FIRM
Frankfurt Institute for
Risk Management and Regulation

November 2025

WHITE PAPER

# Agentic AI in Risk & Compliance: Von Automatisierung zu intelligenter Governance

Von Dr. Sebastian Fritz-Morgenthal, Dr. Jochen Papenbrock,
und Dr. Mark Währisch

FIRM
Frankfurt Institute for
Risk Management and Regulatio

# Inhalt


Management Summary ..... 3

Vom Automatisieren zum Orchestrieren:
Ein Paradigmenwechsel im Risikomanagement ..... 3

Strategische Chancen für Banken ..... 4

Herausforderungen und Gestaltungsfelder ..... 4

Der Weg zur Umsetzung – sechs zentrale Handlungsfelder ..... 5

Vom Experiment zur Resilienzarchitektur ..... 6

A. Agentic AI versus klassische AI: Wie sich die Technologie verändert hat ..... 7

B. Reifegrad von Agentic AI-Anwendungen in Risk & Compliance bei Finanzinstituten ..... 11

C. Zentrale Herausforderungen und Lösungsansätze bei der Umsetzung von Agentic AI ..... 14

D. Schritte zur erfolgreichen Integration von Agentic AI und kritische Erfolgsfaktoren ..... 22

FIRM
Frankfurt Institute for
Risk Management and Regulatio

WHITEPAPER

# Agentic AI in Risk & Compliance: Von Automatisierung zu intelligenter Governance

Von Dr. Sebastian Fritz-Morgenthal und Dr. Jochen Papenbrock

## Management Summary

Künstliche Intelligenz verändert das Risikomanagement der Banken tiefgreifend. Nach Jahren der regelbasierten Automatisierung eröffnet der Aufstieg sogenannter Agentic AI-Systeme eine neue Dimension: KI-Modelle, die nicht nur analysieren, sondern eigenständig Entscheidungen vorbereiten, Aufgaben priorisieren und Prozesse koordinieren. Damit verschiebt sich der Fokus von der reaktiven Datenauswertung hin zur proaktiven Steuerung komplexer Risiko- und Compliance-Prozesse.

***Der Fokus verschiebt sich von der Datenauswertung zur proaktiven Steuerung.***

FIRM beschäftigt sich im Rahmen des Round Tables Artificial Intelligence mit der Frage, wie Finanzinstitute diese Entwicklung gestalten können – mit Blick auf Governance, Datenqualität, Aufsichtsfähigkeit und kulturelle Voraussetzungen. Die zentrale Erkenntnis der bisherigen Diskussionen lautet:

**Agentic AI ist kein technologischer Hype, sondern ein strategischer Hebel für Resilienz, Effizienz, Innovation und regulatorische Sicherheit.**

### VOM AUTOMATISIEREN ZUM ORCHESTRIEREN: EIN PARADIGMENWECHSEL IM RISIKOMANAGEMENT

Klassische AI-Lösungen konzentrieren sich auf spezifische Aufgaben – etwa Scoring, Fraud Detection oder Reporting. Agentic AI hingegen agiert wie ein intelligenter Ko-Akteur: Sie kombiniert generative Modelle (Large Language Models, Foundation Models) mit regelbasierten Verfahren, bezieht externe Datenquellen ein und kann Handlungen selbstständig initiieren.

***Agentic AI agiert wie ein intelligenter Ko-Akteur.***

Das ermöglicht eine neue Qualität in der Prozesssteuerung. Anwendungsfelder reichen von der automatisierten Dokumentenprüfung über das kontinuierliche Monitoring regulatorischer Anforderungen bis zur proaktiven Risikoanalyse auf Basis unstrukturierter Informationen.

Der entscheidende Unterschied: Agentic AI lernt, interpretiert und reagiert kontextsensitiv – innerhalb klar definierter Kontrollgrenzen. Damit wird aus einer Technologie zur Effizienzsteigerung ein Instrument, das Risikoerkennung, Entscheidungsunterstützung und Compliance-Sicherung in Echtzeit verbindet.

***Agentic AI lernt innerhalb klar definierter Kontrollgrenzen.***

## STRATEGISCHE CHANCEN FÜR BANKEN

### a) Operative Effizienz und Qualität

Agentic AI reduziert manuelle Prüftätigkeiten, standardisiert Routineprozesse und ermöglicht eine erhebliche Beschleunigung in Bereichen wie KYC, AML oder regulatorischem Reporting. Damit steigt nicht nur die Geschwindigkeit, sondern auch die Konsistenz und Nachvollziehbarkeit der Ergebnisse.

### b) Frühwarnsysteme und vorausschauende Steuerung

Im Risikomanagement schafft Agentic AI die Grundlage für proaktive Risikoidentifikation. Durch die Analyse heterogener Datenströme – von Markt- und Transaktionsdaten bis zu geopolitischen Signalen – werden Abweichungen oder emerging risks frühzeitig erkannt und automatisiert bewertet.

***Agentic AI schafft die Grundlage für eine proaktive Risikoidentifikation.***

### c) Compliance-by-Design

Die Technologie erlaubt es, regulatorische Anforderungen direkt in die Prozesslogik einzubetten. Audit-Trails, automatische Dokumentation und Explainability-Mechanismen werden Teil des Systems – nicht nachgelagerte Pflichten. So wird Compliance zu einem integrierten Qualitätsmerkmal.

### d) Resilienz und Governance

Agentic AI unterstützt Banken beim Aufbau robuster Governance-Strukturen. Virtuelle „Compliance- oder Risk-Officer-Avatare“ können Risiken in Echtzeit überwachen, Reports generieren und Eskalationsprozesse auslösen – immer im Zusammenspiel mit menschlicher Kontrolle. Dadurch entsteht eine neue Form der organisatorischen Resilienz.

***Es entsteht eine neue Form der organisatorischen Resilienz.***

## HERAUSFORDERUNGEN UND GESTALTUNGSFELDER

Der Weg zur produktiven Nutzung von Agentic AI ist anspruchsvoll. Die größten Herausforderungen liegen nicht in der Technologie, sondern in den Rahmenbedingungen:

***Technische und organisatorische Rahmenbedingungen zählen zu den größten Herausforderungen.***

- Regulatorik und Governance:

  Die Vorgaben aus EU AI Act, DORA und den EBA-Leitlinien schaffen einen neuen Ordnungsrahmen. Entscheidend ist, Compliance nicht als Bremse, sondern als Voraussetzung für vertrauenswürdige Innovation zu begreifen.

- Technologische Voraussetzungen:

  Historisch gewachsene IT-Landschaften und fehlende Datenportabilität erschweren die Integration. Zukünftige Architekturen bzw. Agentic-AI-Ökosysteme müssen modular, interoperabel und souverän sein – unabhängig von einzelnen Hyperscalern.

- Organisation und Kultur:

  Der produktive Einsatz erfordert neue Rollenprofile wie AI Product Owner oder Context Engineer und ein tiefes Verständnis für KI-basierte Entscheidungsprozesse. Nur wenn Mitarbeitende die Funktionsweise und Grenzen der Systeme verstehen, kann Vertrauen entstehen.

Empfehlenswert ist daher ein klarer Governance-first-Ansatz: Technologie, Regulatorik und Organisation müssen von Anfang an integriert gedacht werden.

***Empfehlenswert ist ein Governance-first-Ansatz.***

## DER WEG ZUR UMSETZUNG – SECHS ZENTRALE HANDLUNGSFELDER

**1. Strategische Zielbilder entwickeln**

AI nicht als Einzelinitiative verstehen, sondern als Bestandteil der langfristigen Risiko- und Transformationsstrategie.

**2. Use-Cases gezielt priorisieren**

Statt vieler Pilotprojekte wenige, aber geschäftsrelevante Leuchttürme mit hohem Lernpotenzial realisieren – etwa in Compliance oder Onboarding.

**3. Governance-Strukturen etablieren**

Interdisziplinäre Steuerungskreise aus Risk, Compliance, IT und Legal aufbauen; Zuständigkeiten klar verankern.

**4. Explainability als Designprinzip verankern**

Auditierbare Modelle und nachvollziehbare Entscheidungswege sind Grundvoraussetzung für regulatorische Akzeptanz.

**5. Kompetenzzentren und AI Literacy fördern**

Zentrale Hubs bündeln Know-how, definieren Standards und sorgen für breites Verständnis im gesamten Institut.

**6. Souveränität durch AI-Ökosysteme sichern**

In industriell und lokal verfügbare AI-Ökosysteme investieren sowie mit eigenen Anwendungen nutzen und damit die eigene Zukunftsfähigkeit sichern.

## VOM EXPERIMENT ZUR RESILIENZARCHITEKTUR

***Aufbau lernfähiger Organisationen, die Risiken antizipieren.***

Agentic AI steht am Beginn einer neuen Ära datengetriebener Steuerungssysteme. Ihr Nutzen entfaltet sich dort, wo Technologie und Governance ineinandergreifen – im Aufbau von resilienten, lernfähigen Organisationen, die Risiken nicht nur managen, sondern antizipieren.

Die Expertendiskussionen im FIRM-Round Table zeigen, dass es drei strategisch wichtige Vorteile für Institute gibt, die früh handeln:

- **Lern- und Erfahrungsvorsprung** in Validierung, Governance und regulatorischer Zusammenarbeit
- **Produktivitätsgewinne** durch intelligente Automatisierung standardisierter Abläufe
- **Vertrauensvorsprung** durch nachweislich kontrollierte, auditierbare KI-Systeme

Mit diesem Positionspapier geben die Koordinatoren des Round Tables Artificial Intelligence einen Überblick zu den Funktionsweisen von Agentic AI sowie zum Reifegrad in den Anwendungen für Risikomanagement und Compliance in Banken Sie zeigen auf, wo es Herausforderungen gibt und welche Lösungsansätze die Umsetzung unterstützen. Zudem zeigen sie die Schritte zur erfolgreichen Integration von Agentic AI im Risikomanagement von Banken.

# A. Agentic AI versus klassische AI: Wie sich die Technologie verändert hat

## WAS UNTERSCHEIDET AGENTIC AI VON KLASSISCHER AI?

Künstliche Intelligenz (AI) in der Finanzbranche hat sich in den letzten Jahren stark weiterentwickelt – von regelbasierten Modellen hin zu hochkomplexen, generativen Systemen. Während klassische AI primär mit strukturierten Daten arbeitet und für deterministische Aufgaben wie Betrugserkennung oder Bonitätsscoring eingesetzt wird, bezeichnet Agentic AI künstliche Intelligenzsysteme, die Aufgaben autonom ausführen, eigenständige Entscheidungen treffen und sich dynamisch an neue Bedingungen anpassen können:

| Merkmal | Klassische AI | Agentic AI |
|---|---|---|
| Steuerung | Regelbasiert, vordefinierte Abläufe | Autonom, selbststeuernd, lernend |
| Anpassungsfähigkeit | Funktioniert nur in bekannten Szenarien | Dynamisch, passt sich neuen Daten/Situationen an |
| Entscheidungsfindung | Reaktiv, folgt Vorgaben | Proaktiv, entwickelt eigene Strategien |
| Komplexität | Ideal für spezialisierte Aufgaben | Geeignet für komplexe Prozesse |
| Skalierbarkeit | Stark eingeschränkt, geringer Ressourcenbedarf | Hoch, durch mehrere spezialisierte Agenten, hoher Rechenaufwand, neue Infrastrukturanforderungen |
| Datenformate | Überwiegend strukturierte Daten | Unstrukturierte und strukturierte Daten |
| Ansatz | Regelbasiert, deterministisch | Probabilistisch, kontextbasiert |
| Fähigkeiten | Analyse, Vorhersage | Generierung, Interaktion, Schlussfolgerung |
| Flexibilität | Gering (Modellwechsel nötig bei neuen Tasks) | Hoch (Zero-/Few-Shot Learning, Transfer Learning) |
| Einsatzbereiche | Scoring, Transaktionsprüfung | Agentic AI ermöglicht meiner Meinung nach mehr: Autonom operierende (Teil-)Prozesse im Risikomanagement, z. B. Szenarioentwicklung, aktive Portfolioüberwachung etc. |
| Erklärbarkeit / Überprüfbarkeit (wichtig für Revision, Wirtschafts-Prüfung, Bankaufsicht) | Hoch (regelbasiert, ermöglicht weitestgehende Nachvollziehbarkeit) | Eingeschränkt, Bedarf an Explainability, kontinuierlicher Validierung bzw. Überwachung & Audit-Trails |

Dabei nutzt Agentic AI unter anderem Generative AI, Large Language Models (LLMs) und Foundation Models (FMs), um auf Basis unstrukturierter Daten dynamisch wahrscheinlichkeitsgewichtete Aussagen zu treffen und Inhalte zu generieren, kann diese aber auch mit Klassischen AI-Modellen kombinieren. Damit lassen sich unter anderem Anwendungen wie z. B. Chatbots für die Interaktion mit Kunden entwickeln, die sich für Nutzer „menschlicher" verhalten als auf klassischen statistischen Methoden beruhende Verfahren.

## AGENTIC AI ADRESSIERT STRUKTURELLE SCHWÄCHEN TRADITIONELLER SYSTEME

Ein zentrales Unterscheidungsmerkmal ist die Fähigkeit von Agentic AI, große Mengen unstrukturierter Informationen – etwa Dokumente, E-Mails oder Gesprächsprotokolle – effektiv zu verarbeiten. Dies eröffnet in der Bankenpraxis neue Möglichkeiten, etwa bei der Automatisierung von Compliance-Prozessen, dem Client Onboarding oder der Interpretation komplexer regulatorischer Anforderungen. Agentic AI übernimmt hier Aufgaben, die bislang menschliches Expertenwissen erforderten – mit 24/7-Verfügbarkeit und kontextsensitiver Interaktion über verschiedenste Kanäle hinweg.

Agentic Frameworks erweitern regelbasierte wie Generative AI-Systeme wesentlich, indem sie die Fähigkeiten zur Prozessautomatisierung auf ein neues Level heben. Sie unterstützen autonome AI-Agenten dabei, komplexe Geschäftsprozesse nicht nur sequentiell auszuführen, sondern auch zu koordinieren, anzupassen und sich selbstständig zu optimieren – weit über die Grenzen klassischer Prozessautomatisierung hinaus.

## AGENTIC FRAMEWORKS ERWEITERN GENAI ZUR PROZESSAUTOMATISIERUNG

Mit fortschrittlichen Agentic-Konzepten wie z.B. Chain-of-Thought-Prompting, Retrieval-Augmented Generation (RAG) und ReAct (siehe Tabelle) lässt sich Generative AI von einem Tool zur Inhaltserzeugung zu einem Entscheidungsagenten weiterentwickeln. Diese Frameworks ermöglichen komplexe, mehrstufige Aufgaben wie z. B. die Übersetzung von Orderbüchern oder die automatisierte Erstellung und Auditierung regulatorischer Reports – inkl. durch Anwender durchgeführte (Stichproben-)Kontrollen und Explainability als integralen Bestandteil der Systemarchitektur.

| Begriff | Kurzerläuterung | Zugriff auf Wissen | Steuerung | Quelle |
|---|---|---|---|---|
| Chain Thought Prompting | Das LLM teilt seine Gedankenkette Schritt für Schritt mit, wodurch latente logische/arithmetische Fähigkeiten aktiviert und Antworten nachvollziehbar werden. | **Intern** – nutzt nur in Modellparametern gespeichertes Wissen | Linear (Denken → Antwort) | Chain-of-Thought Prompting Elicits Reasoning in Large Language Models **Zum Link** |
| Retrieval-Augmented Generation (RAG) | Vor der Antwort ruft ein Retriever passende Dokumentpassagen ab und gibt sie mit der Nutzerfrage an das LLM; reduziert Halluzinationen und hält Wissen aktuell. | **Extern** – greift auf eine Dokument- oder Vektor-Datenbank zu | Linear (Retrieval → Antwort) | Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks **Zum Link** |
| ReAct Prompting | Kombiniert Reasoning-Spuren mit konkreten Aktionen in einer Schleife; nach jedem Denk-Schritt kann das Modell z.B. suchen, rechnen oder einen MCP-Server[1] aufrufen und das Ergebnis im nächsten Schritt nutzen. | **Hybrid** – intern + über Aktionen extern | Iterativ (Denken ↔ Handeln) | ReAct: Synergizing Reasoning and Acting in Language Models **Zum Link** |

## KONSEQUENZEN FÜR FINANZINSTITUTE

Agentic AI eröffnet Banken vielfältige neue Möglichkeiten, wie individuelle Kundenberatung, automatisiertes Onboarding, effiziente Dokumentenprüfung bis hin zu komplexen strategischen Entscheidungen. Die Systeme steigern Produktivität und Sicherheit, minimieren Fehlerquellen und eröffnen neue Handlungsspielräume für Finanzinstitute. Damit trägt Agentic AI maßgeblich zur Automatisierung, Qualitätssicherung und Innovationskraft im Bankenwesen bei, insbesondre auch im Bereich Risk Management und Compliance. Diese autonomen AI-Systeme agieren eigenständig, lernen kontinuierlich und orchestrieren komplexe Prozesse in Echtzeit, was Effizienz und Sicherheit deutlich steigert.

## RISK MANAGEMENT

Agentic AI kann im Prinzip eingesetzt werden, Risiken frühzeitig zu erkennen und selbstständig Gegenmaßnahmen einzuleiten. Beispiele dafür sind:

- Echtzeit-Betrugserkennung durch Analyse großer Datenmengen und sofortige Blockierung auffälliger Transaktionen.
- Automatisierte Kreditwürdigkeitsprüfungen und dynamische Portfolioanpassungen basierend auf laufender Marktbeobachtung.
- Proaktives Risikomanagement durch vorausschauende, datenbasierte Analysen statt nur nachträglicher Auswertung.

[1] MCP-Server: Model Context Protocol Server ist ein Dienst, der es AI-Agenten ermöglicht, mit externen Systemen und Datenquellen zu interagieren. Er fungiert als Vermittler, der AI-Modelle mit der digitalen Außenwelt verbindet, indem er ihnen Zugriff auf Ressourcen, Tools und Informationen außerhalb ihres eigenen Wissensbereichs ermöglicht.

## COMPLIANCE

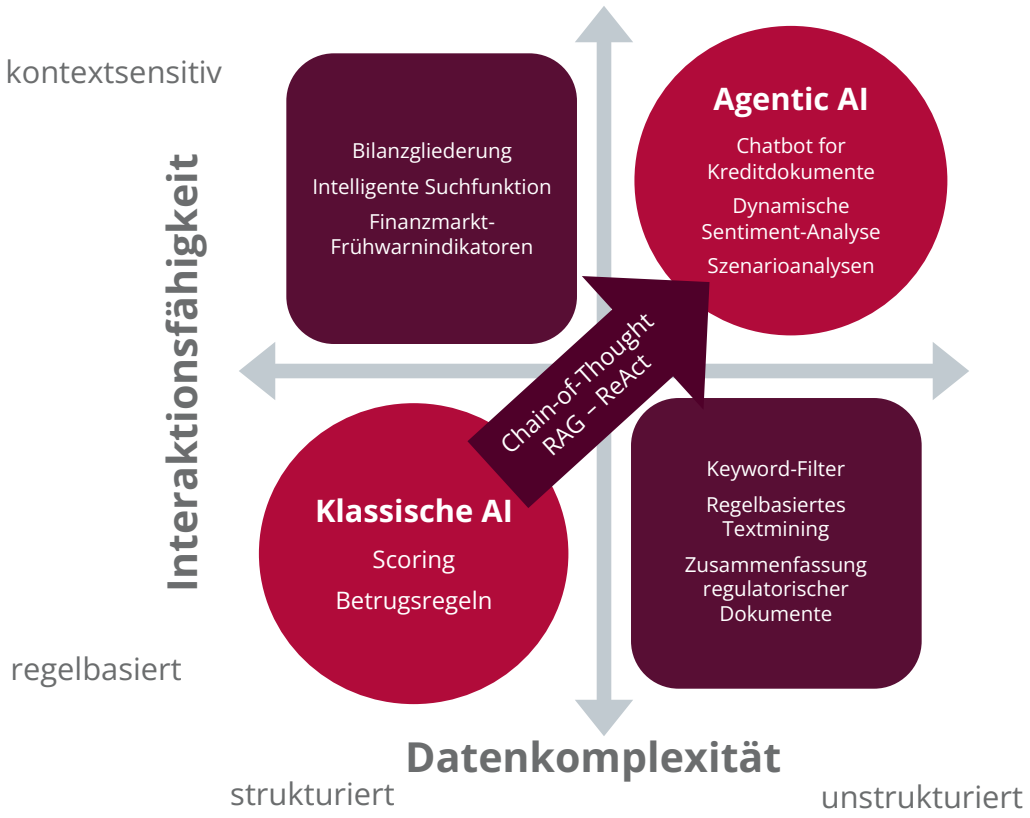
Im Bereich Compliance nutzt Agentic AI fortlaufende Überwachung und automatisierte Abläufe zur Einhaltung gesetzlicher Vorgaben, wie z. B.:

- Automatisierte Überprüfung und Dokumentation regulatorischer Anforderungen (z. B. KYC-Prozesse, Datenschutz, AI Act).
- Erkennung von Verstößen und Erstellung von Berichten ohne manuelles Eingreifen (z. B. AML-Kontrollen).
- kontinuierliche Anpassung an neue regulatorische Standards und Gesetze.

Besonders im Risk- und Compliance-Kontext können durch Agentic AI sogenannte „virtuelle Rollen" entstehen – z. B. ein Risk Officer Avatar, der mit umfassender Domänenlogik ausgestattet ist, regulatorische Entwicklungen auswertet, Reports aufbereitet oder Entscheidungsvorlagen generiert. Dabei agiert Agentic AI zunehmend nicht nur als „Tool", sondern als agentischer Ko-Akteur, eingebettet in Entscheidungsprozesse mit klaren Eskalations- und Kontrollmechanismen.

Für Banken ergeben sich daraus einige strategische Konsequenzen wie z. B. die Möglichkeit von End-to-End-Automatisierung bislang fragmentierter Prozesse, neue Governance- und Kontrollparadigmen bis hin zu Paradigmenwechseln in der Organisationslogik.

### VON KLASSISCHER AI ZU AGENTIC AI – SYSTEMVERGLEICH UND SYNERGIEPOTENZIALE



# B. Reifegrad von Agentic AI-Anwendungen in Risk & Compliance bei Finanzinstituten

## DER ÜBERGANG VON EXPERIMENT ZU STRATEGISCHER RELEVANZ

Agentic AI durchläuft aktuell in vielen Finanzinstituten den Wandel von einem explorativen Innovationsfeld hin zu einem strategischen Hebel mit substanzieller Wirkung auf Effizienz, Risiko- und Compliance-Prozesse sowie Kundeninteraktion. Die Bandbreite der Reifegrade ist dabei groß – von Ad-hoc-Pilotprojekten bis hin zu ersten produktiven, integrierten Systemlösungen. Entscheidend für Fortschritt ist weniger der technologische Reifegrad, sondern vielmehr die Fähigkeit zur orchestrierten Umsetzung – insbesondere in standardisierten, datenintensiven Bankprozessen.

## DREI STUFEN DES AGENTIC AI-REIFEGRADS IN BANKEN

Die institutionelle Reife im Umgang mit Agentic AI lässt sich in drei charakteristische Entwicklungsphasen gliedern:

**1. Experimentierphase**

- Isolierte Proof-of-Concept (PoC) Studien, begrenzt auf einfache Use Cases wie Textzusammenfassungen oder Regel-Chatbots
- Fokus auf interner Exploration – häufig in Innovations- oder IT-Teams
- Hürden: Legacy-IT, fragmentierte Datenlandschaften, fehlende Governance-Strukturen

**2. Skalierung & Integration**

- Übertragung erfolgreicher PoCs in erste produktive Anwendungsarchitekturen, Integration in Business-Workflows z. B. bei Client Onboarding, Abweichungsanalysen, Audit-Prozessen
- Agentic AI kombiniert verschiedene Tools, um End-to-End-Prozesse zu automatisieren
- Erste bereichsübergreifende Teams aus Business, IT und Compliance werden etabliert

**3. Strategischer Produktiveinsatz**

- Agentic AI-Anwendungen sind tief in Betriebsmodelle eingebettet
- Systeme agieren als virtuelle Assistenzinstanzen (z. B. Virtueller Risiko-/Compliance-Analyst, Kopilot Regulatorik)
- Hohe Automatisierung für Standardprozesse / Massenverarbeitung bei gleichzeitiger menschlicher Kontrollmöglichkeit
- Fokus auf Domänenmodelle und erklärbare Anwendung von Agentic-AI zur Absicherung regulatorischer Anforderungen

## TYPISCHE ANWENDUNGSFELDER IN RISK & COMPLIANCE

Zentrale Agentic AI-Anwendungen in Banken fokussieren sich derzeit auf wiederholbare, strukturierte Prozesse mit hoher Regelbindung und hohem manuellem Aufwand. Dabei liegt momentan noch ein großer Teil der skalierbaren möglichen Use Cases in Risk & Compliance im Bereich Effizienz. Beispiele:

- **Compliance-Automatisierung:** Geldwäsche-Reports, DORA-Audits, Transaktionsüberwachung
- **Kreditvergabe & Onboarding:** Automatische Dokumentenprüfung, Gap-Analysen, What-If-Szenarien
- **Research:** Orderbuch-Übersetzungen, Verarbeitung von Finanznachrichten, Markt-Sentiment-Analysen
- **Stresstests & Szenarien:** Konzeptionierung geopolitischer oder klimabezogener Extremszenarien mithilfe semantischer Vernetzung und Knowledge Graphs (dies ist ein Use Case Beispiel jenseits klassischer Effizienz hin zu Anwendungen, die momentan nicht oder nur mit unverhältnismäßig hohem Aufwand möglich wären).

## HERAUSFORDERUNGEN UND BEGRENZUNGEN

Auch bei zunehmender Reife bleiben zentrale Limitierungen bestehen:

- **Regulatorik:** Unklare Zuständigkeiten bei externen, verbrauchernahen Anwendungen; mögliche EU-Zertifizierungspflichten für „High Risk"-Systeme außerhalb der bereits regulierten Systeme.
- **Datenqualität:** Fortschrittliche Use Cases scheitern oft an mangelnder bzw. unvollständiger Dateninfrastruktur oder Konsistenz in den Quellsystemen.
- **Explainability:** Für entscheidungsrelevante Anwendungen im Risikomanagement sind Erklärbarkeit, Nachvollziehbarkeit, Fairness and Transparenz zwingend notwendig. Technologisch und konzeptionell ist das jedoch häufig noch nicht standardisiert lösbar.
- **Kostenstruktur:** Hoher Aufwand für Computer- und Modellbetrieb, besonders für kleinere Häuser nur mit Partnern tragfähig.

## ZENTRALE AUSSAGE

Der Reifegrad institutioneller Agentic AI-Nutzung hängt von vielen harten und weichen Faktoren ab und von der Fähigkeit zur skalierbaren Umsetzung in bestehenden Prozessen, flankiert von starker Governance, klarer Rollenverteilung und robuster Infrastruktur.

Industrielle Plattformen für die Entwicklung und den Betrieb von AI-Modellen unterstützen Institute beim Übergang von der Experimentierphase bis zur strategischen Integration:

- Experimentierphase: Schnelles Prototyping mit Referenz-Workflows und -Architekturen
- Skalierende und integrierte Microservices als produktionsreife Inferenzschicht

### REIFEKURVE DER AGENTIC AI-NUTZUNG IN RISK & COMPLIANCE

| Reifegrad | Experiment | Skalierung | Strategische Integration |
|---|---|---|---|
| Typische Use Cases | • Chatbot-Prototypen<br>• Textklassifikation (E-Mail-Routing u. Ä.)<br>• Einfache Reporting-Automatisierung | • Produktionsreife KYC/AML-Assistenten<br>• Serieller Dokumenten-Review (Reg-Reports)<br>• Generative Berichte für Audit-Teams | • End-to-End-Szenario-Modellierung in Echtzeit<br>• Prädiktive Compliance-Kontrollen<br>• Autonome Kontroll-Workflows |
| Voraussetzungen | • Pilot-Datensätze & Sandbox<br>• Kleine cross-funktionale Task-Force (IT + Fachbereich)<br>• Vorläufige Compliance-Checks | • AI-Rollen & Center of Excellence<br>• Erweiterte Datenpipelines & Feature-Stores<br>• Governance-Framework inkl. Modell-Monitoring | • Integriertes Data-Lakehouse & Model-Serving-Infrastruktur<br>• Klare RACI-Matrizen & Richtlinien<br>• Regulatorische Freigaben/Audit-Trail |
| Hauptherausforderungen | • Datenqualität & -zugang<br>• Abbildung domainspezifischer Logiken<br>• Fehlende Standards | • Kosten & Performance beim Wachstum<br>• Management von Halluzination und Guardrails<br>• Change-Management im Fachbereich | • Dokumentation Vertrauenswürdigkeit & Fairness<br>• Organisatorischer Kultur-Wandel<br>• Kontinuierliche Qualitätskontrolle |
| Verantwortliche Stakeholder | • IT-Innovationsteam Fachbereich<br>• Risk/Compliance-Ansprechperson | • IT-Operations<br>• Risk/Compliance-Teams<br>• Business-Units<br>• Data-Governance-Board | • C-Level (CRO/CIO)<br>• Compliance-Leitung<br>• IT-Security<br>• Datenethik-Komitee<br>• Externe Regulatoren |
| Meilenstein/ Etappenziel | PoC abgeschlossen | Governance-Framework etabliert | Continuous Auditing & Control |

# C. Zentrale Herausforderungen und Lösungsansätze bei der Umsetzung von Agentic AI

## TRANSFORMATION MIT HINDERNISSEN

Die Implementierung von Agentic AI in Finanzinstituten verspricht im ersten Schritt signifikante Effizienzgewinne – doch der Weg dorthin ist komplex. Im Zentrum stehen nicht nur technologische Hürden, sondern strukturelle, regulatorische, organisatorische und unternehmenskulturelle Spannungsfelder. Erfolgreiche Umsetzung erfordert klare Verantwortlichkeiten, belastbare Governance-Modelle, ein tiefes Verständnis regulatorischer Implikationen sowie die Bereitschaft der Mitarbeitenden, sich auf die neue Technologie einzulassen und sie in den Arbeitsalltag zu integrieren.

Im zweiten Schritt erwarten wir Neuerungen im Geschäfts- und Betriebsmodell von Banken, die mit herkömmlicher Technologie nicht möglich wären. Beispielhaft seien hier genannt:

- Die Ableitung physischer Risiken im Immobilienportfolio einer Bank aus Echtzeit-Satelliten oder sich bildenden Extrem-Wetterereignissen.
- Sensitive Frühwarnindikatoren als Hinweise auf idiosynkratische oder systemische Finanzkrisen.
- Verknüpfungen Verhaltens- und Prognosedaten von systemrelevanten Finanzinstitutionen und deren mögliche Auswirkungen auf den Finanzmarkt.
- Anwendungen, die weit über das aktuelle Verständnis der technologischen Möglichkeiten hinausgehen, wie z. B. logisches Reasoning über Domain Wissen eines ganzen Fachbereichs (z. B. „AI-Risk Officer“)

## 1. TECHNOLOGISCHE GRUNDLAGEN UND DATENINFRASTRUKTUR

### HERAUSFORDERUNG:

Fragmentierte Architekturen, fehlende Portabilität und eingeschränkte Datensouveränität

Die Integration von Agentic AI in Banken scheitert bislang oft nicht an der Vision, sondern an technologischen Grundlagen. Insbesondere die Verfügbarkeit qualitativ hochwertiger, strukturierter wie unstrukturierter Daten sowie die Fähigkeit, Agentic AI-Modelle flexibel, sicher und  und im Rahmen aufsichtsrechtlicher Compliance zu betreiben, stellen zentrale Hürden dar. Viele Banken kämpfen mit verteilten Datensilos, historisch gewachsenen Architekturen und monolithischen Legacy-Systemen, die für Agentic AI nicht ausgelegt sind.

Zwei Themen gewinnen in diesem Kontext an strategischer Bedeutung: Portabilität des Tech Stacks und Souveränität über Daten und Modelle.

## PORTABILITÄT: TECHNOLOGISCHE UND STRATEGISCHE FLEXIBILITÄT ALS KRITISCHER ERFOLGSFAKTOR

Moderne Agentic AI-Anwendungsarchitekturen benötigen eine hohe Interoperabilität – sowohl zwischen verschiedenen Modelltypen (Open-Source vs. Closed-Source, Foundation vs. Domain Model) als auch zwischen Plattformen, Rechenumgebungen und Datenquellen. Fehlende Portabilität führt zu klassischen Vendor-Lock-in-Effekten, eingeschränkter Innovationsfähigkeit und unnötig hohen Integrationskosten.

Konkret bedeutet Portabilität heute:

- API-first-Infrastrukturen: Die Fähigkeit, LLMs über standardisierte Schnittstellen wie OpenAPI, LangChain oder HuggingFace Hub anzusprechen und in modulare Microservice-Architekturen zu integrieren.

- LLM-Virtualisierung: Die Möglichkeit, verschiedene Modelle (GPT-4, Claude, LLaMA, Mistral etc.) austauschbar und workload-spezifisch auf einer Plattform zu orchestrieren, ohne tiefgreifende Anpassungen in der Applikationslogik.

- Edge- & Hybrid-Betrieb: Die Fähigkeit, Agentic AI-Workloads je nach Sicherheitsanforderung zwischen Public Cloud, Private Cloud und On-Premises flexibel zu verschieben – auch im Hinblick auf regulatorische Anforderungen zur Datenlokalisierung.

- Modularisierung via MCP-Server-Architektur: Der Einsatz eines Model Context Protocol (MCP) Servers erlaubt die zentrale Steuerung verteilter Agentic AI-Module entlang eines konfigurierbaren Pipelinesystems – z. B. Retrieval Layer, RAG-Augmentierung, Agent Router, Prompt Normalizer, Logging Adapter. Unterschiedliche Use Cases (z. B. Dokumentenreview vs. Compliance Reporting) können dabei mit dedizierten Modulkombinationen adressiert werden, was Wiederverwendbarkeit und Anpassbarkeit verbessert.

Beispiel: Für hochregulierte Prozesse kann ein „Compliance Setup“ mit einem auditierbaren Logging-Modul, regelbasierter Prompt Filterung und On-Prem-Inferenz aktiviert werden, während für interne Wissensarbeit ein „Productivity Setup“ auf cloudbasierte LLMs mit flexibler Tool-Integration setzt.

## SOUVERÄNITÄT: KONTROLLE ÜBER DATEN, MODELLE UND INFRASTRUKTUR

Neben technologischer Portabilität ist Souveränität – insbesondere im Sinne von Datenresidenz, Datenschutz, Schutz vor Abhängigkeiten und regulatorischer Steuerbarkeit – ein entscheidendes Kriterium für Banken. Agentic AI-Systeme operieren in hochsensiblen Bereichen (z. B. Risikobewertung, Compliance, Kreditvergabe) und verarbeiten teils personenbezogene oder marktbeeinflussende Informationen.

Souveränität umfasst heute mehrere Dimensionen:

- Datenlokalisierung: Die Fähigkeit, Modelle vollständig in lokalen (z. B. air-gapped) Rechenzentren zu betreiben – inklusive GPU/TPU-Ressourcen für Inferenz.
- Regelbasierte Kontrollinstanzen: Zentral steuerbare Richtlinien für Zugriff, Logging, Model Updates und Audit-Trails.

- Explainability-Infrastruktur: Mechanismen zur lückenlosen Rückverfolgung von Prompt-Flows, Modellantworten und Retrieval-Schritten (Chain-of-Thought, RAG-Logs).Customizable Model Backends: Fähigkeit, Foundation-Modelle mit bankeigenem Wissen anzureichern, ohne sie an Drittanbieter oder US-Hyperscaler abgeben zu müssen – z. B. durch Fine-Tuning in geschlossenen Rechenumgebungen und/oder mit synthetischen Daten.

## KONSEQUENZ FÜR BANKEN: ARCHITEKTUREN UND AGENTIC AI PLATFORMEN DER NÄCHSTEN GENERATION

Ein tragfähiger Agentic AI-Tech Stack in Banken muss heute drei Ziele vereinen:

1. Interoperabilität durch modulare, API-first-Architekturen mit Unterstützung für diverse LLM-Anbieter und -Formate.

2. Souveränität durch vollständige Kontrolle über Infrastruktur, Datenfluss und Modellbetrieb – unabhängig vom Hyperscaler.

3. Produktionsreife durch standardisierte MCP-Setups für unterschiedliche Use-Case-Klassen (z. B. „Compliance“, „Onboarding“, „Audit“) und deren zentrale Steuerung innerhalb einer skalierbaren Agentic AI-Umgebung.

Banken, die diese Prinzipien umsetzen, sind in der Lage, Agentic AI-Anwendungen schnell zu skalieren, regulatorisch sicher zu betreiben und gleichzeitig auf künftige technologische Entwicklungen flexibel zu reagieren – sei es durch neue Anbieter, veränderte Preismodelle oder disruptive Modellarchitekturen.

Eine Full-Stack-Plattform für Agentic AI ermöglicht die Erstellung, Bereitstellung und kontinuierliche Verbesserung autonomer, ressourcenfähiger AI-Agenten für Finanzinstitute. Diese Architektur integriert leistungsfähige AI-Modelle (oftmals sogenannte ‘Open-Source’ oder ‘Open-Weight’ Foundation-Modelle wie Llama, Mistral, Nemotron[2], gpt-oss, Qwen, etc.), eine kuratierte Sammlung von Microservices, standardisierte Tools und Blueprints, die das Rückgrat des Daten- und AI-Flywheels bilden und sowohl operative Effizienz als auch schnelle Innovation ermöglichen.

### ZENTRALE MODELLE

- Leistungsstarke offene Reasoning-Modelle wie z.B. die Llama Nemotron Reasoning-Familie für fortschrittliche, Tool-unterstützende AI, die programmieren, komplexe Mathematik durchführen, APIs dynamisch aufrufen und domänenspezifische Aufgaben ausführen kann.

- Domänenspezifisch angepasste Modelle, die über spezielle Microservices zugänglich und einfach individualisierbar, bereitstellbar und feinjustierbar für spezifische Unternehmensanforderungen sind, wie z. B. Kundenservice, Dokumentenanalyse oder finanzielle Entscheidungsunterstützung.

### MICROSERVICES

- Vorgefertigte und optimierte Inferenz-Microservices, die API-basierten Zugang zu den neuesten Foundation Modellen auf einer AI-Datacenter-Infrastruktur (Cloud, hybrid, on-prem) bieten, samt Tools für Prompt-Tuning, überwachtes Feintuning und Wissensabruf.

[2] https://www.nvidia.com/en-gb/ai-data-science/foundation-models/nemotron/

- Modulare Komponenten für Datenverarbeitung, Training, Benchmarking und Evaluierung, die als „Motor“ im Daten-Flywheel fungieren.

- Modell-Evaluierungsfunktionen und Modell-Leitplanken: Kontinuierliche Benchmarking- und Sicherheitsüberwachungs-Microservices, die das Modellverhalten optimieren und Zuverlässigkeit beim agentischen Entscheiden sicherstellen.

**TOOLS UND BLUEPRINTS**

- Toolkits zur Profilierung, Optimierung und Koordinierung von Teams aus AI-Agenten mit Telemetrie und Inferenz-Analytik.

- Agentenbasierte Blueprints und Referenz-Workflows: Verbinden Wissensdatenbanken und Unternehmensdaten mit AI-Agenten, ermöglicht autonome Wahrnehmung, Schlussfolgerung und Handlung; integriert Retriever für multimodalen Datenabruf und Toolkits für agentenbasierte intelligente Systeme.

- Vorgefertigte Entwicklerumgebungen und Workflows, um agentische AI-Lösungen schnell hochzufahren.

- Unterstützung gängiger Open-Source-Stacks, die in die unternehmensorientierten Agenten-Blueprints eingebunden sind.

**AUFBAU DES DATEN- UND AI-FLYWHEELS**

- Das Daten-Flywheel ist ein positiver, kontinuierlicher Zyklus, in dem Agenteninteraktionen Daten erzeugen (Benutzeranfragen, Ergebnisse, Produktionslogs), die kuratiert, für iteratives Feintuning genutzt und evaluiert werden, um zukünftige Modelle zu verbessern.

- Stufen des Flywheels:

  - Datenkuratierung (Sammeln/ Reinigen von Praxisdaten)
  - Modellanpassung (Feintuning mit unternehmens- oder nutzerspezifischen Daten)
  - Evaluierung (Benchmarking, Guardrail-Prüfungen)
  - Agenten-Orchestrierung (verbesserte Modelle über Microservices ausrollen)
  - Feedback-Integration (Reales Nutzerfeedback fließt kontinuierlich in den Zyklus zurück).

**END-TO-END-STACK-BEISPIEL**

- Verbindung verschiedener Datenquellen (Dokumente, Video, Unternehmensdaten)

- Einsatz von Reasoning-Modellen wie z.B. Nemotron Inferenz-Microservices, Orchestrierung der Workflows, Optimierung mit Data Flywheel Referenz-Workflows sowie automatisiertes Benchmarking und Monitoring über Modell -Evaluatoren und Modell-Leitplankensysteme.

- Kontinuierliche Verbesserung durch das Flywheel: Mit Handlungen der Agenten werden Ergebnisse und Feedback protokolliert, Modelle werden nachtrainiert und neu ausgerollt, wodurch das gesamte System im Laufe der Zeit immer intelligenter und zuverlässiger wird.

Dieser Full-Stack-Ansatz ermöglicht echte agentische Workflows, bei denen resiliente, bewusste und sich kontinuierlich verbessernde AI eine Schlüsselrolle in Unternehmen, Industrie und der fortgeschrittenen Automatisierung einnimmt.

Die vollständige Agentic AI-Plattform ist darauf ausgelegt, eine umfassende, skalierbare und effiziente Lösung für die Entwicklung, Bereitstellung und Optimierung von AI-Agenten bereitzustellen. Diese Plattform integriert verschiedene Modelle, Microservices und Werkzeuge, um einen nahtlosen Workflow für den Aufbau und die Wartung von AI-Systemen zu schaffen, die autonom denken, planen und handeln können.

Im Kern der Agentic AI-Plattform steht ein cloud-natives Framework für End-to-End Unterstützung der Entwicklung, Anpassung und Bereitstellung von generativen AI-Modellen erleichtert und folgende Schlüsselkomponenten umfasst:

- **Modell-Kurator**: Dieses Tool ist verantwortlich für die Vorbereitung groß angelegter, qualitativ hochwertiger Datensätze für das Pre-Training generativer AI-Modelle.

- **Modell-Customizierung:** Ein Hochleistungs-Mikroservice, der die Feinabstimmung und Anpassung großer Sprachmodelle (LLMs) für spezifische Anwendungsfälle vereinfacht.

- **Modell-Evaluator:** Dieser Mikroservice automatisiert die Bewertung benutzerdefinierter LLMs und Retrieval-Augmented Generation (RAG)-Modelle anhand verschiedener Benchmarks und menschlicher Bewertungen.

- **Retriever**: Bietet latenzarme, hochdurchsatzfähige Informationsabfrage, die Echtzeit-Informationsbereitstellung ermöglicht.

- **Modell-Leitplankensystem:** Sorgt für die Genauigkeit, Angemessenheit und Sicherheit von AI-Interaktionen, indem es Dialog- und Inhaltsmoderation verwaltet.

- **Modell-Startrampe:** Vereinfacht das Management und die Organisation von AI-Modellen und -Diensten.

Sämtliche Komponenten können mitunter viel Rechenkapazität benötigen, sind aber stark parallelisierbar und daher ideal geeignet für GPU-beschleunigte Verarbeitung, um große Datenmengen effizient zu handhaben und den Zeitraum der Produktionseinführung der Modelle und Agenten stark verkürzt, was die 'POC-Falle' minimiert.

### INFERENCE MICROSERVICES

Sie bieten eine Sammlung von produktionsreifen Inferenz-Mikroservices, die für die schnelle, sichere Bereitstellung und Skalierung von generativen AI- und Inferenz-Workloads entwickelt wurden. Sie kombinieren die Flexibilität von Open-Source-Deployment mit der Benutzerfreundlichkeit von Managed Services und unterstützt nahtlose Integration über Cloud-, Rechenzentrums- und Edge-Umgebungen hinweg.

## 2. REGULATORIK, ZERTIFIZIERUNG UND GOVERNANCE

### HERAUSFORDERUNG:

Die regulatorischen Anforderungen – z. B. aus EU AI Act, GDPR, DORA oder EBA-Rahmenwerken – sind dynamisch und teils widersprüchlich. Besonders externe, verbrauchernahe Agentic AI-Systeme bzw. generell Foundation-Modelle könnten in Zukunft der „Hochrisiko"-Klassifizierung mit Zertifizierungspflichten unterliegen.

### LÖSUNGSANSÄTZE:

- Aufbau interdisziplinärer Governance-Strukturen mit klarer Rollenzuweisung (Business, Compliance, IT, Modellvalidierung).
- Frühzeitige Einbindung von Risiko- und Rechtsabteilungen in Use Case-Entwicklung.
- Einsatz transparenter, kontinuierlich validierter, auditierbarer sowie mglw. zertifizierter Modelle mit Explainability-Komponenten (Audit-Trails, Modellrevision).

## 3. EXPLAINABILITY, ZUVERLÄSSIGKEIT UND KONTROLLE

### HERAUSFORDERUNG:

Agentic AI kann plausible, aber fehlerhafte Antworten erzeugen („Halluzinationen") – in risikosensitiven Prozessen wie Kreditvergabe oder regulatorischem Reporting ist dies nicht akzeptabel (wohlwissend, dass menschliche ebenfalls Fehler machen).

### LÖSUNGSANSÄTZE:

- Kombination aus Agentic AI und klassischer deterministischer AI sowie finale Freigabe durch einen Menschen zur Validierung (hybride Modellansätze).
- Nutzung erklärbarer Agentik (z. B. Chain-of-Thought, Retrieval-Augmented-Generation) und standardisierte Prompt-Engineering-Muster.
- Defintion von domainspezifischen Semantik Data Layers, in dem das Fachwissen und die Logik für eine Inferenz deterministisch flexibel gespeichert wird.
- Modell-Testing und Simulationsumgebungen vor dem Go-live , kontinuierliche Qualitätssicherung und Validierung im Betrieb.

## 4. KOSTEN UND SKALIERBARKEIT

### HERAUSFORDERUNG:

Der Betrieb großer Modelle ist rechenintensiv und teuer – insbesondere für mittelgroße Institute wirtschaftlich schwer tragbar.

**LÖSUNGSANSÄTZE:**

- Einsatz spezialisierter, mittelgroßer LLMs (z. B. GPT-3.5, Claude Instant) mit optimalem Kosten-Nutzen-Verhältnis.
- Nutzung skalierbarer Cloud-Infrastrukturen mit Multi-Modell-Flexibilität zur Vermeidung von Vendor Lock-in.
- Partnerschaften mit Technologieanbietern zur gemeinsamen Nutzung von Ressourcen und Innovationskraft, selbstverständlich unter Berücksichtigung, die Übereinstimmung mit der GDPR im Allgemeinen sowie die Integrität von Kundendaten im Besonderen sicherzustellen.

## 5. ORGANISATION, ROLLEN UND KULTURWANDEL

**HERAUSFORDERUNG:**

Der produktive Einsatz von Agentic AI erfordert nicht nur neue Technologien, sondern auch neue Rollen, Verantwortlichkeiten und Fähigkeiten. Oft fehlt es an AI Literacy in der Breite der Organisation.

**LÖSUNGSANSÄTZE:**

- Aufbau zentraler Agentic AI-Kompetenzzentren mit Verantwortung für Rollout, Governance und Best Practices
- Ausbildung neuer Rollenprofile (z. B. Agentic AI Product Owner, Context Engineer)
- Förderung funktionsübergreifender Teams, um Business-Know-how mit Data Science zu verbinden
- Einsatz strukturierter Change-Management-Prozesse sowie niedrig-schwelliger unternehmensweiter Schulungen, um Akzeptanz, Verständnis und Vertrauen in der gesamten Organisation aufzubauen

### ZENTRALE AUSSAGE

Die erfolgreiche Implementierung von Agentic AI in Finanzinstituten ist kein rein technisches Vorhaben – sie erfordert ein strukturiertes Zusammenspiel aus technologischer Exzellenz, regulatorischer Absicherung und tiefgreifender organisatorischer Transformation. Entscheidend ist dabei nicht nur der Zugang zu LLMs oder der Aufbau neuer Infrastrukturen, sondern vor allem die Fähigkeit, Agentic AI-Anwendungen sicher, effizient und skalierbar in hochregulierte Bankprozesse zu integrieren.

**Fünf Hebel sind dabei ausschlaggebend:**

1. **Technologie-Architekturen der nächsten Generation:** Zukunftsfähige Plattformen sind modular, interoperabel und souverän – sie erlauben den Betrieb verschiedenster LLMs (open/closed source), unterstützen hybride Deployment-Modelle und sichern regulatorische Anforderungen durch kontrollierbare Audit-Trails, Explainability-Mechanismen und Datenlokalisierung.

2. **Regulatorik mitdenken, nicht umgehen:** Der EU AI Act, GDPR, DORA und EBA-Leitlinien erfordern eine frühzeitige Verzahnung von Business, Compliance, IT und Legal. Transparente Modellsteuerung, zertifizierbare Prozesse und dokumentierte Entscheidungswege sind die Grundlage für vertrauenswürdige Anwendungen im Hochrisikobereich.

3. **Explainability als Designprinzip:** In risikosensitiven Anwendungsfeldern wie Kreditvergabe, KYC oder regulatorischem Reporting ist die Erklärbarkeit kein „Nice-to-have", sondern eine regulatorische und operative Pflicht. Techniken wie Retrieval-Augmented Generation (RAG), Chain-of-Thought oder hybride Modellarchitekturen mit menschlichem Review stellen die Brücke zwischen Innovationsfähigkeit und Kontrollierbarkeit dar.

4. **Kostenbewusstsein durch intelligente Modellwahl:** Nicht jeder Anwendungsfall benötigt GPT-5 Pro. Mittelgroße, spezialisierte Modelle (z. B. Claude Instant, GPT-3.5, Mistral) liefern heute ein exzellentes Kosten-Nutzen-Verhältnis – insbesondere für dokumentenzentrierte, repetitive Aufgaben. Flexible Plattformarchitekturen ermöglichen einen selektiven Einsatz teurer Modelle, wo erforderlich.

5. **Organisatorische Transformation verankern – auch kulturell:** Der produktive Einsatz von Agentic AI erfordert neue Rollenprofile (z. B. Agentic AI Product Owner, Prompt Engineer), funktionsübergreifende Teams und eine breite AI Literacy in der Organisation. Ein zentraler Enabler: Kompetenzzentren, die Umsetzung, Governance und Schulung orchestrieren – und damit den kulturellen Wandel begleiten.

**Die übergreifende Erkenntnis: Agentic AI wird dann zum strategischen Hebel, wenn Banken Technologie, Regulatorik und Organisation gemeinsam denken – und in konkreten, skalierbaren Use Cases zur Umsetzung bringen.**

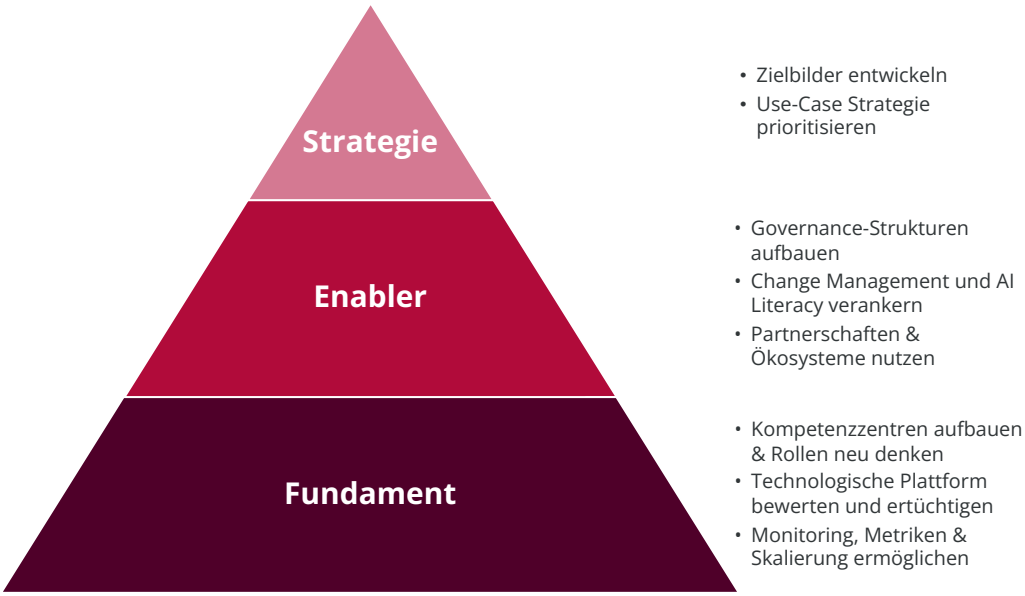
### HERAUSFORDERUNGEN & LÖSUNGSHEBEL FÜR AGENTIC AI IN BANKEN

# D. Schritte zur erfolgreichen Integration von Agentic AI und kritische Erfolgsfaktoren

## WARUM JETZT? – DIE NOTWENDIGKEIT ZUM HANDELN

Agentic AI bietet Banken einen strategischen Hebel zur Effizienzsteigerung, besserer Kundeninteraktion und Automatisierung kritischer Prozesse. Darüber hinaus öffnet es das Potential für neue innovative Produktentwicklungen und Geschäftsprozesse, die mit klassischen Verfahren nicht oder nur schwerlich umsetzbar wären. Doch spontane Einzelinitiativen reichen nicht aus. Ohne klare Governance, gezielte Kompetenzentwicklung und eine koordinierte Use-Case-Strategie droht der Verbleib in einer ineffizienten Pilotphase. Wer früh strategisch vorgeht, profitiert doppelt – durch schnelleren Wissenserwerb und greifbaren Business Impact.

### ACHT KRITISCHE ERFOLGSFAKTOREN FÜR EINE ERFOLGREICHE AGENTIC AI-TRANSFORMATION




## IM DETAIL

### 1. STRATEGISCHE ZIELBILDER ENTWICKELN

- Agentic AI nicht als Technologie, sondern als Transformationsmotor verstehen
- Zielbilder entlang geschäftsrelevanter Hebel (z. B. Kosten, Geschwindigkeit, Kundenbindung, Innovation) definieren
- Frühzeitig Business-Verantwortliche und Regulatorik einbinden

### 2. USE-CASE-STRATEGIE PRIORISIEREN

- Fokus auf 1–2 „heroische“, aber umsetzbare Use Cases mit hohem Hebel und Lernpotenzial

- Keine breite PoC-Landschaft – gezielte Tiefe statt Streuung für Generierung von Traktion mit Schaffung von Wertbeiträgen durch AI

- Effizienz-orientierte Standardprozesse mit Wiederholungspotenzial im Fokus (z. B. Compliance, Onboarding), gleichzeitig Offenheit für Produkt – und Prozess-innovationen

### 3. GOVERNANCE-STRUKTUREN AUFBAUEN

- Einrichtung eines Agentic AI-Steuerungskreises mit Vertretern aus Business, IT, Risk, Compliance, Datenschutz

- Klare Ownership für Policy, Technologie, Validierung und Risikobewertung verankernUmgang mit regulatorischer Unsicherheit vorbereiten (z. B. EU AI Act, DORA)

### 4. CHANGE-MANAGEMENT UND AI LITERACY VERANKERN

- Aufklärungskampagnen, um Vertrauen in Agentic AI zu fördern

- Trainings für Fachbereiche und Management (z. B. AI-Awareness, Prompting, Risiken)

- Fachbereichsverantwortliche zu Botschaftern für Agentic AI machen

### 5. PARTNERSCHAFTEN UND ÖKOSYSTEME NUTZEN

- Zusammenarbeit mit Hyperscalern, spezialisierten Technologieanbietern und RegTechs

- Open-Source-Communities und Kooperations-Initiativen zur Skalierung nutzen

- Austausch mit Aufsichtsbehörden aktiv suchen

### 6. KOMPETENZZENTREN AUFBAUEN & ROLLEN NEU DENKEN

- Zentrales Agentic AI-Kompetenzzentrum für Standardisierung, Know-how-Sicherung und Schulung

- Etablierung neuer Rollen wie Prompt Engineer, AI Product Owner oder Agentic AI Trainer

- Aufbau funktionsübergreifender Chapter & Squads (insb. in Agile@Scale-Organisationen) mit Sandboxes für Erfahrungsaufbau und Test-Umgebungen

### 7. TECHNOLOGISCHE PLATTFORM BEWERTEN UND ERTÜCHTIGEN

- Infrastrukturfähigkeit für LLMs und agentische Architekturen prüfen (Cloud-Readiness, Sandbox-Konzepte)

- Multi-Modell-Strategie (Vermeidung von Lock-in) vorbereiten

- Zugang zu synthetischen Daten und Vector-Datenbanken schaffen

## 8. MONITORING, METRIKEN & SKALIERUNG ERMÖGLICHEN

- Erfolg nicht an Anzahl der PoCs messen, sondern an tatsächlichem Business Impact und Adoptionsgrad
- Skalierbare KPI-Modelle entwickeln (z. B. Reduktion Bearbeitungszeit, Qualitätsindikatoren, Risikoquoten)
- Frühzeitig Feedback- und Iterationszyklen etablieren

### ZENTRALE AUSSAGE

Der Weg zu einer skalierbaren, regulatorisch konformen und strategisch wertstiftenden Agentic AI-Nutzung beginnt mit Klarheit im Zielbild, Mut zu fokussierten Leuchtturmprojekten und einer orchestrierten Umsetzung über Business-, IT- und Risikoabteilungen hinweg. Nur wer jetzt gezielt investiert, baut nachhaltige Fähigkeiten für die nächste Stufe der digitalen Transformation auf.

**DIE AUTOREN:**

**Dr. Sebastian Fritz-Morgenthal**
Co-Koordinator FIRM Round Table Artificial Intelligence

Risk Manager, Advisor, Lecturer and Researcher
Managing Director Advisense

**Dr. Jochen Papenbrock**
Co-Koordinator FIRM Round Table Artificial Intelligence

**Dr. Mark Währisch**
Mitglied FIRM Round Table Artificial Intelligence

Managing Director - Head of Data & AI, Scope Group