RM | REZA MONSHIZADEH
AI · TECHNOLOGY · GOVERNANCE

BOARD BRIEFING REPORT
EUROPÄISCHES BANKING & FINANZMÄRKTE

Wir haben eine Richtlinie, einen Standard und ein Zertifikat — was belegen sie?

Ein Board Briefing Report zur KI-Governance-Architektur — EU AI Act, ISO/IEC 42001, NIST AI RMF, Tests und Nachweise.

Reza Monshizadeh · Monshizadeh.com · 7 Min. Lesezeit

01 SITUATION

Jedes wird als das Rahmenwerk bezeichnet. Keines beantwortet dieselbe Frage.

NEHMEN WIR FOLGENDE SITUATION AN

Das Management legt dem Vorstand vor:

- eine am EU AI Act ausgerichtete KI-Richtlinie,
- ein Zertifizierungsprogramm nach ISO/IEC 42001,
- eine auf dem NIST AI Risk Management Framework basierende Risikomethodik,
- und ein technisches Testverfahren.

> Ein Zertifikat ersetzt keine regulatorische Zuordnungsmatrix.

> Eine Risikobewertung belegt nicht, dass eine Kontrolle funktioniert.

> Ein Testergebnis beweist nicht, dass die richtigen rechtlichen Pflichten identifiziert wurden.

DIE VORSTANDSFRAGE

Kann das Management zeigen, wie rechtliche Pflichten, organisatorische Governance, Risikoentscheidungen und Systemtests in einem einzigen nachvollziehbaren Betriebsmodell zusammenwirken?

02 MANAGEMENT SUMMARY

Drei Orientierungspunkte für den Vorstand.

01

Ein vollständiges KI-Governance-Rahmenwerk hat vier verbundene Ebenen

Recht definiert Pflichten. Das Managementsystem macht Governance wiederholbar. Die Risikomethodik strukturiert Ermessensentscheidungen. Tests und Nachweise zeigen, wie Systeme und Kontrollen funktionieren. Komplementär — nicht austauschbar.

02

Ein Zertifikat ist keine Zuordnungsmatrix

ISO/IEC 42001 kann ein zertifizierbares KI-Managementsystem bereitstellen — sie begründet nicht automatisch die Einhaltung des EU AI Act. **EN 18286** wurde speziell für die Qualitätsmanagementanforderung des AI Act entwickelt.

03

Ein Framework Stack, nicht nur eine Bezeichnung

Der erforderliche Nachweis ist eine nachvollziehbare Linie von der Pflicht über Kontrolle, Test und Verantwortlichen bis zum aufbewahrten Nachweis — eine einheitlich gesteuerte Architektur für den gesamten KI-Bestand und Lebenszyklus.

Ein Institut kann ein Zertifikat kaufen. Eine belastbare Zuordnungsmatrix kann es nicht kaufen.

03 KALIBRIERUNG DER ANTWORTQUALITÄT

Der RAG-Status kalibriert die Qualität der Antwort. Er bewertet nicht das Institut.

DIMENSION	GRÜN	AMBER	ROT
Inventar	Ein einheitlich gesteuerter und abgestimmter KI-Bestand	Ein Inventar besteht, aber Teile der Drittanbieter- oder eingebetteten KI liegen außerhalb	*„Wir wissen, wo unsere KI eingesetzt wird."*
Rechtliche Zuordnung	Zuordnungsmatrix von Anforderungen zu Kontrollen je Anwendungsfall	Eine rechtliche Landkarte besteht, ist aber nicht mit Kontrollen verbunden	*„Wir sind am EU AI Act ausgerichtet."*
Zertifizierungsumfang	Umfang, Ausschlüsse und organisatorische Grenzen sind ausdrücklich benannt	Ein Zertifikat liegt vor, sein Umfang ist aber nicht mit dem KI-Inventar abgeglichen	*„Wir streben eine ISO-Zertifizierung an."*
Risikomethodik	Die Klassifizierung bestimmt den Governance-Pfad	Risikowerte bestehen, verändern aber weder Anforderungen noch Freigaben	*„Wir wenden das NIST-Rahmenwerk an."*
Tests	Akzeptanzschwellen sind an den vorgesehenen Einsatz gekoppelt	Tests werden durchgeführt, sind aber vom Anwendungsfall oder der Entscheidung entkoppelt	*„Der Anbieter hat das Modell getestet."*
Verantwortlichkeit	Eine namentlich benannte Person besitzt die Befugnis zu genehmigen, zu stoppen und zu eskalieren	Gremien sind eingebunden, persönliche Befugnisse bleiben jedoch unklar	*„Das geht durch das KI-Gremium."*
Drittparteien	Nachweise, Änderungspflichten und Prüfungsrechte sind definiert	Vertragsklauseln bestehen, operative Nachweise sind jedoch unvollständig	*„Das ist die Verantwortung des Anbieters."*
Vorstandsberichterstattung	Wirksamkeit, Ausnahmen und Entscheidungen werden berichtet	Der Umsetzungsstatus wird berichtet, die Kontrollwirksamkeit bleibt jedoch unsichtbar	*„Das Programm liegt im Plan."*

GRÜN ist kein Zertifikat. GRÜN ist eine nachvollziehbare Linie von der Pflicht bis zum Nachweis.

04 DER FRAMEWORK STACK

Vier Ebenen. Vier verschiedene Fragen. Ein Betriebsmodell.

01 RECHTSRAHMEN

Was muss das Institut tun?

EU AI Act, DSGVO, DORA, Finanzmarktregulierung sowie anwendbare produkt-, arbeits- und verbraucherschutzrechtliche Anforderungen.

WAS DIESE EBENE ALLEIN NICHT BELEGT
Dass das Institut die Pflichten in wirksame Kontrollen übersetzt hat.

02 MANAGEMENTSYSTEM

Wer steuert KI, mit welchen Verantwortlichkeiten und Prozessen?

ISO/IEC 42001, ISO/IEC 38507 und für die Qualitätsmanagementanforderung des AI Act EN 18286.

WAS DIESE EBENE ALLEIN NICHT BELEGT
Dass jedes KI-System korrekt klassifiziert, rechtlich konform oder technisch vertrauenswürdig ist.

03 RISIKOMETHODIK

Wie werden KI-Risiken identifiziert, bewertet, akzeptiert und behandelt?

NIST AI RMF, ISO/IEC 23894, Modellrisikomethoden und unternehmensweite Klassifizierungsprozesse.

WAS DIESE EBENE ALLEIN NICHT BELEGT
Dass die ausgewählten Kontrollen wirksam funktionieren.

04 TESTS & NACHWEISE

Was zeigt, dass das System und seine Kontrollen wie behauptet funktionieren?

AI Verify, Folgenabschätzungen, Validierung, Robustheits- und Sicherheitstests, Kontrolltests und unabhängige Prüfung.

WAS DIESE EBENE ALLEIN NICHT BELEGT
Dass jede anwendbare Pflicht identifiziert und zugewiesen wurde.

Jede Ebene beantwortet eine andere Frage. Keine beantwortet die jeweils nächste.

05 WER ANTWORTEN SOLLTE

Eine integrierte Managementantwort — geführt von der für unternehmensweite KI, Technologie oder Daten verantwortlichen Führungskraft, gemeinsam mit der für Risiko oder Compliance verantwortlichen Führungskraft.

TYPISCHERWEISE EINZUBINDEN

■ Business-Verantwortung	■ Recht	■ Compliance	■ Risiko
■ Modellrisiko	■ Technologie	■ Daten	■ Cybersicherheit
■ Datenschutz	■ Drittparteirisiko	■ Einkauf	■ Interne Revision

HINWEIS ZUR VERANTWORTLICHKEIT

Die Mitgliedschaft in einem Gremium ist nicht dasselbe wie persönliche Verantwortlichkeit. Die namentlich benannte Person muss die erforderliche Befugnis besitzen, den relevanten KI-Einsatz zu genehmigen, einzuschränken, auszusetzen oder zu eskalieren.

INTERNE REVISION

Die Interne Revision kann Design und operative Wirksamkeit beurteilen. Sie sollte nicht Eigentümerin der Governance der ersten Verteidigungslinie für KI werden.

06 NACHWEISE, DIE DER VORSTAND ANFORDERN SOLLTE

Zehn Artefakte, die die Architektur überprüfbar machen.

01 **Unternehmensweites KI-Inventar**
Ein einheitlich gesteuerter Bestand intern entwickelter, eingekaufter, eingebetteter und von Drittparteien bereitgestellter KI.

02 **Architekturkarte der Rahmenwerke**
Die Beziehung zwischen Recht, Managementsystemen, Risikomethoden, Tests und unabhängiger Prüfung.

03 **Regulatorische Zuordnungsmatrix**
Anwendbare Anforderungen, verbunden mit Richtlinien, Kontrollen, Verantwortlichen, Tests und Nachweisen.

04 **Verantwortlichkeiten und Entscheidungsrechte**
Befugnisse für Genehmigung, Akzeptanz des Restrisikos, Intervention, Aussetzung und Eskalation.

05 **Klassifizierungsmethodik**
Rechtliche Klassifizierung, Wesentlichkeit, Kundenauswirkung, operative Kritikalität und Reversibilität.

06 **Kontrollkarte für den Lebenszyklus**
Anforderungen von Initiierung und Beschaffung über Einführung und Änderung bis zur Außerbetriebnahme.

07 **Folgen- und Risikobewertung**
Eine abgeschlossene Bewertung für einen folgenreichen Anwendungsfall.

08 **Test- und Validierungsnachweis**
Testziele, Methoden, Akzeptanzschwellen, Ausnahmen und Freigabe.

09 **Erklärung zum Zertifizierungsumfang**
Erfasste Rechtsträger, Prozesse, Systeme, Ausschlüsse und Zertifizierungsgrenzen.

10 **Berichtspaket für den Vorstand**
Risikoexposition, Ausnahmen, Vorfälle, wesentliche Änderungen, überfällige Maßnahmen und erforderliche Entscheidungen.

Ein Anwendungsfall sollte von der rechtlichen Klassifizierung bis zum aktuellen Produktionsstatus nachverfolgbar sein — **ohne dass sich Bestände, Definitionen oder Verantwortliche zwischen den Dokumenten ändern.**

07 GOVERNANCE CHECK

WARNSIGNALE

Diese Antworten können in einer Vorstandssitzung beruhigend klingen. Sie sind aber noch nicht entscheidungsfähig.

- ⚠ *„Wir wenden das NIST-Rahmenwerk an.“*
- ⚠ *„Wir sind am EU AI Act ausgerichtet.“*
- ⚠ *„Wir streben eine ISO-Zertifizierung an.“*
- ⚠ *„Der Anbieter hat das Modell getestet.“*
- ⚠ *„Eine Person genehmigt das Ergebnis.“*
- ⚠ *„Das ist durch die KI-Richtlinie abgedeckt.“*
- ⚠ *„Es ist nur ein internes Werkzeug.“*
- ⚠ *„Das Rahmenwerk wird derzeit eingeführt.“*

Keine dieser Aussagen ist notwendigerweise falsch. **Sie reichen lediglich nicht als Grundlage für eine belastbare Vorstandsentscheidung aus.**

08 PATH TO GREEN

Sechs Bedingungen für eine gesteuerte Architektur.

01 Architektur benannt

Die vier Ebenen sind definiert und werden einheitlich verwendet.

02 Zuordnungsmatrix erstellt

Pflichten sind mit Kontrollen, Verantwortlichen, Tests und Nachweisen verbunden.

03 Klassifizierung bestimmt den Pfad

Wesentlichkeit und Rechtsstatus bestimmen die Intensität der Governance.

04 Nachweisstandard definiert

Erforderliche Unterlagen sind vor der Produktionsfreigabe festgelegt.

05 Drittparteien einbezogen

Externe Modelle, Daten, Werkzeuge und Infrastruktur bleiben innerhalb des Governance-Perimeters.

06 Wirksamkeit überwacht

Die Berichterstattung zeigt Kontrollbetrieb, Ausnahmen und Entscheidungen — nicht nur den Programmfortschritt.

NÄCHSTE FRAGE FÜR DEN VORSTAND

Nehmen Sie ein KI-System, das einen Kunden, Mitarbeitenden, eine Transaktion oder einen kritischen Prozess wesentlich beeinflussen kann — kann das Management in einer einzigen Nachweiskette das anwendbare Recht, die verantwortliche, entscheidungsbefugte Person, die genehmigte Risikoentscheidung, die operativen Kontrollen, Testergebnisse, den menschlichen Interventionsweg, Drittparteienabhängigkeiten und den aktuellen Produktionsstatus zeigen?

EXECUTIVE QUESTIONS FOR EUROPEAN BANKING & FINANCIAL MARKETS

Ein Institut kann ein Zertifikat kaufen. Eine belastbare Zuordnungsmatrix kann es nicht kaufen.

Der Vorstand sollte nicht fragen, welches Rahmenwerk das Institut anwendet. Er sollte fragen, ob sich ein folgenreicher KI-Einsatz von der Pflicht bis zum operativen Nachweis lückenlos nachverfolgen lässt.

AUSGEWÄHLTE QUELLEN

Regulation (EU) 2024/1689 — Artificial Intelligence Act.

Regulation (EU) 2026/1744 — Digital Omnibus on AI.

CEN-CENELEC — EN 18286: Quality Management for EU AI Act Purposes.

ISO/IEC 42001:2023 — AI Management Systems.

ISO/IEC 42006:2025 — Certification of AI Management Systems.

NIST — AI Risk Management Framework & Generative AI Profile.

AI Verify Foundation — Testing Framework.

EBA — AI Act Implications for Banking and Payments.

Reza Monshizadeh · Senior Technology Executive · Frankfurt

www.monshizadeh.com