

KI-AUFSICHT UND BOARD ACCOUNTABILITY.

NACHWEIS VOR ZUSICHERUNG.
VERANTWORTUNG VOR ABSICHT.

Es geht nicht mehr nur um das Tool. **Es geht um die Nachweiskette.**



SZENARIO

KI-gestützte Tools unterstützen regulierte Prozesse — sie fassen Informationen zusammen, bereiten Risikosichten vor, bewerten Kontrollen oder formulieren Begründungen.



AUSLÖSER

Wochen später wird der Output von einem Kunden, Prüfer oder Aufseher hinterfragt.



DIE BOARD-FRAGE

Können wir für diesen Output Oversight, Ownership und Human Review nachvollziehbar belegen?



Es geht nicht nur darum, ob das Tool einen Fehler gemacht hat.

Es geht darum, ob wir unsere **Governance belegen können.**



KI-NUTZUNG IST KEIN RANDTHEMA MEHR

Mehr als 85% der großen Banken unter europäischer Aufsicht nutzen KI bereits in irgendeiner Form. Die Frage ist nicht mehr, ob ein Institut KI nutzt — sondern ob diese Nutzung wirksam gesteuert und belegt werden kann.



EVIDENZ VOR MODELLDETAIL

Der Vorstand muss nicht jede Modellspezifikation kennen. Er braucht jedoch Evidenz, dass wesentliche KI-Use-Cases klar verantwortet, überprüft und kontrolliert sind — und bei Bedarf belegt werden können.



ANTWORTQUALITÄT ZÄHLT

Eine starke Antwort ist konkret, aktuell und belegt. Eine schwache Antwort bleibt bei Policy-Aussagen oder Projektstatus stehen.

Evidenzstatus, nicht Institutsbewertung.

	GRÜN Entscheidungsfähig	GELB Teilweise belegt	ROT Nicht entscheidungsfähig
	Aktuelles KI-Use-Case-Inventar existiert.	Inventar existiert, ist aber unvollständig.	„Wir haben eine KI-Policy.“
	Ein klarer Owner pro Use Case ist benannt.	Ownership liegt nur auf Projektebene.	„Das liegt bei IT.“
	Oversight ist definiert und belegt.	Oversight ist beschrieben, aber nicht belegt.	„Der Provider ist verantwortlich.“
	KI-Literacy ist rollenbasiert und dokumentiert.	Training ist generisch, nicht rollenbasiert.	„Training wurde abgeschlossen.“
	Exceptions und Overrides werden überwacht.	Monitoring existiert, Reporting ist fragmentiert.	„Bisher ist nichts passiert.“
	Reporting zeigt Risiko, Wertbeitrag und Kontrollnachweise.	Das Board erhält Statusupdates, aber keine entscheidungsfähige Evidenz.	„Das ist nur ein Copilot.“

GRÜN ist kein Policy-Status. GRÜN ist ein Evidenzstatus.

04

WER ANTWORTEN MUSS

Technologie kann die Plattform verantworten. **Das Business verantwortet die Entscheidungswirkung.**

	CIO / CTO	Plattformarchitektur, Datenfluss und technische Kontrolle. Verantwortet die Deployment-Umgebung.
	Business Owner	Entscheidungswirkung, Prozesseffekt und Output-Validierung. Verantwortet den Use Case und seine Konsequenzen.
	CRO / Compliance / Legal	Risiko, regulatorische Verpflichtungen und Datenschutz. Bewertet, welche regulatorische Relevanz das Modellverhalten hat.
	CISO / Third-Party Risk	Security, Provider-Abhängigkeiten und operative Resilienz. Steuert Risiken aus Provider-Abhängigkeiten und externer Technologie.
	Internal Audit	Unabhängige Prüfung der Nachweiskette. Bestätigt, ob Kontrollen existieren und Dokumentation einer Prüfung standhält.

05

EVIDENZ, DIE DER VORSTAND ANFORDERN SOLLTE

Zehn Artefakte, die eine Antwort überprüfbar machen.

- 01



KI-Use-Case-Inventar
Wo KI eingesetzt wird — Funktionen, Prozesse, Deployment-Status.
- 02



Risikoklassifizierung
Welche Use Cases materiell sind und erhöhte Oversight benötigen.
- 03



Ownership Map
Wer verantwortlich ist — namentlich und funktional, nicht nur auf technischer Ebene.
- 04



Datenklassifizierung
Welche Daten durch KI genutzt oder verarbeitet werden dürfen — erlaubte Nutzung und Datenherkunft.
- 05



Human-Oversight-Design
Wo menschliches Urteil eingreift — Gates, Review, Override.

- 06



KI-Literacy-Nachweis
Rollenbasierte Kompetenz, nicht nur Teilnahmezertifikate.
- 07



Exception- & Override-Log
Ob Probleme sichtbar sind — Overrides, Eskalationen, Incidents.
- 08



Third-Party-Abhängigkeitskarte
Provider-Abhängigkeiten, Konzentrationsrisiko, Exit-Fähigkeit.
- 09



Board-Reporting-Dashboard
Was das Board erhält — zeitnah, strukturiert und ausreichend.
- 10



Decision Rights / Lifecycle-Log
Wer einen Use Case skalieren, einschränken, neu trainieren oder stoppen darf.

Warnsignale.

	„Wir haben eine KI-Policy.“	Eine Policy setzt Absicht. Sie belegt nicht, dass sie auf Use-Case-Ebene umgesetzt, überwacht oder durchgesetzt wird.
	„Das wird von IT gesteuert.“	Technology verantwortet die Plattform. Das Business verantwortet die Entscheidungswirkung. Verantwortung in nur einer Funktion reicht nicht aus.
	„Der Provider ist verantwortlich.“	Vertragliche Pflichten können beim Anbieter liegen. Die Accountability für den Output bleibt beim Institut.
	„Das ist nur ein Copilot.“	Wenn der Output eine regulierte Entscheidung beeinflusst, reduziert das Label nicht die Anforderung. Framing ist keine Kontrolle.
	„Bisher ist nichts passiert.“	Das Ausbleiben dokumentierter Incidents ist kein Kontrollnachweis. Es kann auch bedeuten, dass Monitoring nicht ausreichend greift.
	„Das Tool wird nur intern genutzt.“	Interne Nutzung kann trotzdem regulierte Prozesse, Kundendaten oder Kontrollentscheidungen beeinflussen.
	„Wir haben keine High-Risk-KI-Use-Cases.“	Klassifizierung ersetzt keine Governance, keine Ownership und keine Evidenz.

07

SECHS BEDINGUNGEN FÜR EINE ENTSCHEIDUNGSFÄHIGE ANTWORT

Eine entscheidungsfähige Antwort muss alle sechs abdecken.



Accountability

Klare Ownership für Entscheidungen und Ergebnisse.



Oversight

Human Review gestaltet und belegt.



Transparenz

Erklärbare Nutzung, Grenzen und Kommunikation.



Datendisziplin

Zweck, Qualität, Zugriff und Schutz.



Monitoring

Performance, Drift, Exceptions und Ergebnisse.



Evidenz

Vorlegbar, prüfbar und aktuell.

NÄCHSTE FRAGE FÜR DEN VORSTAND

Welcher KI-Use-Case würde morgen das größte Accountability-Problem erzeugen, wenn ein Kunde, Prüfer oder Aufseher eine Erklärung verlangt?



Assurance ersetzt keine Evidenz. Absicht ersetzt keine belegbare Aufsicht.

Der Vorstand muss nachvollziehen können, was die Institution entscheidet — und wie diese Entscheidung zustande kommt, belegt und geprüft werden kann.