Erwägungsgrund 97 wird klargestellt, dass KI-Modelle wesentliche Bestandteile von KI-Systemen sind, jedoch keine eigenständigen Systeme darstellen (1).

Die Regulierung des Modellrisikomanagements (MRM) für Finanzinstitute in der Europäischen Union ist uneinheitlich. Der Leitfaden der EZB zu internen Modellen (EGIM) ist eine europäische Regelung, die übergreifende Leitlinien für das Modellrisikomanagement bereitstellt, beispielsweise in Bezug auf Risiken des maschinellen Lernens in internen Modellen, wobei der Schwerpunkt auf Erklärbarkeit, Governance, Qualifikationsanforderungen, Validierung und einer robusten IT-/Dateninfrastruktur liegt (4). Der EGIM beschränkt sich jedoch auf Säule-1-Modelle, und es gibt keine einheitliche, EU-weit verbindliche MRM-Regulierung. Infolgedessen stützt sich die Regulierungslandschaft stark auf nationale Rahmenwerke, um Lücken zu schließen, wobei beispielsweise die polnische „Empfehlung W“ Standards für das Modellrisikomanagement von Banken festlegt, jedoch keine expliziten Abschnitte zur KI enthält (5), und die überarbeitete MaRisk (2024) in Deutschland Anforderungen an die Erklärbarkeit von Modellen und die Datenqualität einführt, insbesondere für innovative KI-Modelle, die für das Risikomanagement eingesetzt werden (6).

Regulatorisches Umfeld in den Vereinigten Staaten und im Vereinigten Königreich

Zum Ende des Jahres 2025 verfügen weder die USA noch das Vereinigte Königreich über umfassende, verbindliche und sektorübergreifende Rechtsvorschriften zur künstlichen Intelligenz. Beide Länder stützen sich hauptsächlich auf bestehende Gesetze und sektorale Aufsichtsbehörden und verfügen über einen prinzipienbasierten MRM-Regulierungsrahmen.

In den USA legen die Aufsichtsbehörden des Bundes Wert auf Innovation und steuern Risiken gleichzeitig im Rahmen bestehender Gesetze. Behörden wie das Consumer Financial Protection Bureau wenden seit langem bestehende Gesetze wie den Equal Credit Opportunity Act an, um Fairness zu gewährleisten und Diskriminierung bei KI-gestützten Kreditentscheidungen zu verhindern. Beamte wie der Comptroller of the Currency befürworten eine technologieneutrale, risikobasierte Aufsicht, die bereits in die Bankenaufsicht integriert ist (7), (8), (9), (10). Bis vor kurzem wurde das Modellrisikomanagement für KI im Rahmen etablierter Vorschriften wie SR 11-7 gehandhabt, die eine robuste Modellentwicklung, -implementierung und -validierung vorschreiben, ohne den Banken zusätzliche regulatorische Belastungen aufzuerlegen (11), (7), (8), (9), (10). In den „Revised Guidance on Model Risk Management“ (SR 26-2) werden jedoch in Fußnote 3 der Leitlinien agentische und generative KI-Systeme ausdrücklich von den neu veröffentlichten MRM-Anforderungen ausgenommen. Dennoch fallen nicht-agentische und nicht-generative KI-Modelle weiterhin in den Anwendungsbereich von SR 26-2, und von den Banken wird weiterhin erwartet, dass sie ihre umfassenderen Rahmenwerke für Risikomanagement und Governance auf alle Systeme, Prozesse oder Tools anwenden, die nicht unter die aktualisierten MRM-Leitlinien fallen (12).

Ebenso verfolgt das Vereinigte Königreich einen prinzipienbasierten Ansatz in Bezug auf KI. Die nationale KI-Strategie und das Weißbuch von 2023 legen fünf Leitprinzipien fest, nämlich Sicherheit, Transparenz, Fairness, Rechenschaftspflicht und Überprüfbarkeit, deren Umsetzung von sektoralen Regulierungsbehörden wie der Financial Conduct Authority (FCA) und der Bank of England (BoE) gewährleistet wird (13), (14). Die Aufsichtsrichtlinie SS1/23 definiert allgemeine Standards für das Modellrisikomanagement, die die Interpretierbarkeit und Transparenz von KI-Modellen umfassen (15). Die Aufsicht erfolgt im Rahmen bestehender gesetzlicher Befugnisse, die es den Regulierungsbehörden ermöglichen, bei Bedarf Anforderungen in Bezug auf Verbraucherschutz und operative Widerstandsfähigkeit durchzusetzen (14), (16).

Weitere regulatorische Initiativen

Die Länder des asiatisch-pazifischen Raumes (APAC) verfolgen unterschiedliche Regulierungsansätze im Bereich der KI, wobei sich einige stärker am EU-Modell orientieren, während andere den Rahmenwerken der USA und Großbritanniens ähneln. Japan beispielsweise nutzt einen prinzipienbasierten, innovationsfördernden KI-Rahmen, der durch Grundsätze für das Modellrisikomanagement ergänzt wird (17). Japans KI-Förderungsgesetz und die KI-Geschäftsrichtlinien betonen Fairness, Sicherheit, Menschzentriertheit und Innovation, während die Grundsätze der FSA KI als allgemeine Modelle behandeln, die einer strengen Governance und Validierung unterliegen (18), (19). Demgegenüber ist das südkoreanische KI-Grundgesetz ein übergreifendes, risikobasiertes Gesetz, das ethische und innovative KI fördert und vorschreibt, dass Systeme mit hoher Auswirkung einer Bewertung, einem Risikomanagement, Erklärbarkeit und menschlicher Aufsicht unterzogen werden müssen, jedoch keine Verbote im Stil der EU vorschreibt und relativ niedrige Bußgelder vorsieht (20).

Globale Regulierungslandschaft im Bereich der künstlichen Intelligenz

Risikoorientiert

Innovationsorientiert

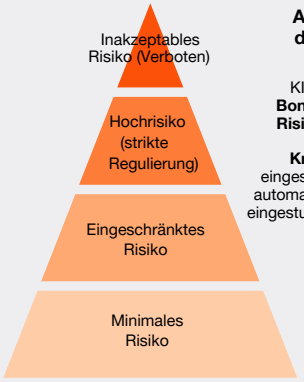
EU: Risikoorientierter Ansatz

KI-Regulierung

- **Sektorübergreifender, risikobasierter** Rechtsrahmen für künstliche Intelligenz
- Fokus auf einen sicheren und verantwortungsvollen Einsatz von KI
- **Verbietet** Modelle, die als **inakzeptables Risiko** eingestuft werden

Modellrisikomanagement

- Es gibt keine unionsweite Regelung
- Leitlinien auf EU-Ebene **(EGIM der EZB)** und nationale Rahmenwerke (z. B. die **MaRisk** in Deutschland) befassen sich ausdrücklich mit dem **Einsatz von KI/ML in quantitativen Risikomodellen**
- Ein besonderer Schwerpunkt liegt auf der **Erklärbarkeit,** auch wenn die verbindlichen Anforderungen in den einzelnen Mitgliedstaaten nach wie vor uneinheitlich sind



Auswirkungen auf den Finanzdienstleistungssektor:

KI-Systeme, die für die **Bonitätsbewertung** und **Risikobewertung in der Lebens- und Krankenversicherung** eingesetzt werden, werden automatisch als **Hochrisiko** eingestuft und erfordern eine **strenge Aufsicht.**

USA: Innovation durch Deregulierung

KI-Regulierung

- **Keine bundesweiten Gesetze zur KI**; die Regulierung beschränkt sich auf Gesetze auf Bundesstaatenebene (z. B. der Colorado AI Act)
- KI wird **durch bestehende Behörden** statt durch eine eigene Regulierungsbehörde geregelt
- Der Schwerpunkt liegt auf Innovation und dem Verständnis von Anwendungsfällen der KI statt auf einer präskriptiven Regulierung

Modellrisikomanagement (SR 26-2)

- **SR 26-2:** Von der Fed und der OCC herausgegebene aufsichtsrechtliche Leitlinien zu **MRM**, in denen Erwartungen hinsichtlich der Modellentwicklung, -validierung und -steuerung festgelegt werden
- **Nicht-agentische und nicht-generative KI-Modelle** unterliegen diesem Rahmenwerk

Ausschließlich spezifische KI-Regulierung — **Konsolidierte Regulierung von KI und MRM** — **Ausschließlich spezifische MRM-Regulierung**

Risikobasierte Standards ohne vollständige Verbote

KI-Regulierung

- Der AI Basic Act legt **risikobasierte Standards** fest; risikoreiche KI erfordert Beurteilungen und menschliche Aufsicht, aber **keine vollständigen Verbote**

Modellrisikomanagement

- Es gibt **weder einen einheitlichen MRM-Rahmen** noch eine klare Definition von KI-Modellen; aktualisierte FSC-Leitlinien werden erwartet

Ausgewogener Ansatz

KI-Regulierung

- Das Gesetz zur Förderung der künstlichen Intelligenz legt **allgemeine Grundsätze** fest; es dient in erster Linie als Rahmen für künftige Rechtsvorschriften

Modellrisikomanagement

- Die MRM-Grundsätze der FSA legen den Schwerpunkt auf eine Governance nach dem **Three-Lines-of-Defense-Ansatz**
- Es wird erwartet, dass KI-/ML-Modelle unter den **bestehenden Rahmen** „Principles for Model Risk Management“ fallen

Branchenspezifischer Ansatz

KI-Regulierung

- **Sektoraler Governance-Ansatz** mit einem freiwilligen Rahmenwerk für KI-Governance (2019, aktualisiert 2024), das Transparenz, Fairness und Rechenschaftspflicht umfasst

Modellrisikomanagement

- Es gibt **kein einheitliches MRM-Rahmenwerk**; die KI-spezifischen MRM-Leitlinien (2024) und die MAS-Leitlinien (2025) führen die ersten formellen Leitlinien für den Einsatz von KI-Modellen im Finanzdienstleistungssektor ein

Großbritannien: Flexibler, prinzipienbasierter Ansatz

KI-Regulierung

- **Keine übergreifende KI-Gesetzgebung**; prinzipienbasierter Ansatz auf der Grundlage bestehender sektorspezifischer Vorschriften (White Paper, 2023)
- **Ergebnisorientierung** statt vorschreibende Regeln

Modellrisikomanagement

- **SS1/23:** PRA-Leitlinien zur Festlegung von **fünf zentralen MRM-Grundsätzen** (Identifizierung, Governance, Entwicklung, Validierung, Risikominderungsmaßnahmen) für Banken, die interne Modelle verwenden
- SS1/23 befasst sich mit **wesentlichen Risikofaktoren** im Zusammenhang mit KI-Modellen, darunter **Interpretierbarkeit, Erklärbarkeit und potenzieller Bias**

Abbildung 1: Globale Regulierungslandschaft im Bereich der künstlichen Intelligenz

03

Modellrisiko-management für KI-Modelle

Modellrisiko-management für KI-Modelle

Künstliche Intelligenz (ML, generative KI und agentische KI) wird immer fester in die Betriebsabläufe europäischer Banken eingebunden und verändert Prozesse, Entscheidungsfindung und Kundeninteraktion grundlegend. Angesichts der zunehmenden Verbreitung von KI stehen Finanzinstitute vor einer doppelten Herausforderung: Sie müssen KI-Systeme sicher und verantwortungsbewusst implementieren und sich gleichzeitig an ein fragmentiertes und sich rasch wandelndes regulatorisches Umfeld anpassen. In diesem Abschnitt liegt der Fokus auf praktischen Erkenntnissen von drei führenden deutschen Banken – Commerzbank, Deka und KfW – darüber, wie MRM-Frameworks für den großflächigen Einsatz von KI angepasst werden können.

Über alle Geschäftsmodelle hinweg zeichnet sich ein vorherrschendes Thema ab: KI ist nicht einfach nur eine weitere Modellart, sondern eine Klasse von Systemen mit einzigartigen operativen, ethischen und governancebezogenen Auswirkungen. Doch uneinheitliche Definitionen in den Aufsichtsstandards führen zu Unklarheiten darüber, wann KI-Systeme unter die klassische Modell-Governance fallen und wann sie neue Aufsichtsmechanismen erfordern. Diese definitorische Unsicherheit wird durch sich überschneidende regulatorische Anforderungen und divergierende internationale Ansätze noch verstärkt, was Banken dazu zwingt, sich in einem komplexen Compliance-Umfeld zurechtzufinden. Vor diesem Hintergrund vergrößern Lücken im KI-Wissen und eine dezentrale Entwicklung das Nutzungsrisiko rasch über die traditionellen Modellnutzer hinaus, während das Tempo der KI-Innovation traditionelle MRM-Prozesse zunehmend überholt.

Aus Interviews mit den drei beteiligten Banken geht hervor, dass sie trotz unterschiedlicher Ausgangslagen mit einer Reihe gleichbleibender praktischer Herausforderungen konfrontiert sind:

- **Definition und Abgrenzung von KI:** Unterschiedliche regulatorische Definitionen der Begriffe „KI-System“, „KI-Modell“ und „Modell“ zwingen jede Institution dazu, einen eigenen Ansatz zu entwickeln, um abzugrenzen, was unter KI-Governance, MRM oder beides fällt.
- **Gestaltung der Governance und Rolle der drei Lines of Defence:** Die Vielfältigkeit und funktionsübergreifende Natur von KI erfordert neue Governance-Strukturen, die die Verteilung der Zuständigkeiten auf die drei Verteidigungslinien neu überdenken.
- **Anwendung des Grundsatzes der Verhältnismäßigkeit und Tiering:** Der Umfang und die Vielfalt der Anwendungsfälle im Bereich der künstlichen Intelligenz erfordern risikobasierte Klassifizierungsrahmen, die den Umfang der Aufsicht an den potenziellen Auswirkungen und der Komplexität ausrichten.
- **Bewältigung von Risiken im Zusammenhang mit Drittanbietern und „Model-as-a-Service“ (MaaS):** Die zunehmende Abhängigkeit von externen KI-Anbietern bringt Risiken in der Lieferkette hinsichtlich Transparenz, Kontrollierbarkeit und Dokumentation mit sich, die herkömmliche Validierungsverfahren vor neue Probleme stellen.
- **Entwicklung KI-spezifischer Validierungsansätze:** Transparenz, Erklärbarkeit, Fairness und das dynamische Verhalten von Techniken wie generativer KI und großen Sprachmodellen erfordern Validierungsmethoden, die weit über die für traditionelle statistische Modelle verwendeten Methoden hinausgehen.

Trotz dieser Herausforderungen verfolgen die Banken ein gemeinsames Ziel: die Einführung einer risikobasierten und verhältnismäßigen Aufsicht, die Weiterentwicklung des MRM (und nicht nur dieses) von einer reaktiven Kontrollfunktion hin zu einem proaktiven Katalysator für verantwortungsvolle Innovation sowie den Einsatz von Technologie, um mit dem Tempo der KI-Einführung Schritt zu halten. Die folgenden Fallstudien spiegeln die individuelle Perspektive und die Prioritäten der jeweiligen Institution wider, die durch ihre Größe, ihr Geschäftsmodell, ihre systemische Einstufung und ihre regulatorische Stellung geprägt sind. Sie sind bewusst nicht nach einem einheitlichen Muster verfasst, und die Vielfalt der Ansätze ist selbst eine Erkenntnis dieser Arbeit. Es gibt jedoch mehrere wiederkehrende Themen, die die Beiträge verbinden und in Tabelle 1 zusammengefasst sind.

	Commerzbank	Deka	KfW
Geschäfts-modell	Internationale Geschäftsbank	Großer Wertpapierdienstleister	Deutsche Förderbank
KI- / Modell-definition	• Dualer Ansatz: derzeit breiterer Anwendungsbereich (vollständiges KI-Inventar einschließlich Regressionsmodellen gemäß ML-Richtlinie) • Künftig engere Definition im Einklang mit der EZB (z. B. Regressionen aus der KI ausgeschlossen)	• Klare Unterscheidung zwischen der Modelldefinition nach MaRisk und der Definition eines KI-Systems nach EU AI Act • Nicht jedes KI-System sollte automatisch als Modell eingestuft werden	• Ein KI-Modell gilt im Sinne des MRM als Modell, wenn es die von MaRsik abgeleitete Modelldefinition erfüllt
Integration MRM und KI-Governance	• Vollständig integriert: KI-Governance, ML-Richtlinien und das MRM-Framework funktionieren als einheitliches System im Rahmen des 3LoD-Modells	• Bewusst parallel: KI-Governance und MRM-Governance laufen als unabhängige, aber miteinander interagierende Steuerkreise • Ein Austausch zwischen den beiden Systemen wird empfohlen	• Separate Richtlinien für den Einsatz von KI und die Nutzung von Modellen • Beide Richtlinien verweisen auf einander
Kategorisierung KI-Risiko	• KI-Risiken werden als übergreifender Faktor innerhalb bestehender Risikokategorien behandelt • Vier Schadenspotenziale: menschliche Aufsicht, Fairness, Transparenz, Zuverlässigkeit; Risikoeinstufung gemäß ML-Leitlinie	• Keine neue (interne) Risikokategorie für KI-Risiken • Die Risikoeinstufung für KI-Systeme erfolgt gemäß dem EU AI Act	• Es wurde nicht als neue Risikokategorie eingestuft, sondern wird als potenzieller Risikofaktor für bereits etablierte Risikokategorien betrachtet
KI-Modelle und -systeme von Drittanbietern	• Diversifizierung der Cloud-Partnerschaften zur Minderung des Konzentrationsrisikos • Prüfung des Einsatzes von Open-Source-Lösungen, um Flexibilität zu wahren und eine Bindung an bestimmte Anbieter zu vermeiden	• Einrichtung einer hybriden Cloud zur Implementierung von Anbietermodellen, wo immer dies möglich ist, um Risiken zu minimieren	• Derzeit in Diskussion
Tiering für KI-Modelle und -systeme	• Proportional nach potenziellen Auswirkungen und Komplexität klassifiziert, unter Berücksichtigung von Funktion, Autonomiegrad, geschäftlicher Bedeutung sowie den Konsequenzen von Fehlfunktionen oder Missbrauch	• Einstufung jedes KI-Systems gemäß den Kategorien des EU AI Act	• KI-Systeme werden gemäß den Kategorien des EU AI Act klassifiziert
Validierung	• Konzeptionelle Beurteilung: Einhaltung der ML-Richtlinien, Wesentlichkeit, Komplexität, Verwendungszweck • Dokumentierte Teststrategie, die relevante Risikoszenarien abdeckt, sowie eine kontinuierliche Überwachung mit klaren Regelungen für die Inbetriebnahme und Modelländerungen	• Aufgrund der Unterscheidung zwischen Modell und KI-System ist die Validierung von KI-Systemen Teil des Softwareentwicklungsprozesses, während für Modelle etablierte Validierungsverfahren zum Einsatz kommen (auch in Fällen, in denen KI-Systeme als Modelle fungieren)	• Koexistenz von Validierungsansätzen für Modelle und Verprobung bei KI-Systemen im Rahmen des Softwareentwicklungs-prozesses

Tabelle 1: Wesentliche Dimensionen und jeweiliger Ansatz der Banken

Detaillierte Fallstudien

Einblicke aus einer internationalen Geschäftsbank – Ratul Ahmed, Commerzbank AG

Der wahre Wert der KI liegt in einer klaren Problemformulierung und nicht in der einseitigen Fokussierung auf die Tools. KI im Bankwesen wird ein koordiniertes System sein, das statistische Modelle, Systeme des maschinellen Lernens, große generative Modelle und regelbasierte Logik umfasst, die jeweils dort eingesetzt werden, wo sie am effektivsten sind. Der Erfolg hängt von der Klarheit der Zielsetzung sowie vom menschlichen Urteilsvermögen ab, wobei Vertrauen, Nachvollziehbarkeit und Kontrolle die Grundlagen bilden, die sicherstellen, dass der Einsatz von KI im Einklang mit Werten, Vorschriften und gesellschaftlichen Erwartungen steht.

Die Commerzbank strebt an, eine KI-gesteuerte Bank zu werden, die KI und GenAI einsetzt, um Entscheidungen zu verbessern, Prozesse zu optimieren und Innovationen in allen Geschäftsbereichen voranzutreiben. Die KI-Strategie ist in die Strategien für IT, Daten und digitale operative Resilienz eingebunden und stützt sich auf drei Säulen:

- Empowered AI (dezentral, abteilungsübergreifende Bereitstellung, eingebettet in Geschäftsabläufe)
- AI Foundation (skalierbare, sichere Plattformen, Tools und Daten)
- KI-Kultur (Kompetenz, Vertrauen, Befähigung zu verantwortungsvollem Einsatz)

Die Operationalisierung umfasst KI-Hubs in den Geschäftsbereichen sowie KI-Partner, um die Einführung und den Austausch voranzutreiben. Der Fortschritt wird anhand von KPIs gemessen, die sich auf KI-Schulungen, skalierbare Dienste, die Reife der Hubs, die Datenbereitschaft, die Plattformakzeptanz, vertrauenswürdige KI-Praktiken und die Wertschöpfung erstrecken. Die KI-Kompetenz im gesamten Bankhaus wird durch Schulungen, Newsletter, Videoserien und Hackathons gefördert. Die ethischen Grundsätze umfassen Transparenz, Nichtdiskriminierung, menschliche Aufsicht, Datenschutz, Inklusivität und Fairness. Diese werden durch 3LoD, eine Richtlinie und Leitlinie für maschinelles Lernen sowie ein KI-Inventar gestützt, das in das Modellrisikomanagement-Tool integriert ist und die Rückverfolgbarkeit über Anwendungsfälle, Modelle und Systeme hinweg gewährleistet. Die Ausrichtung am EU-KI-Gesetz dient als Leitfaden für risikobasierte Verpflichtungen und GPAI-Anforderungen. Die Bank diversifiziert ihre Cloud-Partnerschaften, um Konzentrationsrisiken zu mindern, und prüft Open-Source-Lösungen, um Flexibilität zu wahren und Lock-in-Effekte zu vermeiden.

Dennoch bestehen weiterhin Herausforderungen bei der Umsetzung. Die Definitionen des EU AI Act sind weit gefasst, wodurch die Grenzen zwischen herkömmlichen Risiko- und Preismodellen und KI-Systemen verschwimmen und Unklarheiten hinsichtlich des Anwendungsbereichs entstehen. Die Aufsicht erstreckt sich auf mehrere Stellen, was die Gefahr unterschiedlicher Auslegungen und Widersprüche birgt. Es bestehen Überschneidungen mit der Produktsicherheit, DORA, der DSGVO und MaRisk, was eine sorgfältige Harmonisierung erfordert. Unsicherheiten hinsichtlich der Filter bestehen weiterhin. Die Durchführbarkeit der Übergangsregelungen wird durch Verzögerungen bei den CEN/CENELEC-Normen und das Zusammenspiel mit Branchenstandards erschwert. Die Lieferkette für GenAI wirft Fragen hinsichtlich Souveränität, Wettbewerbsfähigkeit und Compliance auf, da viele grundlegende Modelle ihren Ursprung außerhalb Europas haben.

Rahmenwerke für die Validierung von KI-Modellen

Die Commerzbank wird von der BaFin als O-SII eingestuft, weshalb sich regionale Unterschiede im regulatorischen Rahmen auf die KI-Implementierung der Commerzbank auswirken werden. Die Bank profitiert von einer engen Zusammenarbeit zwischen dem GRM-Modellrisikomanagement und dem Kompetenzzentrum für KI bei GS Data. Als Bank wurde beschlossen, das KI-Risiko als horizontalen Treiber innerhalb bestehender Risikokategorien und nicht als eigenständiges wesentliches Risiko zu behandeln, um sich mit den Aufsichtsbehörden abzustimmen, die bestehende Governance zu nutzen und eine Fragmentierung zu vermeiden. Dies ermöglicht angemessene Kontrollen in den Bereichen Operations, Compliance und Modellrisiko.

Tiering-Ansatz

KI-Systeme und -Modelle werden unter Berücksichtigung ihrer Funktion, ihres Autonomiegrades, ihrer geschäftlichen Bedeutung sowie der Folgen von Fehlfunktionen oder Missbrauch entsprechend ihrer potenziellen Auswirkungen und Komplexität in Stufen eingeteilt. Höhere Stufen (z. B. Entscheidungen mit hohem Risiko oder regulatorische Relevanz) erfordern eine umfassendere Validierung, Dokumentation, Überwachung und Steuerung; niedrigere Stufen unterliegen vereinfachten Kontrollen nach einheitlichen Grundsätzen. Dies gewährleistet Effizienz und die Übereinstimmung mit dem EU AI Act sowie den internen Governance-Standards.

Dynamische Anpassung

Im Zuge der Weiterentwicklung von Regulierung und Technologie überprüfen sowohl die erste als auch die zweite Kontrollinstanz die Klassifizierung und die Governance-Struktur. Eine einheitliche Definition von KI bildet die Grundlage für eine verhältnismäßige Aufsicht und die Vollständigkeit des Bestandsverzeichnisses. Die Commerzbank verfolgt einen dualen Ansatz: einen breiteren Anwendungsbereich für derzeit verbotene Praktiken (vollständige Erfassung im KI-Bestandsverzeichnis, einschließlich Regressionsmodellen, gemäß der Richtlinie zum maschinellen Lernen) und künftig eine engere Definition, die sich an der EZB orientiert (z. B. Ausschluss von Regressionen aus dem KI-Begriff). Dies schafft ein Gleichgewicht zwischen Innovation und Kontrolle und gewährleistet die Einhaltung der regulatorischen Vorschriften. Im Jahr 2025 veröffentlichte die Commerzbank die KI-Governance-Richtlinie und erweiterte damit das Governance-Rahmenwerk um die ML-Richtlinie und die Modellrisikomanagement-Richtlinie für maschinelles Lernen, die alle über die 3LoD umgesetzt werden.

Die Commerzbank hat sich frühzeitig dazu entschlossen, ein KI-Governance-Netz aufzubauen und Rollen und Zuständigkeiten festzulegen:

- First Line (GS-Data unter dem CDAIO): Ist für die KI-Strategie verantwortlich; setzt Richtlinien der zweiten Ebene durch einheitliche Verfahren um; berät Teams in Bezug auf Definitionen, Zulassungskriterien und Einschränkungen; pflegt die ML-Richtlinie; fördert das Verständnis für KI; gewährleistet die Qualität und Vollständigkeit der KI-Bestandsdaten.
- Second Line (GRM-MRM): Ist für die KI-Governance-Richtlinien und das MRM-Rahmenwerk verantwortlich; legt Standards für Risiken im Zusammenhang mit KI-Modellen fest; führt unabhängige Validierungen durch; legt die endgültigen Klassifizierungen fest; kalibriert die Sicherheitsüberprüfung; koordiniert bereichsübergreifende Kontrollen (z. B. Risiken durch Dritte, Datenschutz); bietet frühzeitige Beratung an und validiert Initiativen mit hoher Auswirkung.
- Third Line (GM Audit): Beurteilt unabhängig die Wirksamkeit der Governance und die Kontrollabläufe und passt die Häufigkeit der Überprüfungen an das jeweilige Risiko an.

Praktische Validierungstechniken konzentrieren sich auf

- Konzeptionelle Beurteilung: Sicherstellung, dass die Anforderungen der ML-Richtlinie entsprechend der Risikoklassifizierung berücksichtigt werden; Ermittlung von Wesentlichkeit, Komplexität, Widerstandsfähigkeit, Verwendungszweck und potenziellen Auswirkungen; Anwendung einer Tiering-Struktur für eine verhältnismäßige Überwachung.
- Testing: Dokumentierte Teststrategie für Modellrisikoaspekte; Ergebnisse, die eine ausreichende Zuverlässigkeit belegen; Abdeckung relevanter Risikoszenarien.
- Überwachung und Nachverfolgung: Klare Strategie für Inbetriebnahme und Genehmigungsprozesse; etablierte Governance für Modelländerungen; laufende Überwachung.
- Risikobewertung: Abdeckung aller für das Modellrisiko relevanten Szenarien mit transparenten Annahmen und einer auf Expertenmeinungen abgestimmten Quantifizierung von Wahrscheinlichkeit und Ausmaß.

Wenn jedes Modell zählt – wie geht ein MRM-Team damit in Zukunft um?

Im Rahmen der Aktualisierung ihres Rahmenwerks und ihres Inventars für Modellrisiken hat die Commerzbank Fragen zum GenAI-Inventar behandelt, indem sie Systeme, Modelle und Anwendungsfälle aufgelistet hat, sodass Modelle und Systeme gemäß der ML-Richtlinie unabhängig voneinander klassifiziert werden können. Das Inventar soll:

- Für interne Transparenz bei der Umsetzung im geschäftlichen Kontext sorgen, um Skalierbarkeit zu ermöglichen und Doppelarbeit zu vermeiden.
- Frühzeitige Beratung der Product Owner durch die erste und zweite Ebene (LoD) ermöglichen.
- Die Risikoklassifizierung für die vier Schadenspotenziale (menschliches Versagen, Fairness, Transparenz, Zuverlässigkeit) gemäß der ML-Richtlinie festhalten.
- Die regulatorischen Auswirkungen bewerten, um künftige Verpflichtungen auf europäischer Ebene und in anderen Rechtsräumen zu antizipieren, sowie Prüfung möglicher Sprachprüfungsdienste.

Die Bank treibt zudem das Modelllebenszyklusmanagement über eine Data-Science-Plattform voran, um die konforme Entwicklung, den Betrieb und die Validierung sowohl für zentrale als auch für dezentrale Einheiten zu unterstützen. Dies fördert die kontinuierliche Weiterentwicklung, Robustheit und Skalierbarkeit und verankert bewährte Verfahren für den ML-Lebenszyklus im gesamten Rahmenwerk.

Einblicke aus einem großen Wertpapierdienstleister – Dr. Carsten Wehn & Dr. Cäcilia Zirn, Deka-Gruppe

Einführung in den konkreten Hintergrund

Der Ansatz der Deka zur KI-Governance ist geprägt von einem besonderen institutionellen Kontext und der Erkenntnis, dass KI-Governance und das Governance-System für das Modellrisikomanagement als parallele Regelkreise funktionieren können und in vielen Fällen auch sollten, wobei jeder auf seine jeweiligen regulatorischen Ziele zugeschnitten ist und es definierte Schnittstellen zwischen ihnen gibt. Als großer Wertpapierdienstleister unterliegt die Deka auf ihrer Bankseite der CRR, dem KWG und den MaRisk, jedoch nicht flächendeckend für ihre Vermögensverwaltungsaktivitäten, die unter vermögensverwaltungsspezifischen Vorschriften wie unter anderem den KaMaRisk, dem KAGB und der Derivateverordnung stehen. Da die KI-Entwickler über IT- und Geschäftsabteilungen verteilt sind und nicht in speziellen Modellteams konzentriert sind, hat die Bank ein pragmatisches Governance-Rahmenwerk eingeführt, das sowohl den EU AI Act, die MaRisk-Anforderungen als auch die Anforderungen der EZB-Aufsicht berücksichtigt, ohne diese in eine einzige Struktur zu zwängen.

Bei der Einführung von KI sind hinsichtlich der Rahmenbedingungen zwei Faktoren besonders wichtig.

Der erste Faktor ist die KI-Kompetenz. Herkömmliche Modelle werden in der Regel von einer begrenzten Anzahl von Experten entwickelt, die mit den einschlägigen Vorschriften vertraut sind, und kommen für klar definierte Anwendungsfälle zum Einsatz. KI hingegen wird von zahlreichen Mitarbeitern aus der IT und anderen Abteilungen entwickelt – Personen, die zuvor möglicherweise kaum mit regulatorischen Anforderungen in Berührung gekommen sind. Die Vorschriften selbst sind für den KI-Bereich neu, und ihre konkreten Ausprägungen und Auswirkungen werden erst nach und nach deutlich. Dies führt zu einem Spannungsfeld zwischen der Förderung der Einführung von KI und der Sensibilisierung für die damit verbundenen regulatorischen und internen Anforderungen.

Zweitens ist da der softwarebasierte Charakter der KI. KI-Systeme sind im Grunde genommen Softwareanwendungen und unterliegen daher den bestehenden internen und regulatorischen Anforderungen an die Softwareentwicklung, die Dokumentation und den Umgang mit sensiblen Daten. Wichtig ist, dass sich der EU AI Act in seinen Vorschriften nicht auf KI-Modelle stützt, sondern vielmehr auf die konkrete Anwendung oder den konkreten Anwendungsfall der KI.

Angesichts dieser beiden Faktoren eignet sich die Erweiterung eines bereits etablierten Ansatzes für die Softwareentwicklung besonders gut für ein Finanzinstitut wie die Deka. Da jede Form von KI letztlich mit der Verarbeitung individueller Daten oder einer entsprechenden Anwendung verbunden ist, kann ein solcher Ansatz auf die Softwareentwicklung und deren bestehende Anforderungen ausgerichtet werden. In den folgenden Unterabschnitten wird untersucht, inwieweit dieser Ansatz den regulatorischen Anforderungen (vor allem MaRisk und dem EU AI Act) gerecht wird und welche Vor- und Nachteile er mit sich bringt.

Die MaRisk, der EU AI Act und ihre Auswirkungen auf das Modellrisikomanagement bei der Deka

Die MaRisk als systemische Regulierung für Banken (Modelle im Fokus)

Die regulatorischen Anforderungen an MRM unterscheiden sich je nach Rechtsraum erheblich, siehe Abschnitt 2. Internationale Leitlinien wie SR11-7 wurden im von der EZB regulierten Bereich erst viel später übernommen und sind nach wie vor relativ allgemein gehalten, wobei die Leitlinien der EBA und der EZB speziell auf einzelne Regulierungsbereiche abzielen, wie beispielsweise die normative Perspektive der Säule 1. In Deutschland wurden mit der 7. Änderung der MaRisk in Abschnitt AT 4.3.5 umfassendere Anforderungen für den Einsatz von Modellen eingeführt, die für alle in Deutschland beaufsichtigten Finanzinstitute gelten und die Anforderungen der EZB und der EBA für von der EZB beaufsichtigte Institute ergänzen. Insbesondere gelten für Vermögensverwalter andere Regeln: die MaRisk gilt für Deka auf der Bankenseite, jedoch nicht zwangsläufig auf der Vermögensverwaltungsseite, wo andere Vorschriften relevant sind.

Die Aufnahme von Abschnitt AT 4.3.5 im Jahr 2024 stellt einen bedeutenden Schritt bei der Regulierung der Grundprinzipien für die Modell-Governance dar und trägt gleichzeitig den rasanten technologischen Fortschritten wie maschinellem Lernen und KI Rechnung. Die deutschen Aufsichtsbehörden, darunter die BaFin und die Deutsche Bundesbank, haben eine progressive Haltung eingenommen: anstatt bestimmte Algorithmen oder Methoden zu beschränken, konzentrieren sie sich auf die Erklärbarkeit von Modellergebnissen; siehe BaFin (2021) und Deutsche Bundesbank & BaFin (2021) (21), (22).

Im Rahmen der geänderten MaRisk hat die Modell-Governance zunehmend an Bedeutung gewonnen, sodass Institute nun verpflichtet sind, die im Risikomanagement eingesetzten Modelle bewusst zu implementieren und zu überwachen. Der Umfang dieser Anforderungen hängt von der Komplexität, dem Zweck und den mit dem jeweiligen Modell verbundenen Unsicherheiten ab. Abschnitt AT 4.3.5 erweitert den Anwendungsbereich der MRM-Anforderungen auf alle Modelle, die in nach der MaRisk regulierten Prozessen verwendet werden, und geht damit über die frühere Definition in Abschnitt AT 4.1 hinaus. Eine ausführliche Erörterung der einzelnen Anforderungen von AT 4.3.5 findet sich bei Wehn (2024) (23).

Gemäß MaRisk wird ein Modell als quantitative Methode, System oder Ansatz definiert, das bzw. der statistische oder mathematische Theorien nutzt, um Eingabedaten zu quantitativen Schätzungen zu verarbeiten. Diese Definition umfasst sowohl intern entwickelte als auch von Dritten stammende Modelle, die in Entscheidungsprozessen verwendet werden. Die Leitlinien bieten methodische Flexibilität und erkennen Modelle mit KI-Merkmalen ausdrücklich an, wobei betont wird, dass KI-Anwendungen und traditionelle Modelle grundverschiedene Konzepte darstellen können.

In den MaRisk-Leitlinien werden auch ausdrücklich Modelle erwähnt, die Merkmale künstlicher Intelligenz aufweisen. Dieser letzte Punkt verdeutlicht einmal mehr, dass Anwendungen künstlicher Intelligenz und Modelle zwei grundlegend unterschiedliche Themen sind – oder zumindest sein können.

Der EU AI Act als Verordnung zum Schutz von Verbrauchern und Bürgern

Während die Bankenregulierung im Allgemeinen und die Vorschriften zur Nutzung und zum Einsatz von Modellen im Sinne der MaRisk im Besonderen dazu dienen, unangemessene Verluste für einzelne Banken zu verhindern und letztlich die Systemstabilität zu gewährleisten, zielt der EU AI Act darauf ab, die Rechte der (EU-)Bürger zu schützen.

Der grundlegende Unterschied liegt daher in der Dimension der Regulierung: der EU AI Act betrachtet ein KI-System stets in direktem Zusammenhang mit seinem Verwendungszweck. Die Definition von künstlicher Intelligenz im EU AI Act ist hingegen bewusst weit gefasst, um ein breites Spektrum an KI-Technologien und -Anwendungen abzudecken.

Der Begriff „KI-System“ wird im EU AI Act in Artikel 3 Absatz 1 definiert und bezieht sich auf „ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“. Somit definiert der EU AI Act KI-Systeme ausdrücklich als Software und nicht als Modelle, was für die Umsetzung einer angemessenen Regulierung von entscheidender Bedeutung ist.

Ein KI-System kann zwar die Verwendung eines Modells beinhalten, dies ist jedoch nicht zwingend erforderlich. Es ist wichtig zu beachten, dass KI-Systeme gemäß dem EU AI Act nicht per se als Modelle im Sinne von MaRisk AT 4.3.5 gelten. Sie sind das Ergebnis des jeweiligen Algorithmus für maschinelles Lernen, es wird jedoch keine explizite Definition bereitgestellt. Es gibt keine expliziten Anforderungen an diese Modelle an sich, sondern, wie bereits erwähnt, an KI-Anwendungen[1].

Der EU AI Act konzentriert sich daher auf den Schutz der Bürger und berücksichtigt den spezifischen Zweck von KI-Anwendungen, die in vier Risikoklassen eingeteilt werden (siehe Abschnitt 2).

Darüber hinaus wird zwischen dem Anbieter und dem Betreiber einer KI-Anwendung unterschieden. Gemäß Artikel 3 Absatz 3 des KI-Gesetzes ist ein Anbieter „eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich“. Gemäß Artikel 3 Absatz 4 des KI-Gesetzes ist ein Betreiber „eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet.“

Die im EU AI Act für jede KI-Anwendung festgelegten Anforderungen ergeben sich aus der Konstellation von Rollen und Risikoklassen.

1 Der EU AI Act führt spezifische Vorschriften für sogenannte „KI-Modelle mit allgemeinem Verwendungszweck“ (im Folgenden als GPAI bezeichnet) ein. GPAI-Modelle, zu denen große generative KI-Modelle und insbesondere große Sprachmodelle (LLMs) wie GPT-4 gehören, können für eine Vielzahl von Aufgaben eingesetzt werden. Ist ein GPAI-Modell in ein KI-System integriert oder bildet es einen Teil davon, sollte dieses System als Allzweck-KI-System betrachtet werden, sofern die Integration es ermöglicht, dass es einer Vielzahl von Zwecken dient. Das KI-Gesetz stellt jedoch nur Anforderungen an die Anbieter von GPAI-Modellen. In der Praxis ist es daher unwahrscheinlich, dass Deka von diesen zusätzlichen Anforderungen betroffen ist, da das Unternehmen nicht als Anbieter von GPAI-Modellen auftritt.

Implikationen für eine angemessene Governance

Diese unterschiedlichen Definitionen und regulatorischen Ziele haben direkte Auswirkungen auf die Gestaltung der Governance sowohl für KI-Systeme als auch für KI-Modelle. Der zentrale Grundsatz, an den sich ein Institut halten kann, das nicht dem SR11-7 unterliegt und bei dem die Bankenregulierung nicht flächendeckend gilt (wie beispielsweise bei den Vermögensverwaltungsaktivitäten der Deka), lautet, dass die Governance für beide Bereiche unabhängig voneinander eingerichtet werden kann. Es besteht keine Verpflichtung, beide Bereiche aus einer Hand zu steuern. Vielmehr kann jeder Bereich in einem eigenen Regelkreis behandelt werden, der sich auf seine spezifischen Aspekte konzentriert. Diese Trennung trägt auch einer praktischen Realität Rechnung: Änderungen an Modellen können je nach ihren Auswirkungen sehr langwierig sein (z. B. wenn eine aufsichtsrechtliche Genehmigung erforderlich ist) und erfordern erhebliche Aufmerksamkeit seitens des Managements (bis hin zur Vorstandsebene), während Innovationszyklen für KI-Systeme sehr schnell sein müssen, um wettbewerbsfähig zu bleiben. Die Trennung der beiden Governance-Stränge ermöglicht es jedem, in seinem eigenen Tempo zu arbeiten, was im nächsten Unterabschnitt näher erläutert wird.

Zusammenfassend lassen sich folgende Zusammenhänge ableiten:

- Modelle sind datenverarbeitende Systeme, die sich auf MaRisk-Prozesse auswirken oder den Anforderungen der EZB bzw. der EBA entsprechen müssen.
- Unter künstlicher Intelligenz versteht man Systeme, die auf der Grundlage bestimmter Technologien funktionieren.
- Mit Ausnahme einiger weniger Sonderfälle handelt es sich bei beiden um Softwareanwendungen.
- Entscheidend ist, dass nicht jedes KI-System automatisch als Modell betrachtet werden sollte.

Einbindung von KI in eine angemessene Governance

Wie oben dargelegt, handelt es sich bei Modellen und KI-Systemen um unterschiedliche Einheiten, die Vorschriften mit unterschiedlichen Zielen unterliegen. MaRisk (und gegebenenfalls die Leitlinien der EBA und der EZB) regeln Modelle, um ein solides MRM sicherzustellen. Der EU AI Act regelt KI-Systeme, um Bürger und Verbraucher zu schützen. Wo die umfassenden Anforderungen von SR11-7 nicht gelten, ist es möglich, einen eigenen Governance-Rahmen für Modelle und einen eigenen Governance-Rahmen für KI-Systeme zu schaffen, die jeweils die relevanten Anforderungen und Vorschriften erfüllen. Diese Trennung gewährleistet eine angemessene Berücksichtigung jedes Bereichs. Die gestalterische Frage für Finanzinstitute lautet: Wie kann KI-Governance effektiv mit den etablierten MRM-Anforderungen koexistieren?

Trotz ihrer Unterschiede weist die Governance für Modelle und KI-Systeme mehrere Gemeinsamkeiten auf:

- Inventar: Sowohl Modelle als auch KI-Systeme müssen in einem Inventar erfasst werden, wobei sich die Anforderungen unterscheiden. Ein Modellinventar muss die wesentlichen Aspekte des Modells, die neuesten Validierungsergebnisse und den Bearbeitungsstatus erfassen. Ein KI-Inventar muss insbesondere die Risikoklasse eines KI-Systems (im Hinblick auf seinen Anwendungsfall) gemäß dem EU AI Act sowie die Rolle (Anbieter oder Betreiber) dokumentieren, die die Bank in Bezug auf das System einnimmt.
- Lebenszyklus: Innerhalb jedes Lebenszyklus gibt es verschiedene Rollen.
- MRM legt klare Zuständigkeiten und Entscheidungsbefugnisse durch fünf definierte Rollen fest (24): Modellverantwortliche, Modellentwickler, Modellnutzer, Modellbetreiber und Modellvalidierer. Diese Rollen arbeiten über den gesamten Modelllebenszyklus hinweg zusammen, wie in Abbildung 2 dargestellt.

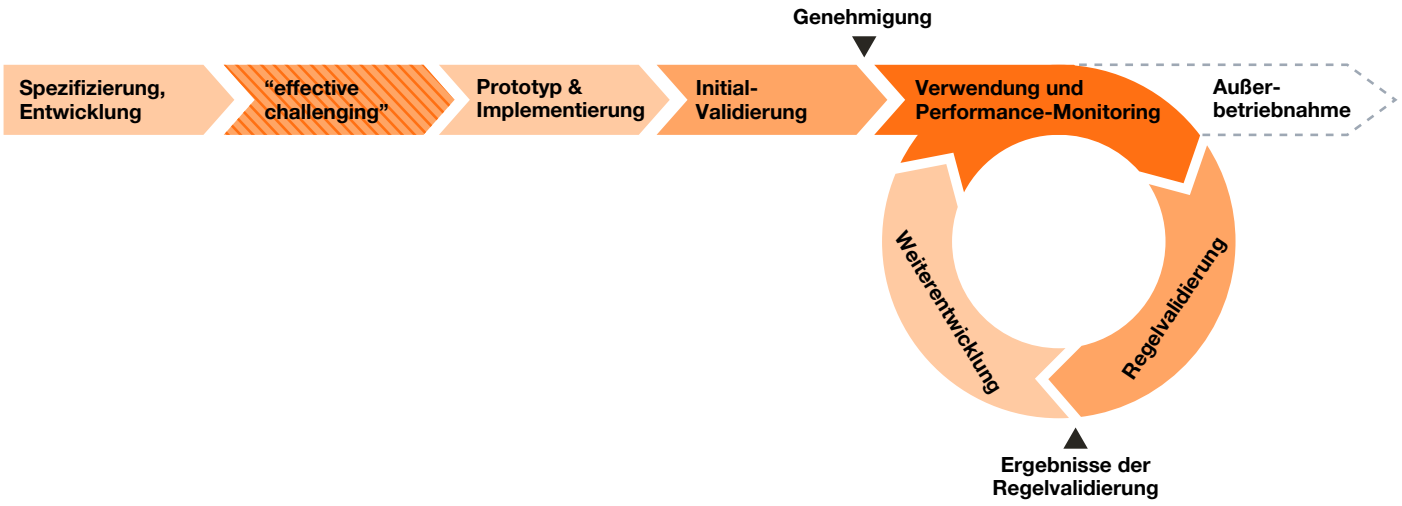


Abbildung 2: Schematische Darstellung des Modelllebenszyklus, vgl. (24)

Auf der Grundlage ihrer Ziele und der aus der Finanzkrise gewonnenen Erkenntnisse überträgt die Aufsichtsbehörde die Verantwortung für die Verwendung von Modellen, insbesondere im Management von Finanzinstituten, der obersten Führungsebene. Von der Geschäftsleitung wird erwartet, dass sie sich der Stärken, Schwächen und Grenzen der Modelle bewusst ist.

Ebenso müssen bei der Regulierung von Systemen der künstlichen Intelligenz verschiedene Anforderungen berücksichtigt werden. Da es sich bei KI-Anwendungen um IT-Anwendungen handelt, gelten die Anforderungen für die Softwareentwicklung und -implementierung. Spezifische Anforderungen, die sich aus der jeweiligen Risikoklasse und der Rolle als Anbieter oder Betreiber im Rahmen des EU AI Act ergeben und über bestehende Anforderungen hinausgehen, können in bestehende Leitlinien aufgenommen werden.

Im Gegensatz zu Modellen, die in der Regel in ihrem spezifischen Kontext betrachtet werden und selten einer übergreifenden „Modellstrategie“ unterliegen, erfordert KI eine eigene Strategie. Eine solche Strategie sollte die geschäftspolitischen Auswirkungen und Perspektiven berücksichtigen sowie strategische Anwendungsfälle erörtern. Es kann auch im Voraus festgelegt werden, welche Risikoklassen von KI-Systemen gemäß dem EU AI Act akzeptabel sind, beispielsweise ob Systeme mit hohem Risiko akzeptabel sind, standardmäßig ausgeschlossen werden oder zusätzlichen Anforderungen unterliegen.

Da KI-Anwendungen in der Regel gemeinsam von den Fachabteilungen und der IT-Abteilung entwickelt werden, sind die Aufgaben auf mehrere Abteilungen verteilt:

- Die Fachabteilungen konzipieren die Funktionen und technischen Inhalte der KI-Anwendung und bewerten deren wirtschaftlichen Nutzen.
- Der Fachbereich und die IT-Abteilung sorgen gemeinsam für die Einhaltung der Anforderungen an KI-Systeme.
- Die IT-Abteilung sorgt für die Einhaltung der technischen Vorgaben (Entwicklung, Tests, Betrieb usw.) und legt Infrastruktur- und Technologiestandards fest.
- Angesichts der damit verbundenen Cyberrisiken erfordert die Informationssicherheit besondere Aufmerksamkeit, die durch die Zusammenarbeit zwischen den jeweiligen Abteilungen und den zentralen IT-Sicherheitsabteilungen gewährleistet wird.

In der Praxis lässt sich ein KI-Inventar effizient auf der Grundlage des bestehenden Software-Inventars einrichten, beispielsweise eines bereits gepflegten Unternehmensarchitektur-Systems. Es müssen lediglich die zusätzlichen Merkmale, die sich aus dem EU AI Act ergeben (Risikoklasse, Rolle), in das Inventar aufgenommen werden.

Wie oben dargelegt, ist es möglich, eine KI-Governance parallel zur MRM-Governance zu etablieren, die auf die spezifischen Anforderungen und die hohe Dynamik der KI zugeschnitten ist. Dies ermöglicht eine präzise Einhaltung der Vorschriften, ohne dass es zu nennenswerten Redundanzen zwischen den beiden Regelkreisen kommt. Dennoch ist ein Austausch zwischen den beiden Systemen sowohl ratsam als auch in bestimmten Fällen unerlässlich, da ein KI-System auch ein Modell sein kann und umgekehrt.

KI-Anwendungen unterscheiden sich aufgrund der damit verbundenen Risiken von herkömmlichen Softwareanwendungen: Zusätzlich zu den im EU AI Act definierten Risikoklassen können KI-Anwendungen beispielsweise Reputations- oder Cyberrisiken mit sich bringen. Daraus ergeben sich zwei Konsequenzen:

- Die Definition der Risikoklassen für KI-Anwendungen sollte entsprechend angepasst und innerhalb der bestehenden Risikokontrollstellen zentral koordiniert werden. So kann beispielsweise eine Anwendung, die nach dem EU AI Act als risikoarm eingestuft wird, dennoch hohe Reputationsrisiken bergen und sollte daher intern als risikoreichere Anwendung behandelt werden, für die strengere Standards gelten.
- Besonderes Augenmerk sollte auf die Validierung gelegt werden. Insbesondere bei kritischen KI-Anwendungen sollte das Fachwissen im Bereich der Modellvalidierung für Bewertungen genutzt werden, die über Systemtests hinausgehen.

KI als Chance

Zusammenfassend lässt sich sagen, dass die Herausforderungen bei der Einführung von KI-Systemen in mittelgroßen Finanzinstituten und Banken zwar vielfältig sind, KI insgesamt jedoch positiv zu bewerten ist. Die Angleichung des Governance-Rahmens für KI an die Richtlinien für die Einführung von Softwareanwendungen ist ein pragmatischer Ansatz, da potenzielle KI-Entwickler über die gesamte Prozesskette verteilt sein können, anstatt in einem einzigen Team konzentriert zu sein.

Diese KI-Governance kann sich von der Modell-Governance unterscheiden, da für Modelle lediglich die Anforderungen der MaRisk relevant sind. In diesem Fall beschränken sich die Modelle auf jene Verfahren, deren Prozesse in den Anwendungsbereich der MaRisk fallen, der in der Regel deutlich enger gefasst ist als der potenzielle Anwendungsbereich von KI-Systemen. Für KI-Systeme gelten die Anforderungen des EU AI Act, was Erweiterungen der bestehenden Software-Governance und Ergänzungen des Inventars erforderlich macht.

Beide Steuerkreise können dann entweder durch einen Vergleich der damit verbundenen Risiken (z. B. nichtfinanzielle Risiken) oder durch einen systemischen Vergleich angemessen miteinander verknüpft werden.

Mit Blick auf die Zukunft bleiben weitere Herausforderungen bestehen. Die Regulierung von KI-Systemen wird sich weiterentwickeln, und das Tempo der technologischen Entwicklung ist nach wie vor sehr hoch. Diese beiden Dynamiken zeitnah in den Governance-Rahmenbedingungen zu berücksichtigen, ist keine leichte Aufgabe. Die Autoren empfehlen daher eine pragmatische Umsetzung der jeweiligen Anforderungen, damit auf künftige Entwicklungen so flexibel wie möglich reagiert werden kann.

Die Autoren danken Fabian Müller (statworx) für anregende Gespräche über die Einrichtung einer praxisorientierten KI-Governance.

Einblicke aus einer deutschen Förderbank – Hans Elbracht, KfW

Die Initiierung und Umsetzung von KI-gestützten Anwendungsfällen ist ein schnell wachsender Bereich innerhalb der KfW, der Prozessoptimierung, Entscheidungshilfen und Interaktionsansätze in nahezu allen Geschäftsbereichen umfasst. Infolgedessen verteilen sich Anbieter und Nutzer von KI-Anwendungsfällen zunehmend über die gesamte Bank (und darüber hinaus), was sowohl das transformative Potenzial als auch die Herausforderung verdeutlicht, die (bekannten und unbekannten) Chancen und Risiken konsequent zu steuern.

Die Art und Vielfalt der Anwendungsfälle im Bereich der künstlichen Intelligenz führt nicht nur zu einer steigenden Zahl potenzieller Nutzer, sondern auch zu einem breiteren Spektrum an beteiligten Akteuren und Fachbereichen. Neben den Abteilungen, die die Anwendungsfälle entwickeln, sollten zumindest die Bereiche IT, Daten- und Informationssicherheit, Drittanbietermanagement, Recht sowie Risiko (nichtfinanziell und finanziell) einbezogen werden.

Anwendungsfälle für KI können als spezifische Anwendungen von KI-Technologien (d. h. ML, NLP, GenAI) betrachtet werden. Der EU AI Act definiert ein KI-System als „maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“ (25). Diese Definition weist eine gewisse Ähnlichkeit mit der (bankaufsichtsrechtlichen) Definition eines Modells als „quantitative Methode, System oder Ansatz, der statistische, ökonomische, finanzielle oder mathematische Theorien, Techniken und Annahmen anwendet, um Eingabedaten zu quantitativen Schätzungen zu verarbeiten“ auf (siehe SR 11-7 oder MaRisk).

Für eine effiziente und nachhaltige Einführung von KI-Anwendungsfällen sollte die Institution daher unter anderem Gemeinsamkeiten zwischen bereits etablierten Ansätzen für Systeme und Modelle ermitteln. Dies ist entscheidend, um geeignete Kompromisse zu finden, die sowohl den Verbraucherschutz- als auch den Bankvorschriften gerecht werden. Das Leitprinzip der KfW besteht jedoch darin, konkrete Anwendungsfälle in den Mittelpunkt der Aufmerksamkeit und der Bemühungen zu stellen.

Aktuelle Ansätze der KI- und der Modell-Governance

Eine der größten Herausforderungen bei der Konzeption und Umsetzung von KI-Anwendungsfällen besteht darin, die Geschwindigkeit und Innovationskraft der KI mit der Notwendigkeit einer nachhaltigen Vertrauenswürdigkeit in Einklang zu bringen. Angesichts des breiten Spektrums an KI-Anwendungsfällen hat die KfW die bankweite Verantwortung für das Management von KI-Anwendungsfällen bislang noch keiner bestimmten Abteilung oder Funktion zugewiesen, da sie der Ansicht ist, dass eine verfrühte Zentralisierung die sich entwickelnde Landschaft einschränken könnte. Um Redundanzen und Ineffizienzen zu vermeiden, halten wir eine prozessübergreifende Integration von Softwareentwicklung, Beschaffung und Risikomanagement für unerlässlich.

Die KfW verfolgt daher einen stärker kooperativen Ansatz, bei dem die Zuständigkeiten gemeinsam wahrgenommen werden, und zieht insbesondere bei der Verwaltung von Systemen und Modellen die verschiedenen Fachbereiche innerhalb der Institution hinzu. Angesichts der bankweit steigenden Nachfrage nach der Umsetzung von KI-Anwendungsfällen ist die derzeitige Governance der KfW zur Erkennung und Steuerung der damit verbundenen Risiken wie folgt strukturiert:

- Strategischer Ansatz: Die Entwicklung und Nutzung von KI-Anwendungsfällen ist Teil der IT-Strategie, da jeder KI-Anwendungsfall in gewissem Maße in IT-Prozesse, -Technologien und -Anwendungen eingebettet ist. Die Abteilung für nichtfinanzielle Risiken ist dafür verantwortlich, die Einhaltung der (verbraucherbezogenen) Vorschriften, insbesondere des EU AI Act, sicherzustellen. Die Abteilung für Finanzrisikokontrolle ist für die strategische Entwicklung (aller) Modelle und die Einhaltung der (bankaufsichtsrechtlichen) Vorschriften verantwortlich, wodurch MRM Teil der Risikostrategie wird. Darüber hinaus wurde das KI-Risiko nicht als neue Risikokategorie bewertet, sondern KI-Risiken werden als potenzielle Risikotreiber für bereits etablierte Risikokategorien sowohl bei finanziellen als auch bei nichtfinanziellen Risiken behandelt. Daher decken etablierte Risikomanagementprozesse auch das KI-Risiko ab.
- Leitlinien: Die KfW hat interne Leitlinien für den Einsatz von KI und Modellen erstellt. Die Leitlinien zum KI-Einsatz übernehmen die Definitionen des EU AI Act für KI-Systeme und Allzweck-KI-Modelle und umfassen allgemeine Grundsätze für den verantwortungsvollen Einsatz, Rollen, Risikoklassifizierung, Anwendungen von Drittanbietern sowie KI-Kompetenz. Die Einhaltung wird durch eine Checkliste für jeden KI-Anwendungsfall sichergestellt, die von einer KI-Community unterstützt wird. Die Modellrisikorichtlinie definiert Modelle anhand der MaRisk-basierten Definition (und deckt damit auch KI-Modelle ab) und legt spezifische Anforderungen in Bezug auf Modellrisiken, Rollen, Prozesse (Entwicklung, Validierung, Genehmigung) und Berichterstattung fest. Wichtig ist, dass beide Richtlinien (KI-Nutzung und Modellnutzung) auf einander verweisen.
- Inventare: Anwendungsfälle für KI werden im Anwendungsinventar erfasst, während Modelle in einem separaten Modellinventar verwaltet werden. Letzteres unterstützt zudem wichtige Arbeitsabläufe zur Verwaltung der Inbetriebnahme, Nutzung und Deaktivierung von Modellen. Die KfW hat sich bewusst dafür entschieden, beide Inventare bislang nicht zusammenzuführen, sondern führt stattdessen regelmäßige Abgleiche durch, um einen einheitlichen Überblick über beide Bereiche zu gewährleisten.

- Rollen: Zur Verwaltung von KI-Anwendungsfällen und -Modellen über deren gesamten Lebenszyklus hinweg werden verschiedene Rollen verwendet und implementiert. Bei KI-Anwendungsfällen handelt es sich dabei um Nutzer der KI-Anwendungen, technische Rollen (Entwicklung, Implementierung, Wartung) sowie Kontrollverantwortlichkeiten. Für Modelle im Allgemeinen sind diese Rollen Nutzer, (Modell-)Eigentümer, Entwickler, Validierer und andere etablierte Rollen, die aufgrund der (durch Regulierung bedingten) Reife des Modellmanagementbereichs bereits seit längerer Zeit bestehen. Es gibt natürliche Ähnlichkeiten zwischen den Verantwortlichkeiten dieser Rollen für KI und Modelle. Die Rollen für anspruchsvolle Modelle (Entwicklung, Überwachung, Validierung) entwickeln sich jedoch rasch weiter, was auf das Tempo des technologischen Wandels, die Schwierigkeit, klar zwischen Systemen und Modellen zu unterscheiden, sowie die zunehmende Abhängigkeit von Lösungen Dritter und deren Fachwissen zurückzuführen ist.
- Klassifizierung: Die KfW hat verschiedene Bewertungsmethoden zur Risikobewertung eingeführt und priorisiert die Maßnahmen für KI-Anwendungsfälle und -Modelle. KI-Systeme werden gemäß den Kategorien des EU AI Act klassifiziert (siehe Abschnitt 2). Die Priorisierung der Umsetzung ist das Ergebnis einer umfassenden Abstimmung über alle IT-Anwendungsfälle hinweg (nicht beschränkt auf KI). Zur Priorisierung der Maßnahmen zur Pflege von (Risiko-)Modellen wendet die KfW einen mehrstufigen Ansatz an, der auf der Wesentlichkeit und den steuerungsrelevanten Auswirkungen dieser Modelle für das Institut basiert. Das Risiko der Nutzung dieser Modelle wird in erster Linie durch laufende Überwachungs- und Validierungsmaßnahmen ermittelt, wobei potenzielle Genehmigungen im Rahmen des Genehmigungsverfahrens erörtert werden.

Zusammenfassend lässt sich sagen, dass die KfW Cluster feststellt, in denen der Umgang mit KI-Systemen und -Modellen vergleichbar ist, sodass es sinnvoll erscheint, die bestehenden Ansätze zu bündeln, um Wissen und Ressourcen zusammenzuführen.

Dementsprechend hat die KfW zwei Initiativen ins Leben gerufen. Es wurde die Funktion eines KI-Accelerators geschaffen, eine spezielle Rolle, deren Aufgabe es ist, bankweite Hindernisse bei der Initiierung und Umsetzung von KI-Anwendungsfällen zu identifizieren und zu beseitigen, wobei das etablierte 3-Lines-of-Defence-Modell beibehalten wird. Zu ihren Zielen gehören die Transparenz über alle KI-Anwendungsfälle und die Koordination vergleichbarer Fälle, die Überwachung der Gesamtleistung, rechtliche und regulatorische Themen sowie die institutionenweite Weiterbildung und Schulung. Parallel zu dieser Koordinierungsfunktion wurde eine nach dem Agile Release Train (SAFe) strukturierte KI-Fabrik eingerichtet, die darauf ausgelegt ist, KI-Entwicklungsressourcen zu rationalisieren und zu skalieren, mit dem strategischen Ziel, eine zentralisierte KI-Plattform aufzubauen. Zusammen zielen beide Initiativen darauf ab, die Implementierung und Wartung von KI-Anwendungsfällen zu beschleunigen und gleichzeitig die allgemeine KI-Governance zu verbessern.

Gleichzeitig wird die bereits bestehende Governance-Funktion dazu angehalten, bestehende und neue KI-Anwendungsfälle zu begleiten, wobei besonderes Augenmerk auf die wesentlichen Merkmale dieser neuen Klasse von Systemen und Modellen gelegt wird, darunter Rückverfolgbarkeit, Autonomie und Anpassungsfähigkeit. Dies umfasst auch die Erkennung und Eindämmung von KI-spezifischen Phänomenen wie Modelldrift, Konzeptdrift und Halluzinationen.

Vielfalt als Chance

Die Herausforderung, Innovation und Aufsicht in ein angemessenes Gleichgewicht zu bringen, ist nicht neu, doch die breite Palette an Anwendungsfällen und die große Zahl (zukünftiger) Nutzer unterscheiden sich von früheren Veränderungen. Die Vielfalt sowohl der KI-Anwendungsfälle (geschäftlicher Kontext und technische Lösung) als auch der beteiligten Disziplinen bietet jedoch die Chance, bestehende Rollen neu zu definieren und die Zusammenarbeit innerhalb der gesamten Institution zu optimieren – ein Prozess, der weit über die Modellrisikofunktion hinausgeht.

Ein wesentlicher Faktor für die Verbesserung der Zusammenarbeit ist ein fortschrittliches Lebenszyklusmanagement. Die derzeitigen Lebenszyklusphasen, die durch sequenzielle Arbeitsabläufe und Dokumentationsanforderungen gekennzeichnet sind, bergen die Gefahr, dass sie Innovationen bei KI-Anwendungsfällen von vornherein behindern. Die KfW strebt eine Beschleunigung der zweckmäßigen Bewertungen und der entsprechenden Genehmigungsverfahren an, doch dies beginnt ganz klar mit einem Umdenken und einer Verhaltensänderung bei allen Beteiligten. Zudem erfordert dies eine größere Flexibilität bei den regulatorischen Anforderungen, da sequenzielle Prozesse und Dokumentationen im Hinblick auf modernes Modellmanagement nicht mehr dem Stand der Technik entsprechen. Gemeinsame Plattformen, die eine gleichzeitige Entwicklung, Prüfung und Dokumentation ermöglichen, sind unerlässlich.

Ein weiterer Faktor ist das Umdenken hinsichtlich der Rolle von Steuerungseinheiten. Angesichts des rasanten Innovationstempos und der Eigenschaften von KI-Modellen (selbstlernend, unbekannte Kausalität) ist es wichtig, die Rollen neu zu definieren, um einen proaktiveren oder präventiveren Charakter zu erreichen, was ein Umdenken und Umhandeln erfordert. Die auf Richtlinien basierende Validierung und Freigabe muss um situationsbezogene Herausforderungen erweitert werden, insbesondere angesichts des zunehmenden Mangels an internen Lösungen (für KI-Anwendungsfälle).

Ein dritter Treiber ist die strategische Konsolidierung von Systemen und Modellen. Derzeit liegt der Schwerpunkt bei der Erneuerung und Wartung von Modellen sowie deren Anwendungsfällen häufig auf einzelnen Modellen. Viele künftige Anwendungsfälle im Bereich Automatisierung und KI richten sich jedoch an ein breiteres Publikum und sind darauf ausgelegt, Effizienzsteigerungen in großem Maßstab zu erzielen. Eine bankweite Transparenz über künftige Anwendungsfälle und vergleichbare Anwendungen ist daher unerlässlich, um die (KI-)System- und Modelllandschaft angemessen zu verwalten.

Schließlich bietet die Vielfalt der KI-Anwendungsfälle die Möglichkeit, Geschäfts- und Kontrollbereiche über alle Unternehmensbereiche hinweg enger zusammenzuführen, und dies sollte bei der Umsetzung künftiger KI-Anwendungsfälle als Chance betrachtet werden.

04

Proportional, praxis-orientiert, prinzipien-geleitet: Überlegungen zu einer wirksamen Regulatorik für KI im Bankensektor

Proportional, praxis-orientiert, prinzipien-geleitet: Überlegungen zu einer wirksamen Regulatorik für KI im Bankensektor

Dieses Whitepaper bietet wichtige Einblicke in die Umsetzung der Anforderungen an das Modellrisikomanagement und der sich abzeichnenden Verpflichtungen im Rahmen des EU AI Act bei großen deutschen Banken.

Unser Vergleich verdeutlicht, dass es angesichts der einzigartigen Merkmale jedes einzelnen Instituts derzeit kein allgemeingültiges Modell für Compliance- oder Risikomanagementstrategien gibt. Stattdessen unterscheiden sich die gewählten Ansätze erheblich voneinander, was sowohl die spezifischen internen Gegebenheiten jeder Bank als auch das rasante Innovationstempo widerspiegelt, das der künstlichen Intelligenz innewohnt. Diese Unterschiede zeigen sich in den Organisationsstrukturen, den Governance-Modellen und der Integration von KI-Systemen in bestehende Risikomanagement-Rahmenwerke. Die Institute passen ihre Strategien zum Modellrisikomanagement nicht nur an, um regulatorische Anforderungen zu erfüllen, sondern auch, um in einem Umfeld, das von kontinuierlichem technologischen Fortschritt geprägt ist, Agilität und Reaktionsfähigkeit zu gewährleisten. Für Banken und Finanzinstitute, die in diesem sich wandelnden Bereich nach Inspiration und praktischen Lösungen suchen, ist es unser Ziel, eine Auswahl wichtiger Überlegungen und möglicher Ansätze bereitzustellen. Indem wir aktuelle Praktiken teilen und die Herausforderungen hervorheben, denen sich Branchenkollegen gegenübersehen, hoffen wir, andere bei der Entwicklung robuster, zukunftsorientierter Strategien für die Governance und Überwachung von KI- und modellbezogenen Risiken zu unterstützen.

Je nach ihrer Sichtweise haben sich die Banken dafür entschieden, ein vollständig integriertes Management von KI-Modellen (einschließlich Modell-Governance und Entwicklungsplattformen) einzuführen oder planen dies, oder sie verfolgen eher pragmatische Ansätze, bei denen sie Synergien zwischen MRM und KI-Governance und -Management nutzen, wo dies möglich und sinnvoll ist, diese Bereiche jedoch getrennt halten, wo dies praktischer ist. Alle Banken sind sich jedoch einig, dass die (Modell-)Governance in einem angemessenen Verhältnis zum inhärenten Risiko stehen sollte, unabhängig davon, ob KI zum Einsatz kommt oder nicht, und dass dies auch für die regulatorische Praxis gelten sollte.

Ein wesentliches Ergebnis des Vergleichs der Standpunkte und der Situation verschiedener Banken in den vorangegangenen Abschnitten ist, dass sich die Banken – je nach dem Ausmaß ihrer Betroffenheit von internationalen Vorschriften und dem Grad ihres Engagements im Bereich KI – für eine stärker harmonisierte Regulierung der KI einsetzen, und zwar sowohl länderübergreifend als auch im Hinblick auf die Anforderungen an das MRM.

Die EU verfolgt einen hybriden Ansatz mit geplanten sektoralen Leitlinien für den Finanzsektor. Einige Teile des EU AI Act wurden als überflüssig eingestuft, da sie bereits vollständig durch die bestehende Bankenregulierung abgedeckt sind. Andere Teile des EU AI Act erfordern jedoch eine spezifische Auslegung im Zusammenhang mit den bestehenden Vorschriften oder stellen neue Vorschriften für den Finanzsektor dar.

Unabhängig vom gewählten Ansatz ist das rasante Tempo der KI-Innovation grundsätzlich unvereinbar mit starren, äußerst detaillierten Regeln und Vorschriften und erfordert stattdessen einen flexibleren, prinzipienbasierten Rahmen. So wurde ChatGPT beispielsweise erst vor etwa drei Jahren eingeführt, und heute stehen KI-Agenten und agentische Systeme an der Spitze der KI-Entwicklung, was verdeutlicht, wie exponentiell dieser Fortschritt mittlerweile verläuft. Basierend auf den Ergebnissen dieses Papiers sollten solche Grundsätze zumindest Leitlinien für die folgenden Bereiche bieten:

- **Nach welchen Kriterien sollten KI-Modelle, KI-Systeme und Anwendungsfälle unterschieden werden?** Die Einstufung als Modell führt zur Anwendung von FS-spezifischen MRM- und Validierungsanforderungen. Dabei sollte auch die Verhältnismäßigkeit berücksichtigt werden, und zwar nicht unbedingt im Sinne der Komplexität und Größe des Instituts, sondern vielmehr im Hinblick auf den jeweiligen Anwendungsfall.
- **Sollte KI als eigenständiger (Unter-)Risikotyp oder als übergeordneter Risikofaktor eingestuft werden?** Eine Einstufung als eigenständiger (Unter-)Risikotyp führt zu zusätzlichem Druck auf die Standardsetzer und die zweite Kontrollinstanz und bekräftigt damit die traditionelle 3LoD-Struktur. Die Einstufung als übergeordneter Risikofaktor ermöglicht einen pragmatischen Ansatz und kann genutzt werden, um innerhalb der Organisation Autonomie zu schaffen und das 3LoD-Modell flexibel zu handhaben. Während Letzteres eine schnellere Umsetzung als Ersteres ermöglicht, muss die Risikoakzeptanz im Allgemeinen höher sein.
- **Wie ist mit KI-Modellen von Drittanbietern umzugehen?** Diese Frage unterstreicht die Notwendigkeit klarer, branchenspezifischer Leitlinien für den Einsatz von Allzweck-KI-Modellen (GPAI) von Drittanbietern im Finanzdienstleistungssektor. Ohne solche Leitlinien stehen die Institute vor der Herausforderung, Transparenzlücken zu schließen – insbesondere hinsichtlich der Praktiken der Anbieter in Bezug auf Daten, Modelle und Cybersicherheit –, während sie gleichzeitig mit einer übermäßigen Abhängigkeit von wichtigen Anbietern und unzureichender Notfallplanung zu kämpfen haben. Daher wurden im EU AI Act unterschiedliche Verpflichtungen für Anbieter und Nutzer eingeführt, doch die Grenzen zwischen diesen Rollen können verschwimmen: Nutzer, die GPAI-Modelle erheblich modifizieren oder in ihre Systeme integrieren, können selbst zu Anbietern werden. Diese Doppelrolle bringt erhöhte regulatorische Verantwortlichkeiten mit sich, darunter Pflichten in Bezug auf Transparenz, Dokumentation und Risikominderung.
- **Wie lässt sich eine wirksame risikobasierte Bewertung der KI-Risiken etablieren und wie lässt sich ein entsprechender Risikoappetit im Sinne einer Anwendungsfallabdeckung festlegen?** Aufgrund der Vielzahl der Anwendungsfälle eines KI-Modells können nicht alle Anwendungsfälle bei der Validierung rechtzeitig umfassend berücksichtigt werden.
- **Welche KI-spezifischen Validationsdimensionen sind erforderlich?** Dimensionen wie Fairness und Erklärbarkeit sind bei der Bewertung von KI-Modellen von besonderer Bedeutung, doch ihre Bewertung ist nicht für alle Modelltypen einheitlich. Neuartige Ansätze wie GenAI und agentische KI erfordern eine Reihe innovativer Validationsansätze. So könnten GenAI-Modelle beispielsweise in anwendungsfallbasierte Architekturtypen unterteilt werden, für die jeweils spezifische Validationsverfahren gelten.

Diese Aspekte sollten eher als Ausgangspunkt für einen Dialog zwischen den Regulierungsbehörden und der Finanzdienstleistungsbranche betrachtet werden und nicht als abschließende Liste.

05

Quellenverzeichnis

Quellenverzeichnis

1 **European Parliament**. EU AI Act: first regulation on artificial intelligence. [Online] 8. Juni 2023. https://artificialintelligenceact.eu/.

2 **White & Case**. AI Watch: Global regulatory tracker - European Union. [Online] 21. Juli 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] 28. Juli 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] Juli 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. Mai 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. Oktober 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. August 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] 4. 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. März 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. Mai 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. Mai 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] Dezember 2025. 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. Juni 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. Juli 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] 6. Februar 2025. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application.

Autoren

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

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

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

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

Dr. Philipp Schröder
Partner, PwC Deutschland
p.schroeder@pwc.com

Dr. Janis Müller
Senior Manager, PwC Deutschland
janis.mueller@pwc.com

© 2026 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft.
Alle Rechte vorbehalten. "PwC" bezeichnet in diesem Dokument die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsgesellschaft der PricewaterhouseCoopers International Limited (PwCIL) ist. Jede der Mitgliedsgesellschaften der PwCIL ist eine rechtlich selbstständige Gesellschaft.

Bei diesem Dokument handelt es sich um eine maschinell erstellte und redaktionell überprüfte Übersetzung der englischsprachigen Originalfassung des White Papers. Im Falle von Abweichungen oder Auslegungsfragen ist allein die englischsprachige Fassung maßgeblich.