“Vom Hype zum Trusted AI-Betrieb“

Was Finanzdienstleister für den vertrauenswürdigen KI-Einsatz jetzt sicherstellen sollten



17. September 2026

1

Standortbestimmung: KI im Spannungsfeld von Aufsicht und Innovation

KI im Asset & Wealth Management: Status Quo in der DACH-Region 2026

Breit im Einsatz, aber überwiegend Produktivitätstools – Investitionen, Reife und Regulierung ziehen 2026 an

16/73

Privatbanken gelten im AI Advancement Index als „fortgeschritten“ oder „Vorreiter“

KPMG/HSG 2026 [1]

14 %

der in Deutschland aktiven Fondshäuser haben KI im Investmentprozess integriert

Gerle 2026 [2]

> 60 %

der Banken nutzen GenAI (Q1 2025; Ende 2024: ~40 %) – v. a. intern

BaFin/EBA 2026 [3]

Deutschland [2]

- KI vor allem in Marketing & Kommunikation (29 %), Kundenservice und sonstigen Abteilungen (je 16 %)
- Nur 14 % nutzen KI „in allen Prozessen“; fast niemand verzichtet ganz
- Aufsicht: Textgenerierung, Chatbots, Betrugserkennung; kaum Einsatz in Kreditprüfung und Handel [3]

Regulierung (EU/DE) [3] [4]

- BaFin-Orientierungshilfe zu IKT-Risiken bei KI (Dez. 2025) – Bezug auf DORA
- EU AI Act: Transparenzpflichten ab 2. Aug. 2026, Hochrisiko-Anforderungen ab 2. Dez. 2027
- BaFin überwacht KI in regulierten Finanztätigkeiten; Fokus: Erklärbarkeit, Bias, Drittparteirisiko, Herdenverhalten

Kernbotschaft: DACH startet aus einer Position der Stärke, aber mit struktureller Zurückhaltung – der Wertbeitrag ist noch kaum messbar, während die regulatorischen Anforderungen 2026/27 konkret werden.

Quellen: [1] KPMG Schweiz, Clarity on Swiss Private Banks 2026 (68 Banken; KI-Umfrage n = 34; AI Advancement Index der HSG, Juni 2026) · [2] Gerle Financial Communications, Asset-Manager-Umfrage 2026 (Feb.–März 2026, n = 26 ausländische Fondsgesellschaften/Dienstleister am deutschen Markt) · [3] BaFin, Risiken im Fokus 2026 (EBA-Umfrage unter Banken) · [4] BaFin, Pressemitteilung zur KI-Verordnung, 29.07.2026

Finanzinstitute stehen unter massivem Druck aus drei Richtungen gleichzeitig



Aufsicht

- **EU AI Act**
- Digital Operational Resilience Act (**DORA**)
- EZB **CEO-Letter**
- ESA Statement

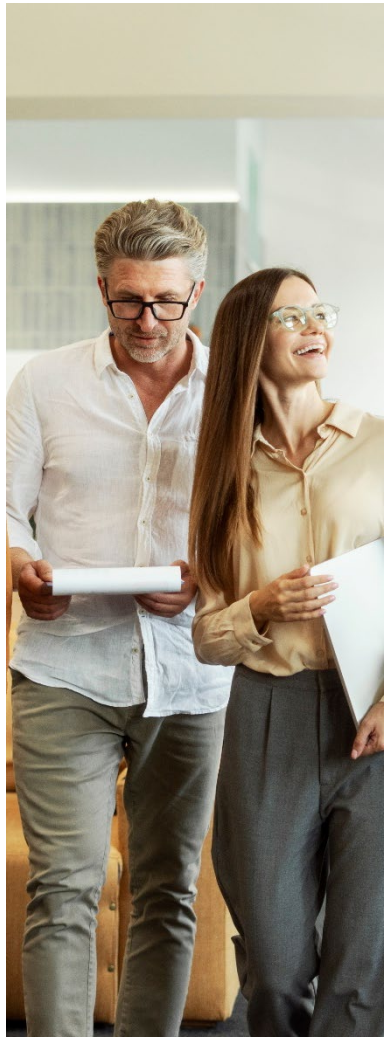
Angreifer

- **Frontier AI** / AI-enabled cybersecurity threats:
  Angriffe in Minuten statt Monaten
- AI agiert eigenständig

Business & Mitarbeiter

- Mitarbeiter mit Wunsch KI zu nutzen
- **Zeitdruck** aus dem Business, um wettbewerbsfähig zu bleiben
- Entstehung von Schatten-KI
- **Budget** für Token und Upskilling

KI-Aufsicht wird konkret: wer überwacht was, und ab wann?



Gilt bereits
seit Feb 2025 / Aug 2025
Verbotene Praktiken · AI Literacy (Art. 4) · GPAI-Pflichten

NEU: 2. August 2026
jetzt scharf
Transparenzpflichten (Art. 50) + voller Sanktionsrahmen + Governance-Struktur

Ab 2. Dezember 2027
verschoben (Digital Omnibus)
Hochrisiko-KI (Anhang III): Kredit- & Bonitätsprüfung

BaFin – KI im regulierten Kerngeschäft
→z. B. Kreditwürdigkeit, Bonität, Versicherungs-Pricing

Prüft ab sofort:
- Transparenzpflichten
- Verbotene KI-Praktiken
- KI-Kompetenz / AI Literacy (Nachweis!)

Sanktionsrahmen (seit 2. Aug 2026)
Verbotene Praktiken: bis 35 Mio. € / 7 %
Hochrisiko & Transparenz: bis 15 Mio. € / 3 %

„Es bleibt viel Raum für Innovation … DORA bietet ein sehr gutes Fundament."
— Jens Obermöller, BaFin · Interview 29.07.2026

Bundesnetzagentur
KI in Support-Funktionen → z. B. HR / Recruiting

✓ **Auftrag = Überwachung, nicht Aufsicht**
risikoorientiert & stichprobenhaft

✓ **„Wer frühzeitig auf uns zukommt** … für den bleiben Strafen die Ausnahme."
— BaFin, 29.07.2026

ESAs Statement sowie EZB Letter
DORA als solides Fundament für KI-Resilienz
— EBA, EIOPA, ESMA, 31.07.2026; EZB 07.07.2026

2

AI Trust by design, AI Compliance by default

Warum ist Vertrauen in KI so wichtig und KI-Governance nicht länger optional – auf einen Blick

Vertrauen in KI ist die Grundlage für Erfolg

Die Leistungsfähigkeit von KI entwickelt sich weiterhin rasant (mit aktuellen Veröffentlichungen wie Gemini 3.1 Pro und Claude Fable 5), dennoch …

… sorgen prominente KI-Fehler weiterhin für Schlagzeilen.

01

Das Betriebsmodell von morgen ist in einer Mensch-KI-Symbiose verankert, dennoch …

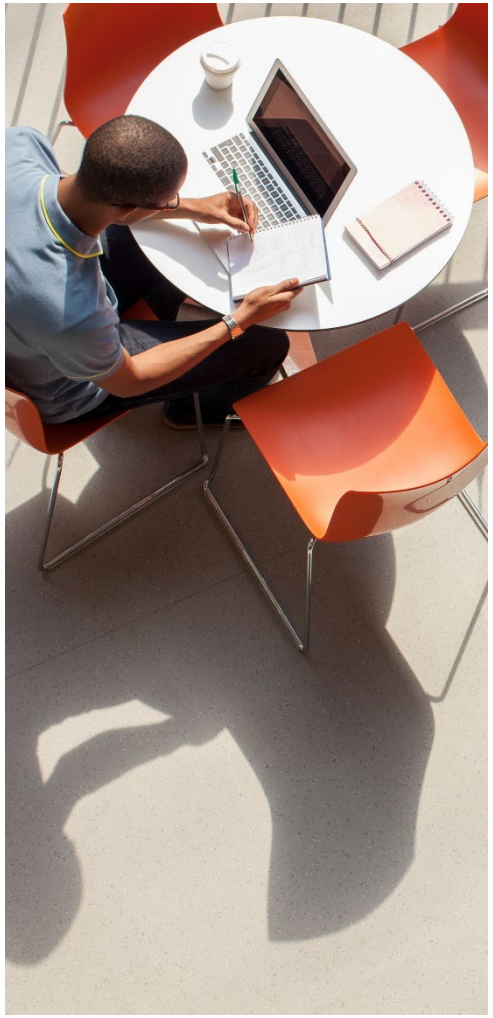
… bleibt die Definition der richtigen Arbeitsteilung — das Ausbalancieren automatisierter Routineprozesse mit menschlicher Verantwortlichkeit für Strategie, Governance und komplexe Fälle — entscheidend.

02

KI-Ambitionen sind weit verbreitet, dennoch …

… werden nur Organisationen, die Vertrauen in großem Maßstab aufbauen, Ambitionen in nachhaltige Transformation umwandeln.

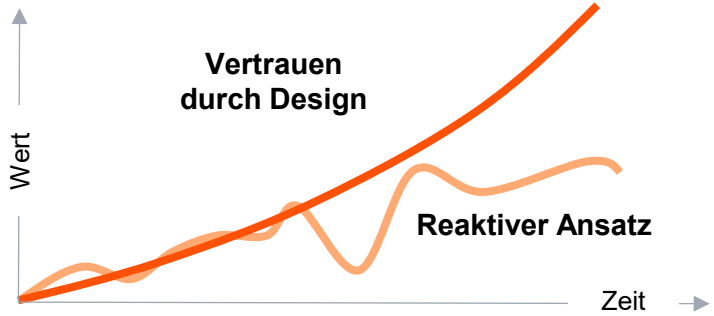
03



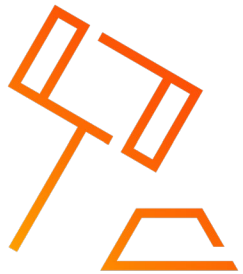
Vertrauen durch Design ist essenziell

Trust by Design integriert Governance von Anfang an direkt in den KI-Lebenszyklus, anstatt sie nachträglich hinzuzufügen. In diesem Modell wird Vertrauen zu einem Innovationsbeschleuniger und schafft nachhaltigen Mehrwert.

Dies steht im Gegensatz zum **reaktiven Ansatz**, bei dem die Innovation die Governance überholt und anfängliche Erfolge zu kostspieligen Misserfolgen werden können.



Der EU AI Act sowie DORA spannen einen initialen Rahmen, um KI unternehmensweit sicher einzusetzen



DORA

vertikale Regulierung
→ IKT-Risiken
→ branchenspezifisch

EU AI Act

horizontale Regulierung
→ KI-Risiken
→ Branchen-übergreifend

DORA

Gemeinsame Ziele identifizieren, Synergien nutzen und doppelte Regulierung vermeiden

- IKT-Risikomanagement
- Governance und Verantwortlichkeiten
- Dokumentation und Nachweispflichten
- Testing und Monitoring
- Vorfallmanagement
- Drittparteienrisiko

- Sicherstellung der digitalen Betriebs- und Cyberresilienz im Finanzsektor
- Harmonisierung der IKT-Risikovorgaben in der gesamten EU
- Reduzierung systematischer Risiken
- Stärkung der Kontrollen über Drittanbieter, insbesondere Cloud-Dienste

EU-KI Act

- Förderung eines sicheren, vertrauenswürdigen und menschenzentrierten Einsatzes von KI
- Minimierung von KI-Risiken durch Risikoregelwerk
- Schutz von Grundrechten und Verbrauchern vor schädlicher KI
- Sicherstellung von Transparenz, Nachvollziehbarkeit und Aufsicht über KI-Systeme



Zusätzlich zu klassischen IKT-Risiken entstehen durch KI auch andere Arten von operationellen Risiken, die bei der Umsetzung der Anforderungen des EU AI Act zu berücksichtigen sind (z. B. Modellrisiken, Prozessrisiken durch erhöhte Autonomie oder Risiken des Einsatzes von KI durch Non-IKT-Dienstleister)

Die „Trust in AI“ Reise zu einer angemessenen KI-Governance ist reifegradabhängig und bringt unterschiedliche Herausforderungen

Reifegrade & PainPoints

Exploring
„Was kann KI für uns tun?“
Erste Erkundung ohne Standards

Schatten-KI
Ohne klare Klassifikation keine Transparenz und Risikobewertung

Operationalizing
„Läuft es stabil im Betrieb?“
Produktion, Governance Designumsetzung

Qualitätsverluste im Betrieb
Mangelnde KI-Kontrollen verursachen Fehlentscheidungen

Transforming
„KI als Geschäftstreiber?
Transformation und automatisiert, proaktive KI-Echtzeitüberwachung

Mensch-Maschine Grenzen
Unkontrollierte KI überschreitet ethische Grenzen

Schlüsselfaktor "KI-Governance"

Aware
„Wissen wir, dass es KI gibt?“
Sporadische Nutzung ohne Struktur.

Unkoordinierter KI
Keine Steuerung ohne Inventar

Experimenting
„Funktioniert es technisch?“
Pilotierung, erste Standardisierung

Unklare Regulatorik
Fehlende Konkretisierung führt zu verzögerten/ineffektiven Maßnahmen

Scaling
„Läuft es überall?“
Skalierung, Governance-Etablierung.

Technische Barrieren
Fehlende Standardisierung bremst die KI-Skalierung

Erfolgreicher KI-Einsatz erfordert eine ganzheitliche KI Governance und adressiert im Zielbild wesentliche Dimensionen

Organisation

Rollen und Schnittstellen

- **Chief AI Officer,**
- **Head of AI Governance,**
- **AI-Engineer […]**

Mit Schnittstellen zu Data Protection, InfoSec, …

Art der KI-Organisation

- **Dezentrales Modell**
- **Hybridmodell**
- **Zentrales Modell**

Drei Verteidigungslinien

1st LoD - Risikoverantwortung:
Identifizierung von Risiken und Entwicklung interner Kontrollen zur Risikominderung

2nd LoD - Risikokontrolle
Überwachung der Wirksamkeit der durchgeführten Maßnahmen

3rd LoD - Risikoabsicherung
Interne Audit-Prozesse zur Sicherstellung der Wirksamkeit der ersten und zweiten LoD

verlangt

Fordert, operationalisiert und prüft

Kultur & Fähigkeiten

- Awareness durch Kommunikation
- Befähigung durch Trainings
- KI-Support durch “Champions”

Governance

1) Leitlinien: Beschreibung des gesamten KI Governance Frameworks

2) Richtlinien: Anforderungen in Abhängigkeit vom KI-Anwendungsfall

3) (Verfahrens-)Anweisungen: Systematische Einführung des KI-Lebenszyklus

Prozesse (Lifecycle)

Onboarding-Prozess

- **Identifizierung**
- **Klassifizierung**
- **Freigabe**
- **Go-Live**

Betrieb &Revalidierung

Periodischer Prozess

Überprüfung und Neubewertung
Risiko- und nutzungsklassenabhängige Neubewertung (Umfang und Häufigkeit)

Ereignisbasiert

Update-Management
Vorfall / Problem Update
Neue Anforderung
(geschäftlich, technisch, regulatorisch)

Kontinuierliches Monitoring

End-of-Life

Auslöser

- Leistung / Business
- Regulatorik
- Technik / Anbieter

Strukturierte Außerbetriebnahme

KI-Anwendungsfall- & Technologie-Inventar (Single Source of Truth)

Das Inventar ist die Basis für…

Plattformen

- MLOps & monitoring tooling
- Automation & agentic controls
- AI risk dashboards & analytics

3

Agentic AI Governance

Kein Sonderregime – aber deutlich höhere Kontroll- und Nachweistiefe

Sobald ein Agent plant, Tools auswählt oder produktiv schreibt, muss Governance nicht nur den Output, sondern die delegierte Handlungsmacht beherrschen.



EU AI Act

Risikoklasse und Pflichten folgen Zweck, Wirkung und Rolle – nicht dem Etikett „Agent“. Systemgrenze, Rollen-/Change-Test, Logs und Aufsicht.



DORA

Autonomie · Tool-/Schreibrechte · dynamische Planung · externe APIs. Change, Tests, Incidents, Provider und Exit.



DSGVO

Identität · Handlungsgrenzen · Human Oversight · End-to-End-Trace · Resilienz. Datenflussgrenzen; Art. 22/35.



Weitere...

MaRisk/KWG · MiFID II/ESMA

IKS, Datenqualität und Validierung. Kontrollen umfassen die gesamte Kette: Orchestrator, Policy, Memory, Identität, Tools, APIs und Sub-Agenten.

Drei wesentliche Fragestellungen beim Einsatz von KI-Agenten



Auftrag und Autonomie: Was soll und darf der Agent tun?
→ Aufgaben, Autonomie, Verantwortung und Human Oversight

Identität und Zugriff: Worauf darf der Agent zugreifen?
→ Agentenidentität, IAM, Tools, Daten, Berechtigungen

Kontrolle und Nachweis: Wie erkennen und begrenzt man Fehlverhalten?
→ Tests, Orchestrierung, Logging, Monitoring, Kill Switch

Welche Compliance-Artefakte sollte eine Organisation nachweisen können?

Daraus resultieren sechs grundlegende Nachweistypen

Der Prüfmaßstab verschiebt sich vom Modelloutput zur kontrollierten Aktion: mit Evidenz vor, während und nach der Ausführung.

1

Systemgrenze & Rollen

Inventar der gesamten Kette: Modell, Orchestrator, Prompt/Policy, Memory, Identität, Tools, APIs, Daten, Zielsysteme und Sub-Agenten.
Rollen-/Change-Test: Betreiber, Anbieter oder neue Anbieterpflicht?

2

Identität & Berechtigung

Eigene technische Identität: keine Shared Credentials, Least Privilege nach Zweck, Zeit, Kontext und Transaktionsart.
Nachweis: Agent–Tool–Daten–Rechte-Matrix, Allowlist, Secret Isolation, SoD, Rezertifizierung.

3

Handlungsgrenzen & Aufsicht

Aktionsklassen von read-only bis finanziell/rechtlich bindend; Wert-, Mengen- und Frequenzlimits.
Freigabe vor irreversibler Wirkung; Aufsicht mit Information, Zeit, Befugnis, Stop, Override und Rückabwicklung.

4

End-to-End-Evidenz

Trace von Trigger, Ziel, Plan und Versionen bis Datenabruf, Agent-Nachricht, Tool-Call, Policy-Entscheid, Freigabe, Aktion und Systemantwort.
Logs datensparsam, geschützt und fristgerecht.

5

Validierung, Change & Resilienz

Task-, Tool-, Workflow-, Orchestrierungs-, Negativ-, adversariale und Failover-Tests.
Revalidierung nach Modell-, Prompt-, Tool-, Rechte- oder Datenänderung; Szenarien inkl. Injection, Loop und Provider-Ausfall.

6

Provider & Incident

DORA-Sicht auf Modell, Plattform, Plugin, API, Datenquelle, Memory und Sub-Agent: Register, Audit, Konzentration, Exit.
Playbook: Tool sperren, Rechte entziehen, Agent in Quarantäne setzen/abschalten, rückabwickeln, sicher neu starten.

Rechtsanker: AI Act Art. 9/12/14/16/26 · DORA ICT-Risiko, Change, Tests, Incidents und Drittparteien · DSGVO Art. 22/35 · MaRisk AT 4 / Modell- und IKS-Anforderungen.

4

Was ist nun zu tun?

Die konkreten Schritte zum Zielbild: Von der strategischen Ambition zur kontinuierlichen Verbesserung

Ambition definieren

- Zielzustand je Fähigkeit Ambitionsniveau & Priorisierung
- Übersicht über KI-Fähigkeiten

01

Verantwortlichkeiten zuweisen

- RACI nach Kompetenzbereich
- Abgrenzung zwischen 1. und 2. LoD
- Ausgangssituation

02

Umsetzung ermöglichen

- Talente, Kompetenzen und Prozesse
- Schnittstellen (Rechtsabteilung, Datenschutzbeauftragter, IT)
- Tooling (AI-GRC, Register)

03

Steuern & vernetzen

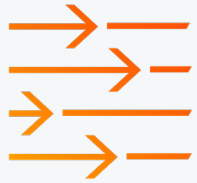
- KI-Ethikkommission Eskalations- & Vorfallswege
- Ausrichtung an Meilensteinen des KI-Gesetzes (AI Act)

04

Kontinuierlich verbessern

- Erkenntnisse aus KI-Vorfällen nutzen
- Benchmarking
- Reifegrad-Steigerung
- FrontierAI

05



Die KI-Dynamik übersteigt rein menschliche Überwachung. Die **Operationalisierung** ist eine **kontinuierliche Schleife**, kein Projekt mit festem Enddatum. Das KI-Betriebsmodell entfaltet seinen Wert nur, wenn es sich kontinuierlich an neue Regulierung, Modelle und Anwendungsfälle anpasst. Der Übergang von der **„Ambitionsdefinition"** hin zu echter **„kontinuierlicher Verbesserung"** ist eine **mehrjährige Disziplin, die von knappen Fachkompetenzen und nachhaltiger Governance abhängt**. Umso wichtiger sind technisch gestützte Prozesse für eine sichere Implementierung und kontinuierliche Resilienz.

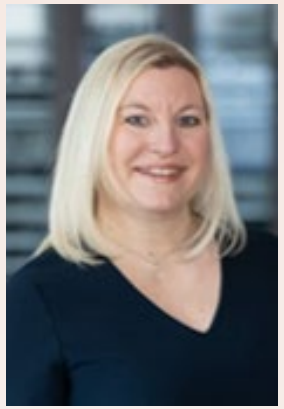
Vom Hype zum Trusted AI-Betrieb: Der Weg beginnt heute.

Viel Erfolg auf Ihrer KI-Reise!

© 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.

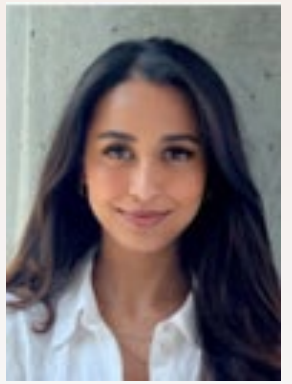
pwc.com

Ihre Ansprechpartner:



Alexandra Naumann

Director
alexandra.naumann@pwc.com
+49 170 7601590



Sounia Arbib

Manager
sounia.arbib@pwc.com
+49 171 3884024