



Whitepaper Agentic AI

AGENTIC AI IM BANKING

Von der Automatisierung zur Autonomie



WHITEPAPER

AGENTIC AI IM BANKING

Von der Automatisierung zur Autonomie

AUTOREN

Dr. Torsten Stuska
Patrick Natus
Thomas Linnemann
Michael Oettinger

www.moonroc.de

IMPRESSUM

AGENTIC AI IM BANKING Von der Automatisierung zur Autonomie

Ein Artikel von MOONROC Advisory Partners GmbH und dem
MOONROC Institute of Economic Research (MIER)
in Zusammenarbeit mit der oetti-ds GmbH

Auflage 03/2026
Herausgeber
MOONROC Advisory Partners GmbH
Steinsdorfstraße 14
80538 München
E-Mail: company@moonroc.de
Internet: www.moonroc.de

Registergericht
Amtsgericht München
HRB 191134 / Steuernummer 143.164.01148
Sitz der Gesellschaft: München
USt-ID - DE276206799
Umsatzsteuer-Identifikationsnummer gemäß §27 a UstG
Inhaltlich Verantwortlicher gemäß §6 MDStV: Patrick Natus

EXECUTIVE SUMMARY

Die Finanzindustrie steht an der Schwelle einer fundamentalen Transformation, die in ihrer Tragweite mit der Einführung des Online-Bankings oder der mobilen Finanzdienste vergleichbar ist. Während das letzte Jahrzehnt von der Digitalisierung der Kundenschnittstellen und der regelbasierten Automatisierung (Robotic Process Automation, RPA) geprägt war, markiert der Aufstieg der **Agentic AI** (agentenbasierten Künstlichen Intelligenz) den **Übergang von der bloßen Automatisierung starrer Prozesse zur echten kognitiven Autonomie**.

GENAI (GENERATIVE KI) HAT DER WELT GEZEIGT, DASS MASCHINEN NEUE INHALTE ERSTELLEN KÖNNEN; AGENTIC AI BEWEIST NUN, DASS SIE IN KOMPLEXEN UNTERNEHMENSUMGEBUNGEN INTELLIGENT HANDELN KÖNNEN.

Dieses Whitepaper richtet sich an Vorstände, Strategieleiter, Bereichsleiter, IT-Leiter und Risikomanager in Banken, die verstehen müssen, wie sich diese Technologie von bisherigen KI-Wellen unterscheidet und wie sie wertstiftend eingesetzt werden kann. Es bietet eine Analyse des Paradigmenwechsels hin zu KI-Systemen, die nicht nur auf Eingabeaufforderungen (Prompts) reagieren, sondern proaktiv Ziele verfolgen, Werkzeuge nutzen, Entscheidungen treffen und komplexe Prozessketten Ende-zu-Ende orchestrieren.

Die Relevanz dieses Themas wird durch die aktuelle Dynamik im Bankenmarkt unterstrichen. Zahlreiche Banken pilotieren bereits agentenbasierte Systeme, um dem Druck aus geändertem Kundenverhalten, steigenden regulatorischen Anforderungen und dem Bedarf an operativer Effizienz zu begegnen. Analysen zeigen, dass Agentic AI das Potenzial hat, **25 bis 50 Prozent der operativen Prozesskosten** in Kernbereichen wie Compliance (KYC/AML)¹ und Kreditbearbeitung einzusparen, indem sie Aufgaben übernimmt, die bisher menschliche kognitive Fähigkeiten erforderten. Doch mit diesen Chancen gehen signifikante Risiken einher, insbesondere im Hinblick auf Governance, Modellstabilität und die strikten regulatorischen Anforderungen des bevorstehenden EU AI Acts sowie der BaFin-Verwaltungspraxis (MaRisk, BAIT)².

Im Zentrum dieses Dokuments steht eine Sammlung von **Use Cases**, die das Spektrum von der Modernisierung von Legacy Code über einen Modernisation Agent bis hin zum autonomen Wealth Management Agent abdecken. Es werden beispielsweise Agenten für die Kreditrisikoprüfung, für das Cash Management, für die Governance sowie für das Risikomanagement vorgestellt, die sicherstellen, dass Banken die Dividende der Autonomie ernten können, ohne die institutionelle Integrität zu gefährden. **Agentic AI im Banking – dies ist ein Praxisleitfaden zum richtigen Aufsetzen und Einsetzen von modernen und führenden AI-Modellen.**

¹ KYC / AML = **Know Your Customer** / **Anti-Money Laundering**

² MaRisk = **Mindestanforderungen an das Risikomanagement**, BAIT = **Bankaufsichtliche Anforderungen an die IT**

INHALT

1. WARUM AGENTIC AI JETZT RELEVANT WIRD	1
1.1 Effizienzrevolution im Banking	4
1.2 Was macht eine KI „Agentic“?	5
2. HERAUSFORDERUNGEN BEI DER EINFÜHRUNG VON AGENTIC AI	7
2.1 Technik-Integration	7
2.2 Datenqualität und Silos	8
2.3 Halluzinationen und Modell-Risiko	9
2.4 Regulatorische Anforderungen	9
2.5 Change-Management	11
3. WIE DIE EINFÜHRUNG VON AGENTIC AI ZUM ERFOLG WIRD – 3 PHASEN	13
4. WICHTIGE ANWENDUNGSFÄLLE – USE CASES	16
4.1 Agentic AI Framework - Strukturierung der Anwendungsfälle	16
4.2 Die Top 15 Anwendungsfälle	19
4.3 Softwarelösungen für Agentic AI	35
5. HANDLUNGSEMPFEHLUNG	37

ABBILDUNGEN

Abbildung 1:	Die vier Kernkompetenzen von Agentic AI	4
Abbildung 2:	Gegenüberstellung verschiedener Beurteilungsdimensionen bei Robotic Process Automation, Generative AI und Agentic AI	5
Abbildung 3:	Fünf Hürden bei der Einführung von Agentic AI	6
Abbildung 4:	Drei Phasen der Einführung von Agentic AI	12
Abbildung 5:	Einordnung von Agentic AI Banking Use Cases in Wertschöpfungsbereich und Komplexitätsgrad der Autonomie	17
Abbildung 6:	Der AI-Agenten Kompass	35

1. WARUM AGENTIC AI JETZT RELEVANT WIRD

Die Bankenbranche steht trotz vieler positiver Entwicklungen vor einem großen Transformationsdruck. Dieser Druck wird den Einsatz autonomer KI-Systeme (Agentic AI) nicht nur begünstigen, sondern – unter Berücksichtigung aller rechtlichen Vorgaben – auch notwendig machen. Folgende strategische Handlungsfelder bilden den Kontext:



Kundenerwartung und Wettbewerb: Neue Wettbewerber wie Fintechs und Big Techs haben die Messlatte für Geschwindigkeit und Verfügbarkeit (24/7) neu definiert, was zu einem veränderten Kundenverhalten führt. Manuelle Prozesse und langwieriges Onboarding sind nicht mehr zeitgemäß. **Agentic AI ermöglicht Banken, sich der erhöhten Wettbewerbsintensität erfolgreich zu stellen:** Durch sofortige, personalisierte Interaktion und Fallabwicklung in Echtzeit – ohne dabei den Personalbestand linear skalieren zu müssen.



Effizienz und Cost-Income-Ratio: Der Druck auf die Margen und die dichte Kostenstruktur (insbesondere in Deutschland) erfordern Maßnahmen jenseits klassischer Sparprogramme. Während einfache Prozesse bereits automatisiert sind, bindet das Back Office (z.B. komplexe Compliance-Prüfungen, Kundenservice) weiterhin massive Personalkapazitäten. **Agentic AI bietet hier den Hebel, auch kognitiv anspruchsvolle Aufgaben zu automatisieren und frühere „Fix-Kostenblöcke“ signifikant zu reduzieren.**



Regulatorik intelligent managen: Die Regulierungsdichte (Basel, AML, ESG)³ steigt und damit nehmen die Anforderungen an Banken, Mitarbeiter und die eingesetzten Compliance Verfahren kontinuierlich zu. **Agentic AI transformiert Compliance von einer stark mitarbeiterbezogenen Tätigkeit zu skalierbaren, regelbasierten Prozessen** – etwa durch die drastische Reduktion von „False Positives“ bei der Geldwäschebekämpfung oder automatisierten Compliance Reportings. Mit Blick auf den EU AI Act wird robuste AI-Governance dabei vom bloßen Pflichtprogramm zum Fundament für den sicheren Einsatz dieser Technologien.

³ AML, ESG = **A**nti-**M**oney **L**aundering, **E**nvironmental **S**ocial **G**overnance



Legacy-IT und Datensilos: Historisch gewachsene Kernbankensysteme bremsen Innovationen oft aus. Der entscheidende Vorteil von Agentic AI liegt in ihrer Integrationsfähigkeit: Sie erfordert keinen sofortigen Austausch alter Systeme, der mit signifikanten Kosten und Risiken verbunden wäre, sondern kann als intelligenter Layer über bestehende Systeme gelegt werden. So lassen sich Prozesse modernisieren und Daten verknüpfen, ohne die Stabilität der Kernbankensysteme zu gefährden. **AI ertüchtigt somit alte IT-Systeme und führt diese in die Zukunft.**



Risikomanagement und Cyber-Security: Im Bereich Risikomanagement, Modellierung, Test und Aufsetzen neuer und ergänzender Risikomodelle und Parameter sowie allen Belangen des Risikoreportings setzt AI neue Maßstäbe. Die bisherige hoch-personalintensive Betreuung jedes Risikomanagement-Prozessschrittes kann mit Hilfe von AI deutlich erleichtert werden. Standardreportings und -berichte können AI-Agenten vorfinal konfigurieren. In einem Umfeld steigender Cyber-Bedrohungen ist KI ein zweiseitiges Schwert. Sie erfordert strikte Kontrolle, ist aber gleichzeitig das effektivste Werkzeug zur Abwehr. **Agentic AI kann Anomalien und Betrugsmuster (Fraud Detection) schneller und präziser erkennen als jeder menschliche Analyst, sofern die Governance stimmt.**

1.1 Effizienzrevolution im Banking

Die Effizienzrevolution im Banking begann mit klaren Regeln und starren Prozessen. Klassische Software und später **Robotic Process Automation (RPA)** automatisierten, was sich exakt beschreiben ließ: standardisierte Abläufe, hohe Volumina, kein Interpretationsspielraum. Ein Bot tat genau das, was man ihm sagte, alles war vorkonfiguriert und vorgedacht. Prozesse waren asphaltierte Straßen, denen man genau folgen musste. Das war erfolgreich. Und es war begrenzt.

Aber Banken agieren längst nicht mehr in einer Welt, in der die Nachfrage immer prognostizierbar ist, Prozesse stabil, Daten bereinigt und Oberflächen unveränderlich sind. RPA-Systeme geraten an ihre Grenzen, sobald sich kleinste Details ändern. **Klassische Software oder Automationslösungen verstehen weder Kontext noch Zielsetzung von Aufgaben.**

Mit dem Aufkommen **Generativer KI** kamen erstmals Systeme ins Spiel, die Sprache verstehen, neue Inhalte erzeugen und komplexe Informationen verarbeiten können. Doch auch GenAI bleibt im Kern reaktiv: Sie antwortet auf Prompts – sie handelt nicht.

Agentic AI schließt die Lücke zwischen dem Sprachverständnis der GenAI und der Handlungsfähigkeit von Software. Ein KI-Agent wartet nicht auf den nächsten Befehl, sondern erhält ein übergeordnetes Ziel (z. B. „Analysiere das Kreditrisiko dieses Kunden“). Um dieses Ziel zu erreichen, plant der Agent selbstständig die notwendigen Schritte, beschafft fehlende Informationen, nutzt Werkzeuge (wie Datenbankabfragen oder API-Calls⁴) und adaptiert sein Verhalten, wenn er auf Hindernisse stößt. **Wir bewegen uns also von einer Welt der Skripte („Tue genau das“) zu einer Welt der Ziele („Erreiche das“).**

⁴ API = Application Programming Interface

AGENTIC AI MARKIERT DEN NÄCHSTEN EVOLUTIONSSCHRITT. WEG VOM PASSIVEN WERKZEUG, HIN ZUM DIGITALEN AKTEUR, DER ZIELE VERFOLGT, ENTSCHEIDUNGEN TRIFFT UND PROZESSE EIGENSTÄNDIG STEUERT. FÜR BANKEN BEDEUTET DAS: NICHT NUR AUTOMATISIERUNG – SONDERN ECHTE OPERATIVE INTELLIGENZ.

1.2 Was macht eine KI „Agentic“?

In der Praxis herrscht oft Unklarheit über die genauen Abgrenzungsmerkmale. Agentic AI definiert sich durch vier Kernkompetenzen, die sie von rein generativen Modellen unterscheidet:

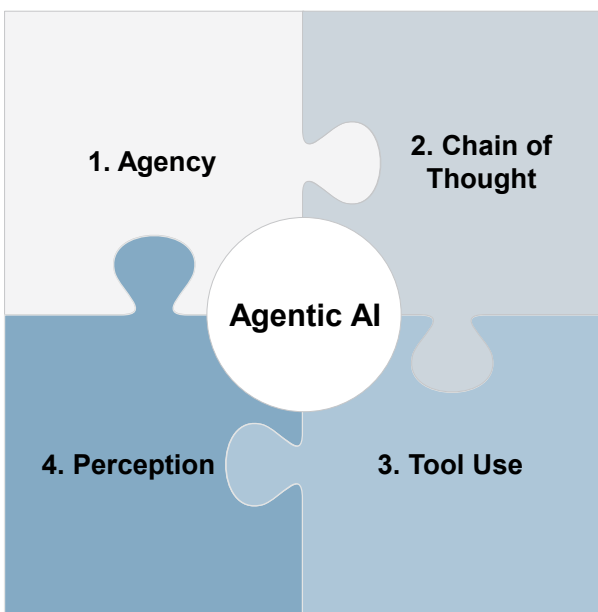


Abbildung 1: Die vier Kernkompetenzen von Agentic AI

1. Zielorientierte Autonomie (Agency): Der Agent operiert nicht in einem einfachen Frage-Antwort-Zyklus. **Er besitzt einen persistenten Zustand und verfolgt Aufgaben über längere Zeiträume hinweg, ohne ständige menschliche Eingriffe.**

2. Schlussfolgerung & Planung (Chain of Thought): Bevor der Agent handelt, „denkt“ er nach. **Er zerlegt komplexe Probleme in Teilaufgaben, bewertet seine Optionen und erstellt einen Ausführungsplan.** Diese Fähigkeit zur logischen Schlussfolgerung erlaubt es ihm, mit Ambiguität umzugehen – eine Fähigkeit, die in der komplexen Finanzwelt essenziell ist.

3. Werkzeugnutzung (Tool Use/Function Calling): Ein reines Large Language Model (LLM) ist in seinem Wissen auf den Trainingszeitpunkt beschränkt. **Ein Agent hingegen kann aktiv mit der IT-Infrastruktur der Bank interagieren.** Er kann den Kontostand in Echtzeit abfragen (Core Banking API), eine E-Mail an einen Kunden senden (Exchange Server) oder Dokumente in einem Dokumenten Management System (DMS) ablegen.

4. Wahrnehmung & Adaption (Perception): **Der Agent** nimmt seine Umgebung wahr (z.B. durch Analyse von Logfiles oder eingehenden Dokumenten) und **passt sein Verhalten an.** Wenn eine API „Timeout“ meldet, bricht der Agent nicht ab, sondern versucht es später erneut oder über alternative Datenquellen.

Dimension	Robotic Process Automation (RPA)	Generative AI (GenAI)	Agentic AI
Kernfunktion	Regelbefolgung ("The Doer")	Inhaltserstellung ("The Creator")	Autonomes Problemlösen ("The Actor")
Auslöser	Zeitplan / Event	Menschlicher Prompt (Reaktiv)	Übergeordnetes Ziel (Proaktiv)
Datenbasis	Strukturierte Daten	Unstrukturierte Daten	Strukturiert & Unstrukturiert
Flexibilität	Gering (Zero Tolerance for Change)	Hoch (Kreativ/Halluzinierend)	Hoch (Adaptiv & Logisch)
Typischer Use Case	Datentransfer zwischen Systemen	Entwurf einer Marketing-Mail	Klärung eines Geldwäsche-Verdachtsfalls
Entscheidungslogik	Deterministisch (If-Then-Else)	Probabilistisch (auf Wahrscheinlichkeiten beruhend, Token Prediction)	Probabilistisch mit Reasoning & Execution Loops

Abbildung 2: Gegenüberstellung verschiedener Beurteilungsdimensionen bei Robotic Process Automation, Generative AI und Agentic AI

2. HERAUSFORDERUNGEN BEI DER EINFÜHRUNG VON AGENTIC AI

Trotz des enormen Potenzials stehen Banken vor spezifischen, teils massiven Hürden bei der Einführung von Agentic AI.

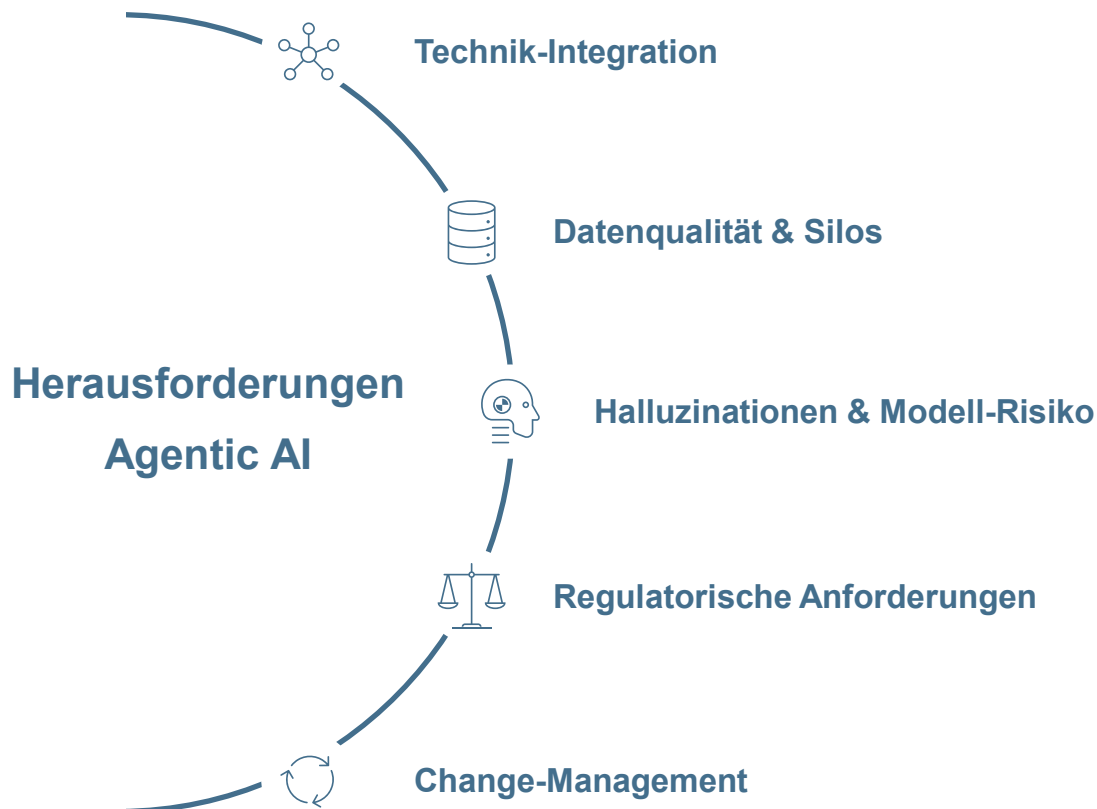


Abbildung 3: Fünf Hürden bei der Einführung von Agentic AI

2.1 Technik-Integration

Viele Banken arbeiten im Kern noch mit Legacy Systemen, also alten IT-Systemen (z.B. auf einem Mainframe-Rechner mit COBOL⁵ programmiert). Diese sind stabil, aber schwer erweiterbar und nicht einfach mit modernen digitalen Lösungen vernetzbar.

⁵ COBOL = **C**ommon **B**usiness **O**riented **L**anguage

Als Lösungsansatz kommen drei Herangehensweisen in Frage:



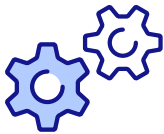
Übersetzungsschicht (Middleware):

Bestehende Systeme werden über eine Art „Übersetzer“ angebunden, sodass sie mit modernen Anwendungen zusammenarbeiten können – ohne sie sofort ersetzen zu müssen.



Digitale Assistenten für bestehende Oberflächen:

Software-Agenten bedienen die bestehenden Systeme so, wie es heute noch Menschen tun (über Textbildschirme). Sie lesen Informationen aus und geben Eingaben ein – nur schneller, automatisiert und rund um die Uhr.



Schrittweise Modernisierung:

Alte Funktionen werden nach und nach durch neue, intelligentere Lösungen ersetzt. So bleibt der Betrieb stabil, während die IT zukunftsfähig wird.

2.2 Datenqualität und Silos

Agenten benötigen Zugriff auf qualitativ hochwertige Daten, um korrekte Entscheidungen zu treffen. Bankdaten sind oft in Silos verteilt (Kreditabteilung, Zahlungsverkehr und Compliance haben getrennte Datenbanken). Agentic AI deckt Datenprobleme gnadenlos auf. Ein Agent, der z.B. keinen Zugriff auf das CRM-System hat, kann keinen KYC-Prozess durchfüh-

ren. Die Einführung von Agenten erzwingt daher oft eine Modernisierung der Datenarchitektur, wie z.B. einer sogenannten Data Fabric, die die Aufgabe hat, Daten unternehmensweit verfügbar zu machen, Zugriffsrechte bereitzustellen und zu monitoren.

2.3 Halluzinationen und Modell-Risiko

Im Banking ist Vertrauen die härteste Währung. Ein Agent, der einem Kunden fälschlicherweise einen Kredit zusagt oder eine falsche Überwei-

sung tätigt, kann großen Schaden anrichten. Um dem entgegenzuwirken, haben sich folgende Mitigations-Strategien bewährt:



RAG (Retrieval Augmented Generation):

Der Agent darf nur Fakten nutzen, die er aus verifizierten Dokumenten abgerufen hat.



Determinismus-Layer:

Kritische Aktionen (Geld bewegen) werden nicht direkt vom Agenten ausgeführt. Der Agent konfiguriert stattdessen einen „Vorschlag“, der dann aber von einem Menschen validiert und ausgeführt wird (Human-in-the-Loop).

2.4 Regulatorische Anforderungen

Die BaFin macht keine detaillierten Technikvorgaben für KI-Agenten, erwartet aber, dass der **Einsatz sicher, kontrollierbar und verantwor-**

tungsvoll erfolgt (MaRisk AT 4.3.5 – Verwendung von Modellen). Für Banken ergeben sich daraus folgende zentrale Anforderungen:



Klare Verantwortlichkeiten:

Auch wenn KI-Agenten Entscheidungen treffen oder Prozesse ausführen, muss immer eindeutig festgelegt sein, welcher Mensch dafür die Verantwortung trägt. Es darf keine „Grauzonen“ geben, in denen unklar ist, wer haftet oder eingreift.



Geregelte Zugriffsrechte für KI-Agenten:

KI-Agenten sind wie digitale Mitarbeiter zu behandeln: mit eigener Identität, klar definierten Rollen und streng begrenzten Zugriffsrechten. Sie dürfen nur auf die Systeme und Daten zugreifen, die sie für ihre Aufgaben wirklich benötigen.

Nachweisbare Qualität und Fairness der KI:



Banken müssen belegen können, dass ihre KI-Modelle zuverlässig, nachvollziehbar und fair arbeiten. Entscheidungen dürfen nicht diskriminierend sein und müssen im Zweifel erklärbar bleiben.

Um diese Anforderungen zu erfüllen, sollten Banken ein spezifisches technisches Governance-Modell etablieren:

1

Agent Identity:

Jeder Agent hat eine eindeutige ID und wird in einem Register geführt.

2

Audit Trail:

Sofern möglich, sollen alle Schritte eines Agenten („Thought“, „Action“, „Observation“) unveränderbar protokolliert werden (Logging).
In Fällen, in denen dies z.B. aufgrund der Anzahl der Agenten oder der hohen Transaktionsmenge nicht praktikabel ist, muss ein Logging-Konzept definiert werden. Dieses legt fest, welche Agentenaktionen zwingend dokumentiert werden müssen.

3

Risk Tiering:

Klassifizierung von Agenten nach Risiko.
Tier 1 (hoch): Kundenkontakt, Kreditwürdigkeitsprüfungen, Zahlungen (strenge Aufsicht, Human-in-the-Loop).
Tier 3 (niedrig): Interne Recherche, Assistenz (geringere Aufsicht).

4

Red Teaming:

Regelmäßige simulierte Angriffe auf die Agenten, um Schwachstellen (z.B. Prompt Injection Attacks) zu finden und zu beheben.

5

„Menschliche Aufsicht“:

Banken müssen technische „Kill-Switches“ und Eskalationspfade implementieren, bei denen der Agent ab einem gewissen Risikoscore (Confidence Score) zwingend an einen Menschen übergibt.

2.5 Change-Management

Der Change-Prozess bei der **Einführung von Agentic AI in Banken muss als integrierte Business-Transformation orchestriert werden** – nicht als IT-Programm mit begleitender Kommunikation. Erfolgreiche Orchestrierung erfordert eine klare Kommunikationsstruktur (Warum? Wo? Wie viel AI?), aktive Führungskräfte

sowie eine systematische Einbindung der Mitarbeiter entlang der gesamten Wertschöpfung. Die Schnelligkeit des Wandels ist dabei die größte Herausforderung. In einem KI-Change-Prozess sollte man mit nicht-finalen Zielbildern, Übergangsverantwortlichkeiten und gefühlt inkonsistentem Führungsverhalten rechnen.

Strategische Klarheit trotz Unschärfe:



Durch die Erstellung eines klaren Zielbildes für Agentic AI im Operating Model (z.B. Effizienz, Risikoqualität, Kundenerlebnis, Skalierbarkeit) wird die Sinnhaftigkeit und Notwendigkeit von Agentic AI vermittelt. Vorstand und Bereichsleitung senden einheitliche Signale an die Mitarbeiter aus, die auf der operativen Ebene durch sogenannte Change-Agents oder AI-Champions verstärkt werden. Die Verankerung von AI im Berufsalltag ist eine primäre Aufgabe der Führungskräfte. **Die Besonderheit ist, dass nicht alle Zielparameter zum Projektstart definierbar sind. Das Reiseziel ist klar definiert, bei der Routenwahl, den unterstützenden Tools und Partnern auf diesem Weg ist aber Flexibilität gefordert.**

Governance & Accountability:



Es muss eine klare Zuordnung von Entscheidungsverantwortung (AI vs. Mensch) und von möglicher Haftung bzw. Eskalation vorliegen. Prozesse sollen optimiert aber nicht verwässert werden. Im Zweifelsfall muss es eine übergeordnete Institution geben (z.B. AI Steering Committee), die bei strittigen Themen finale Entscheidungen treffen kann. **Die Übertragung von einfachen Entscheidungen auf AI kann dabei schnell erfolgen, bei schwierigeren Aufgaben sind Übergangslösungen sinnvoll, um Vertrauen in die neue Zusammenarbeit aufzubauen.**

Kulturelle Akzeptanz:



Die Angst vor Bedeutungs- oder gar Jobverlust wird durch die wirkungsstarken Use Cases, in denen die unterstützende Funktion von Agentic AI hervorgehoben wird, erst einmal nicht minimiert. Der Agent wird zunächst als potenzieller „Konkurrent“ und nicht als „Kollege“ wahrgenommen. **Der neue Kollege arbeitet schneller, zuverlässiger, wird nicht krank und ist 24/7 im Einsatz.** Er greift im Idealfall in Millisekunden auf Datenpools und Datenbanken zurück. Es ent-

steht ein unfairen Wettbewerbsvorteil, bei dem der Mensch in den mittelschweren repetitiven Tätigkeiten immer schlechter als der Agent aussehen wird. Im Change-Management Ansatz wird es daher darauf ankommen zu vermitteln, dass AI trotz aller Vorteile nicht in Konkurrenz zum Menschen steht. Es wandeln sich aber sehr wohl die Aufgabenfelder für viele Mitarbeiter. **Der Mensch wird in der neuen Welt in anderen Rollenbildern und Aufgaben benötigt. Diesen Wandel gilt es, kommunikativ zu vermitteln und zu begleiten.** Helfen kann dabei auch, den hinter Agentic AI liegenden Workflow sehr transparent zu machen, damit Vorurteile abgebaut werden und Mitarbeiter sehen, dass AI in dieser Funktion einen wirklichen Mehrwert schafft.

ZWISCHEN MENSCH UND AGENTIC AI ENTSTEHT EIN UNFAIRER WETTBEWERBSVORTEIL. DER NEUE „AGENTIC AI- KOLLEGE“ WIRD NICHT KRANK, LÖST PROBLEME IN MILLISEKUNDEN UND IST 24/7 IM EINSATZ.

3. WIE DIE EINFÜHRUNG VON AGENTIC AI ZUM ERFOLG WIRD – 3 PHASEN

Das Planen, das Aufsetzen und die Implementierung von Agentic AI Lösungen ist als strategische Weiterentwicklung zu verstehen, die bis hin zu grundlegenden Veränderungen im gesamten Geschäftsmodell führt.

Demnach ist es von elementarer Bedeutung, in einem AI-Projekt strategische, organisatorische und prozessuale Aspekte sowie das Change-Management parallel zu verfolgen. Die Auswirkungen auf das Geschäftsmodell müssen grundlegend betrachtet werden.

AI-Agenten nur über alte, ineffiziente Prozesse zu stülpen, hilft demnach nicht. Stattdessen müssen das Geschäftsmodell, die Prozessebenen und Prozesse von Grund auf neu gedacht werden – mit der Autonomie und den Interaktionen/Schnittstellen der Agenten/Agentenlayer im Zentrum.

Um die strategischen, prozessualen und technologischen Risiken zu minimieren, empfiehlt sich ein strukturierter, phasenbasierter Ansatz, der von der strategischen Ausrichtung bis zur industriellen Skalierung reicht.

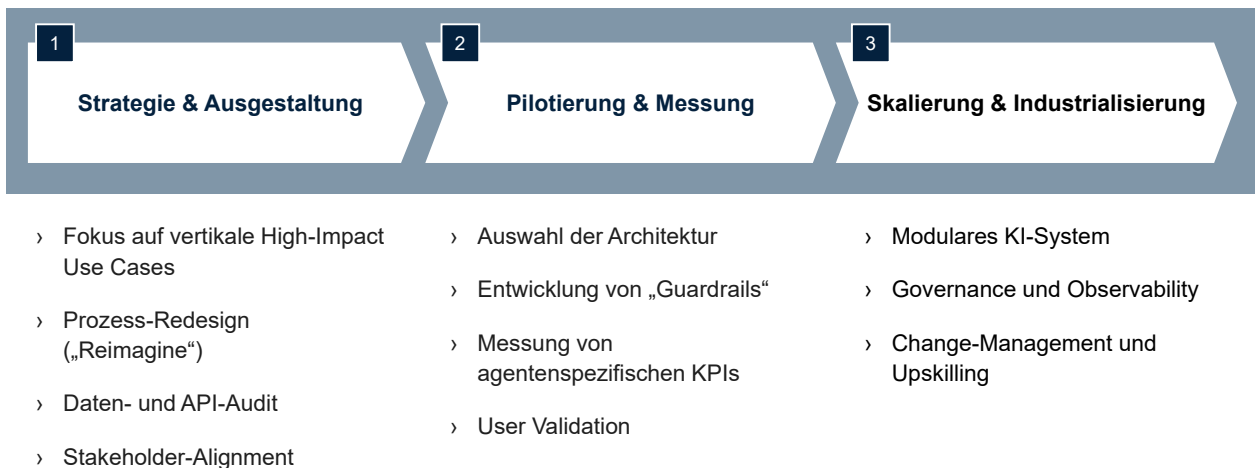


Abbildung 4: Drei Phasen der Einführung von Agentic AI

AI ÜBERHASTET EINZUFÜHREN FÜHRT OFT ZU ‚SCHNELLERER INEFFIZIENZ‘ UND EINER WEITEREN VERHÄRTUNG VON SILOLÖSUNGEN. DAVOR WARNEN ZAHLREICHE STUDIEN.

Phase 1: Strategie und Ausgestaltung (Discovery & Strategy)

In dieser Phase geht es darum, die Einführung von Agentic AI koordiniert und strategisch zu planen und den Erfolg sicherzustellen. Viele Unternehmen scheitern, weil sie sich auf „horizontale“ Ansätze konzentrieren (z.B. „ein allgemeiner Chatbot für alle Mitarbeiter“), die sicherlich nett sind, aber keinen klaren Geschäftswert liefern. Empfehlung: Was Chat GPT bereits kann, sollte man als Firma nicht mehr nachbauen.

- **Fokus auf vertikale High-Impact Use Cases:** Suchen Sie nach Prozessen, die tief in einer Funktion verankert sind (vertikal), hohe Reibungsverluste aufweisen und auf komplexen, aber logischen Entscheidungen basieren.
- **Prozess-Redesign („Reimagine“):** Stellen Sie die radikale Frage: „Wie würde dieser Prozess aussehen, wenn wir ihn heute neu erfinden würden und ein Agent 60-80% der Arbeit autonom erledigen könnte? Welche Auswirkungen hätte das auf unsere Organisation und unsere Mitarbeiter?“ Dies erfordert oft das Aufbrechen alter Organisationsstrukturen, da Agenten prozessübergreifend agieren.
- **Daten- und API-Audit:** Agentic AI benötigt Treibstoff. Ein Audit der Datenqualität (strukturiert vs. unstrukturiert) und der Zugänglichkeit von Systemen via APIs ist zwingend notwendig.
- **Stakeholder-Alignment:** Da Agenten autonom handeln, müssen Compliance, Rechtsabteilung und IT-Sicherheit (CISO) von Tag 1 an eingebunden sein, um Governance-Richtlinien zu definieren. Es muss geklärt werden: Was darf der Agent *niemals* tun?

Phase 2: Pilotierung & Messung (Proof of Concept & Value)

Hier wird die Theorie in die Praxis umgesetzt. Ziel ist nicht nur ein funktionierender technischer Prototyp, sondern der Beweis der Wertschöpfung und der Beherrschbarkeit der Sicherheit.

- **Auswahl der Architektur:** Entscheidung für ein Software-Framework (siehe Abschnitt 4.3) und gegebenenfalls Implementierung der ersten MCP⁶-Server für den Datenzugriff.
- **Entwicklung von „Guardrails“:** Implementierung von Sicherheitsmechanismen in Form einer spezifischen Governance. Agenten dürfen in dieser Phase oft nur „vorschlagen“, nicht „ausführen“ (Human-in-the-Loop), oder sie operieren in einer streng isolierten Sandbox-Umgebung („Red Teaming“).
- **Messung von agentenspezifischen KPIs:** Traditionelle Software-KPIs wie Uptime oder Response Time reichen nicht aus. **Um die Wirksamkeit von Agentic AI messbar zu machen, benötigt es neue Metriken:**

⁶ MCP = Model Context Protocol

- » **Goal Accuracy:** Wurde das übergeordnete Ziel erreicht? (Nicht nur: Wurde der Task ausgeführt?)
 - » **Task Adherence:** Hat der Agent sich an den vorgeschriebenen Prozessweg gehalten oder unerlaubte Abkürzungen genommen?
 - » **Cost per Outcome:** Setzt man die entstandenen Kosten ins Verhältnis zum wirtschaftlichen Wert der Handlung und kommt zum Ergebnis, dass der Agent 5 EUR an Rechenleistung kostet, um einen 10.000-Euro-Deal zu retten, dann ist er hocheffizient.
 - » **Intervention Rate:** Wie oft musste ein Mensch eingreifen, um den Agenten zu korrigieren? Dieser Wert muss über die Zeit sinken.
- **User Validation:** Testen mit echten Nutzern, um das Vertrauen in die autonomen Entscheidungen des Agenten aufzubauen und die UX der Kollaboration zu verfeinern.

Phase 3: Skalierung & Industrialisierung (Scale & Industrialise)

Der Übergang vom erfolgreichen Pilotprojekt zur breiten Anwendung ist der kritischste Schritt, an dem ein sehr hoher Anteil der KI-Projekte scheitert.

- **Modulares KI-System:** Aufbau einer modularen Infrastruktur, die es erlaubt, Agenten flexibel zu verknüpfen und zu warten. Vermeidung von monolithischen „Super-Agenten“, die unwartbar sind. Das Ziel ist eine flexible Service-Architektur aus spezialisierten Agenten.
- **Governance und Observability:** Einführung von professionellen Systemen zur Überwachung der Agenten-Performance in Echtzeit. Tracing (die Nachverfolgung der Gedankenschritte des Agenten aka „Chain of Thought“) ist essenziell für das Debugging und die Compliance. Man muss im Fehlerfall genau nachweisen können, warum der Agent eine Entscheidung getroffen hat.
- **Change-Management und Upskilling:** Die Schulung der Mitarbeiter, da sich die Rolle des Mitarbeiters wandelt vom „Ausführer“ zum „Manager“ und „Supervisor“ von Agenten-Flotten. Dies erfordert neue Kompetenzen in der Beurteilung von KI-Ergebnissen.

4. WICHTIGE ANWENDUNGSFÄLLE – USE CASES

4.1 Agentic AI Framework - Strukturierung der Anwendungsfälle

Um das transformative Potenzial von Agentic AI systematisch zu erschließen, bedarf es einer strukturierten Analyse wo und wie Agentic AI eingesetzt werden kann. Dies beinhaltet auch die Abschätzung möglicher Potenziale und Risiken und unterstützt bei der Priorisierung der Anwendungsfälle für die Umsetzung.

Wir schlagen ein Framework vor, das Use Cases entlang mehrerer Dimensionen ordnet: **Wertschöpfungsbereich** (Front, Middle, Back Office),

Komplexitätsgrad der Autonomie (Assistenzsystem bis autonome Orchestrierung) und **Impact** (Wirkungs- und Veränderungsgrad bzw. wirtschaftliche Potenziale).

Diese Strukturierung hilft Banken, ein ausgewogenes Portfolio an KI-Initiativen zu entwickeln, das sowohl schnelle Effizienzgewinne (Quick Wins) als auch strategische Differenzierung ermöglicht.

Front Office: Kundenkontakt & Vertrieb

Hier liegt der Fokus auf Umsatzsteigerung, Personalisierung und Reaktionsgeschwindigkeit. Agentic AI agiert hier oft als „Super-Assistent“ für den Kundenberater oder direkt als Kundeninterface.

Ziel: Hyper-Personalisierung, 24/7-Verfügbarkeit komplexer Beratungsleistungen und bessere Loyalisierung des Kundenstamms.

Middle Office: Risk, Compliance & Steuerung

Dies ist der Bereich mit dem höchsten unmittelbaren ROI-Potenzial durch Agentic AI. Die Aufgaben hier sind oft kognitiv anspruchsvoll, datenintensiv und fehleranfällig. Agenten können hier als unermüdliche Analysten fungieren.

Ziel: Präzision, Risikominimierung und Bewältigung massiver Datenmengen (z.B. bei der Geldwäschebekämpfung) und Erstellung regulatorischer Reportings.

Back Office: Operations, IT & Internal Functions

Hier stehen Kosteneffizienz, Stabilität und die Modernisierung veralteter Systeme im Vordergrund. Agenten übernehmen die Rolle von digitalen Ingenieuren oder Sachbearbeitern. Außerdem sollen Querschnittsfunktionen (z.B. HR und Marketing) unterstützt werden.

Ziel: Dunkelverarbeitung (Straight-Through-Processing), autonome Kreditprüfung, System Resilienz und Legacy-Modernisierung.

Nachfolgend werden 15 Use Cases dargestellt, die sich auf die drei Wertschöpfungsbereiche verteilen:

LEVEL 1: ASSISTENZ

- Use Case 1: Hyperpersonalisierter Wealth Management Co-Pilot
- Use Case 2: Regulatory Reporting & Compliance Monitor
- Use Case 3: Corporate Banking & Trade Finance Orchestrator
- Use Case 4: Competitor Intelligence & Market Research Agent
- Use Case 5: Legacy Code Migration & Modernisation Agent
- Use Case 6: Der „Recruiting Orchestrator“ Agent

LEVEL 2: TEILAUTONOMIE

- Use Case 7: Intelligente Kreditrisikoprüfung & Underwriting
- Use Case 8: Cash Management & Liquidity Planning
- Use Case 9: Smart Audit & Internal Control Agent (Governance)
- Use Case 10: Der 24/7 HR-Concierge & Policy Agent

LEVEL 3: VOLLAUTONOMIE

- Use Case 11: Customer Service & Dispute Resolution Avatar
- Use Case 12: Hyper-Personalisierung & „Next Best Action“
- Use Case 13: Autonomer AML-Analyst
- Use Case 14: Autonomer IT-Operations & Incident Response Agent
- Use Case 15: Autonomes Onboarding & Employee Lifecycle Management

Bereich / Ebene	Front Office (Kunde & Vertrieb)	Middle Office (Risiko & Steuerung)	Back Office (Abwicklung, IT & Internal Functions)
Level 1: Assistenz <i>(System liefert Informationen, Mensch handelt)</i>	Use Case 1 Hyperpersonalisierter Wealth Management Co-Pilot	Use Case 2 Regulatory Reporting & Compliance Monitor Use Case 3 Corporate Banking & Trade Finance Orchestrator Use Case 4 Competitor Intelligence & Market Research Agent	Use Case 5 Legacy Code Migration & Modernisation Agent Use Case 6 Der "Recruiting Orchestrator" Agent
Level 2: Teilautonomie <i>(System bereitet vor und führt aus, Mensch genehmigt)</i>		Use Case 7 Intelligente Kreditrisikoprüfung & Underwriting Use Case 8 Cash Management & Liquidity Planning Use Case 9 Smart Audit & Internal Control Agent	Use Case 10 24/7 HR-Concierge & Policy Agent
Level 3: Vollautonomie <i>(System agiert selbstständig, Mensch greift nur bei Fehlern ein)</i>	Use Case 11 Customer Service & Dispute Resolution Avatar Use Case 12 Hyper-Personalisierung & "Next Best Action"	Use Case 13 Autonomer AML-Analyst	Use Case 14 Autonomer IT-Operations & Incident Response Agent Use Case 15 Autonomes Onboarding & Employee Lifecycle Management

Abbildung 5: Einordnung von Agentic AI Banking Use Cases in Wertschöpfungsbereich und Komplexitätsgrad der Autonomie

4.2 Die Top 15 Anwendungsfälle

Im Folgenden werden 15 Anwendungsfälle beispielhaft dargestellt. Dabei wird jeder Use Case beschrieben und sowohl das Potenzial als auch die Risiken aufgezeigt.

Use Case 1: Hyperpersonalisierter Wealth Management Co-Pilot

Kundenberater im Private Banking verbringen bis zu 70% ihrer Zeit mit Administration und Vorbereitung. Ein „Wealth Agent“ agiert als proaktiver Assistent, der Kundenportfolios kontinuierlich überwacht. Bei Marktereignissen (z.B. EZB-Zinsänderung, Tech-Aktien-Crash) simuliert der Agent die Auswirkungen auf jedes einzelne Kundenportfolio. Dabei übernimmt er die folgenden Aufgaben:

- **Monitoring:** Der Agent überwacht Märkte und Kundenportfolios 24/7.
- **Simulation:** „Was bedeutet der Kurssturz von Aktie X für Kunde Y?“
- **Planning:** Der Agent identifiziert Handlungsbedarf (z.B. Umschichtung zur Risikominimierung) und prüft steuerliche Auswirkungen. Der Agent kann eigenständig Optionen für den Kunden aufbereiten und den „House-View“ der Bank berücksichtigen.
- **Engagement:** Er entwirft eine personalisierte Nachricht an den Berater oder direkt an den Kunden (in der App) mit einem konkreten Handlungsvorschlag („Switch Recommendation“).



Potenziale:

- **Skalierung:** Jeder Berater kann **50–60 mehr Kunden** betreuen, ohne die Servicequalität zu senken.
- **Umsatz:** Erhöhung der Assets under Management (AuM) und der Kundenzufriedenheit (Net Promoter Score, NPS) durch proaktive Ansprache.



Risiken:

- Es kann zu einem Vertrauensverlust der Kunden kommen, wenn dieser sich nicht persönlich von einem Berater betreut fühlt.

Use Case 2: Regulatory Reporting & Compliance Monitor

Banken stehen unter stetig wachsendem regulatorischem Druck. Neue Vorschriften wie DORA, ESG-Regulatorik, Basel IV, CRR/CRD sowie regelmäßige Meldepflichten wie COREP, FINREP oder AnaCredit erfordern kontinuierliche Anpassungen von Prozessen, IT-Systemen und internen Richtlinien. Ein Agent-AI-basierter Regulatory Agent unterstützt Banken entlang des gesamten Compliance-Lebenszyklus.

- **Horizontal Scanning:** Der Agent überwacht automatisch Veröffentlichungen von Aufsichtsbehörden (EBA, EZB, BaFin, ESMA), Gesetzesentwürfe und Konsultationspapiere, regulatorische

Leitlinien, Q&As und Rundschreiben. Mithilfe von NLP und semantischer Analyse erkennt er relevante Änderungen frühzeitig.

- **Gap-Analyse:** Die identifizierten regulatorischen Anforderungen werden mit internen Richtlinien, Policies und Prozessen abgeglichen, gegen bestehende Kontrollmechanismen gemappt und auf Umsetzungsdefizite („Gaps“) geprüft. Der Agent priorisiert Handlungsbedarfe nach Risiko, Frist und Auswirkungsgrad.
- **Umsetzungsunterstützung:** Der Agent kann Maßnahmenpläne vorschlagen, Verantwortlichkeiten zuordnen, Fristen überwachen und Dokumentation vorbereiten.
- **Reporting-Unterstützung:** Für COREP-, FINREP- oder ESG-Reports werden Daten aus verschiedenen Daten-Silos (Finance, Risk, IT, Sustainability) aggregiert, auf Konsistenz und Plausibilität geprüft und die Erstellung strukturierter Berichte wird unterstützt.



Potenziale

- Effizienzsteigerung durch Reduktion manueller Analysearbeit
- Risikominimierung durch frühzeitige Erkennung regulatorischer Änderungen
- Konsistenz durch einheitliche Interpretation regulatorischer Anforderungen



Risiken

- Fehlinterpretation regulatorischer Texte
- Abhängigkeit von der Datenqualität & Datenverfügbarkeit
- Abhängigkeit von automatisierten Entscheidungen
- Mangelnde Akzeptanz durch die Regulierungsbehörde, da nachvollziehbare Entscheidungsprozesse und dokumentierte Verantwortlichkeiten erwartet werden.

Use Case 3: Corporate Banking & Trade Finance Orchestrator

Trade Finance gilt als eines der komplexesten und reibungsintensivsten Geschäftsfelder im Bankwesen. Es ist geprägt durch eine hohe Abhängigkeit von papierbasierten Dokumenten, zersplitterten internationalen Rechtsrahmen und der Notwendigkeit einer präzisen Koordination zwischen Importeuren, Exporteuren, Logistikdienstleistern, Versicherern und korrespondierenden Banken.

Der Corporate Banking & Trade Finance Orchestrator ist weit mehr als ein einfaches OCR-Tool (Optical Character Recognition). Er ist ein autonomer Agent, der den gesamten Lebenszyklus einer Transaktion orchestriert. Technologisch fungiert dieser Agent als multimodales System, das unstrukturierte Daten (Verträge, Konnossemente/Bills of Lading, Rechnungen) und strukturierte Daten (Zahlungsverkehrsdaten, Kreditlimits) integriert, um komplexe Finanzinstrumente wie Akkreditive (Letters of Credit, L/C) und

Supply Chain Finance (SCF) Programme auszuführen.

Der Workflow basiert auf „Chain-of-Thought“-Reasoning, durch das der Agent die Konformität mit internationalen Regelwerken wie den „Einheitlichen Richtlinien und Gebräuchen für Dokumenten-Akkreditive“ (ERA 600 / UCP 600) prüft. Ein konkretes Szenario verdeutlicht die Arbeitsweise: Sobald digitale oder gescannte Versanddokumente eingehen, referenziert der Agent autonom Versanddaten, Hafencodes und Warenbeschreibungen gegen das ausgestellte Akkreditiv. Entdeckt er Diskrepanzen – beispielsweise eine abweichende Schreibweise eines Hafennamens oder ein Datum, das außerhalb der Verladefrist liegt –, bewertet der Agent die Materialität dieser Abweichung. Handelt es sich um einen unwesentlichen Fehler, kann er autonom einen „Waiver Request“ (Verzichtserklärung) an den Käufer entwerfen, oder, sofern die Abweichung innerhalb vorab genehmigter Risikotoleranzen liegt, die Zahlung freigeben.

Zusätzlich agieren diese Agenten in einer Multi-Agenten-Architektur. Ein spezialisierter „Compliance-Agent“ prüft parallel das Transportschiff gegen Echtzeit-Sanktionslisten (z.B. OFAC) und analysiert dessen Routenhistorie auf verdächtige Stopps („Going Dark“), während ein „Kredit-Agent“ das Kreditlimit des Firmenkunden dynamisch an den aktuellen Wert der Sicherheit (Warenwert) anpasst.



Potenziale

Der Einsatz agentenbasierter Orchestratoren im Trade Finance bietet einen transformativen ROI, indem er die operative Latenz, die Liquidität bindet, drastisch reduziert.

- **Beschleunigung des Cash-Conversion-Cycle:** Traditionelle manuelle Dokumentenprüfungen können Zahlungen um Tage oder Wochen verzögern. Agentic AI-Systeme reduzieren die Verifikationszeit auf Sekunden. Durch die Identifizierung und Lösung von Diskrepanzen in Echtzeit (oder das autonome Erstellen von Waiver-Anfragen) beschleunigen Banken den Geldumschlag für ihre Firmenkunden und setzen gebundenes Working Capital frei.
- **Reduktion der Cost-to-Serve:** Die manuelle Prüfung von Handelsdokumenten ist arbeitsintensiv und erfordert hochspezialisiertes Personal. Agenten ermöglichen es Banken, das Ertragswachstum vom Personalwachstum zu entkoppeln. Dies verbessert die Cost-Income-Ratio (CIR) signifikant, da Routineprüfungen vollständig automatisiert werden.
- **Umsatzwachstum durch SME-Inklusion:** Historisch gesehen machten die hohen Prozesskosten Trade-Finance-Produkte für kleine und mittlere Unternehmen (KMU/SME) unwirtschaftlich. Agentic AI senkt die Grenzkosten einer Transaktion auf ein Niveau, das es Banken erlaubt, auch KMU profitabel zu bedienen, die zuvor vom globalen Handelsfinanzierungsmarkt ausgeschlossen waren.

- **Risikoadjustierte dynamische Bepreisung:** Durch die kontinuierliche Überwachung des Standorts und Status von Waren (via API-Verbindungen zu Logistikern) kann der Agent dynamische Preise anbieten. Erreicht eine Lieferung einen sicheren Hafen, kann die Risikoprämie in Echtzeit gesenkt werden, was wettbewerbsfähige Raten bei gleichzeitiger Margensicherung ermöglicht.



Risiken

- **Halluzination in der rechtlichen Interpretation:** Das primäre Risiko besteht in der Fehlinterpretation komplexer Klauseln in nicht-standardisierten Handelsverträgen. Wenn ein Agent eine Force-Majeure-Klausel falsch auslegt oder fälschlicherweise eine Diskrepanz als nichtig einstuft, haftet die Bank unter Umständen für Millionenbeträge bei fehlerhaften Auszahlungen.
- **Sanktionsumgehung und TBML (Trade-Based Money Laundry):** Geldwäsche im internationalen Handel ist hochkomplex. Kriminelle Akteure nutzen adversarial attacks (z.B. manipuliertes Bildrauschen in Scans) oder subtile Textänderungen, um KI-Systeme zu täuschen. Wenn ein Agent nicht erkennt, dass ein Schiff sein Transpondersignal deaktiviert hat oder von einer Briefkastenfirma kontrolliert wird, die sanktionierten Entitäten nahesteht, drohen massive regulatorische Strafen.
- **Systemische Gleichschaltung (Herdung):** Wenn mehrere Banken dieselben zugrundeliegenden Foundation Models für ihre Trade-Agenten nutzen, könnte eine einzelne Schwachstelle oder ein Bias in diesem Modell zu systemischen, simultanen Ausfällen im globalen Handelsnetzwerk führen.

Use Case 4: Competitor Intelligence & Market Research Agent

Der Competitor Intelligence Agent demokratisiert die strategische Analyse. Traditionell erfordert Benchmarking ganze Teams von Analysten, die manuell 10-K-Filings, Transkripte von Earnings Calls und Produktseiten durchforsten. Der Agent automatisiert diese gesamte Pipeline.

Unter Nutzung von Tools wie BankIQ+ überwachen diese Agenten autonom ein definiertes Set von Wettbewerberbanken. Sie konsumieren öffentliche Finanzoffenlegungen (SEC EDGAR), regulatorische Meldungen (FDIC Call Reports) und sogar Marketingmaterialien. Der Agent kann strategische Anfragen beantworten: „Vergleiche unseren Net Interest Margin (NIM) Trend mit J.P. Morgan und Wells Fargo über die letzten 8 Quartale und korreliere ihn mit deren Exposure in Commercial Real Estate (CRE).“

Jenseits von Finanzkennzahlen überwacht der Agent Produktlaunches. Er kann Websites von Wettbewerbern verarbeiten, um Änderungen bei Sparzinsen oder neuen Kreditkarten-Perks in Echtzeit zu erkennen und Produktmanager auf „White Space“-Chancen oder Wettbewerbsbedrohungen hinzuweisen.



Potenziale

- **Strategische Agilität in Echtzeit:** Banken können auf Preisbewegungen von Wettbewerbern (z.B. eine Erhöhung der Einlagenzinsen) innerhalb von Stunden reagieren. Diese Agilität ist im digitalen Banking-Zeitalter, in dem Kunden den Anbieter sofort wechseln können, entscheidend.
- **Tiefes Benchmarking:** Der Agent erlaubt granulares Benchmarking, das zuvor zu arbeitsintensiv war (z.B. Vergleich der „App-Login-Geschwindigkeit“ oder „Anzahl der Klicks zur Kontoeröffnung“ über 20 Wettbewerber hinweg). Dies treibt spezifische, handlungsorientierte Verbesserungen der Produkt-Roadmap voran.
- **Demokratisierung der Strategie:** Strategische Einsichten sind nicht mehr das Hoheitsgebiet eines zentralen „Strategie-Teams“. Product Owner, Filialleiter und Marketing-Leads können „On-Demand“ auf High-Level-Wettbewerbsintelligenz zugreifen, um fundierte lokale Entscheidungen zu treffen.



Risiken

- **Geistiges Eigentum und Scraping-Risiken:** Aggressives Scraping (automatisierte Datenextraktion) von Wettbewerber-Websites kann gegen Nutzungsbedingungen oder IP-Rechte verstoßen. Wenn der Agent versehentlich auf zugangsbeschränkte Inhalte oder proprietäre Daten zugreift, drohen der Bank rechtliche Konsequenzen.
- **Halluzination von Daten:** Finanzanalyse erfordert 100% Präzision. Wenn ein Agent eine Kapitalquote oder NPL-Zahl (Non-Performing Loan) eines Wettbewerbers „halluziniert“, könnte dies zu desaströsen strategischen Fehlentscheidungen führen. Das „Grounding“ des Agenten in verifizierbaren Dokumenten (10-Ks) ist essenziell, aber nicht fehlerfrei.
- **Herding und Kollusion:** Wenn alle Banken ähnliche Agenten nutzen, um gegenseitig ihre Preise zu überwachen, könnte dies zu algorithmischer Kollusion (implizite Preisabsprache) führen, bei der Agenten sich gegenseitig Preise signalisieren, um hohe Margen zu halten. Regulierungsbehörden wie FTC und DOJ prüfen zunehmend „algorithmische Angleichung“.

Use Case 5: Legacy Code Migration & Modernisation Agent

Viele Banken, insbesondere im deutschsprachigen Raum (Sparkassen, Großbanken), betreiben ihre Kernsysteme auf Mainframes (IBM Z) mit jahrzehntealtem COBOL-Code. Das Wissen über diese Systeme schwindet mit der Pensionierung der Entwickler („Grey Hair Problem“).

Agentic AI dient hier nicht nur als Übersetzer, sondern als intelligenter Modernisierungs-Partner. Der Agent analysiert ganze Code-Repositories, extrahiert die Geschäftslogik, dokumentiert diese in natürlicher Sprache, schreibt Unit-Tests und migriert den Code in moderne Sprachen wie Java, Python oder C#. Der Agent scannt Millionen Zeilen Code, um Abhängigkeiten zu verstehen („Wer ruft wen auf?“). Er kommentiert den Code und erklärt die Business-Logik (z.B. „Dies ist die Zinsberechnung für Sparbücher“).

von vor 1990“). Dabei nutzt er spezialisierte LLMs (z.B. IBM watsonx Code Assistant), um COBOL in Java zu übersetzen. Außerdem schreibt der Agent Tests, führt den neuen Code aus, vergleicht das Ergebnis mit dem alten Code und korrigiert Fehler autonom („Self-Healing“).



Potenziale

- **Geschwindigkeit:** Beschleunigung von Migrationsprojekten um 50–80%.
- **Beispiel:** Der IT-Dienstleister **Globant** berichtet von einem Bankprojekt, bei dem 11.600 Zeilen COBOL in nur 105 Stunden (statt 560 Stunden manuell) in Java-Microservices migriert wurden.
- **Strategischer Wert:** Reduktion der Abhängigkeit von teuren COBOL-Freelancern und Ermöglichung von Cloud-Migrationen.



Risiken

- Der generierte Code könnte subtile Logikfehler enthalten oder ineffizient sein.
- Es kann zu einem Verlust von implizitem Wissen kommen.
- **Hürde:** Zugriff auf Mainframe-Testumgebungen und Integration in moderne CI/CD-Pipelines.

Use Case 6: Der „Recruiting Orchestrator“ Agent

Der **Recruiting Orchestrator Agent** revolutioniert die Talentakquise (Talent Acquisition, TA), indem er von der reinen Stichwortsuche zur autonomen Kandidatenansprache und zum Lifecycle-Management übergeht. Dieser Agent operiert über den gesamten Einstellungsstrichter („Funnel“) hinweg.

In der Sourcing-Phase scannt der Agent das offene Web, Netzwerke wie LinkedIn oder GitHub sowie interne Alumni-Datenbanken, um eine „Slate“ (Liste) passiver Kandidaten zu erstellen. Er nutzt Analysen zu „Erfolgssignalen“ – indem er Muster in den Hintergründen von leistungsstarken aktuellen Mitarbeitern identifiziert –, um externe Kandidaten zu ranken, anstatt sich auf einfache Keyword-Übereinstimmungen in Lebensläufen zu verlassen.

Sobald Kandidaten identifiziert sind, agiert der Agent als primärer Kontaktpunkt. Er versendet autonom hyper-personalisierte Nachrichten (unter Bezugnahme auf spezifische Projekte im Portfolio des Kandidaten), beantwortet Fragen zur Unternehmenskultur oder Benefits rund um die Uhr und verhandelt Interviewtermine durch direkte Koordination mit den Kalendern der Hiring Manager. Er kann sogar „Level 1“-Screening-Interviews per Chat oder Voice durchführen, um technische Kompetenzen und kulturelle Passung zu bewerten, bevor ein menschlicher Recruiter involviert wird.



Potenziale

- **Kompression der „Time-to-Hire“:** Durch die Automatisierung von Sourcing, Screening und Terminierung kann Agentic AI die Einstellungszeit um das bis zu Zehnfache reduzieren. Dies ist kritisch im Banking, wo der Wettbewerb um digitale und quantitative Talente (Quants) extrem hoch ist.
- **Proaktives Talent Pipelining:** Der Agent wandelt das Recruiting von einer reaktiven Tätigkeit (Besetzung einer Vakanz) in eine proaktive Strategie um. Er pflegt kontinuierlich einen „Bench“ von warmen Kandidaten und hält diese mit relevanten Inhalten engagiert, sodass bei Freiwerden einer Stelle die Besetzungszeit gegen null geht.
- **Kandidatenerfahrung (Candidate Experience):** Das „Schwarze Loch“ des Recruitings (Bewerbung ohne Antwort) wird eliminiert. Der Agent stellt sicher, dass jeder Kandidat zeitnahes Feedback und Updates erhält, was die Arbeitgebermarke (Employer Brand) signifikant stärkt.
- **Reduktion von Bias (Potenzial):** Bei korrekter Kalibrierung ignoriert der Agent demografische Daten (Name, Alter, Geschlecht) und fokussiert sich rein auf Fähigkeiten und Erfolgssignale, was potenziell diversere Kandidatenlisten erzeugt als bei menschlichen Recruitern, die unbewussten Vorurteilen unterliegen.



Risiken

- **Verstärkung algorithmischer Vorurteile:** Wenn der Agent auf historischen Einstellungsdaten trainiert wird, die vergangene Vorurteile widerspiegeln (z.B. eine Historie, in der fast nur Männer für Trading-Rollen eingestellt wurden), wird er diesen Bias aggressiv replizieren und skalieren (das „Amazon Resume Tool“-Problem). Dies birgt massive rechtliche Risiken unter Antidiskriminierungsgesetzen (AGG in Deutschland, Equality Act in UK).
- **Enthumanisierung von Talenten:** Hochwertige Kandidaten für Senior-Banking-Rollen könnten sich durch die Interaktion mit einer Maschine entfremdet fühlen. Eine übermäßige Abhängigkeit von Agenten für das Engagement könnte zum Verlust von Top-Talenten führen, die einen persönlichen „White Glove“-Ansatz erwarten.
- **Rechtliche Compliance (EU AI Act):** Automatisierte Entscheidungsfindung im Beschäftigungskontext (z.B. ein Agent, der einen Lebenslauf automatisch ablehnt) wird im EU AI Act als „Hochrisiko“ klassifiziert. Banken müssen sicherstellen, dass bei Ablehnungsentscheidungen ein Mensch involviert bleibt („Human-in-the-Loop“), um DSGVO-Konformität (Art. 22) zu gewährleisten.

Use Case 7: Intelligente Kreditrisikoprüfung & Underwriting

Im Firmenkunden-, aber auch im Fördergeschäft ist die Kreditprüfung ein dokumentenintensiver, manueller Prozess. Ein „Underwriting Agent“ automatisiert die Erstellung der Kreditvorlage (Credit Memo). Der Agent liest unstrukturierte Bilanzen und GuV-Rechnungen (oft PDF-Scans), extrahiert Daten, berechnet Kennzahlen (DSCR, EBITDA) und vergleicht diese mit den Risikoricthlinien der Bank.

Folgende Funktionen deckt der Agent ab:

- **Ingest:** Upload der Jahresabschlüsse des Kunden und weiterer kreditrelevanter Parameter.
- **Extraction & Spreading:** Agent extrahiert KPIs, Kreditratings, Historie, KYC-Daten, Finanzkennzahlen mittels OCR und Vision-Modellen und überführt sie in das Standardformat der Bank.
- **Reasoning:** Analyse der Daten und Zahlen im Zeitverlauf und Vergleich mit Peer-Group-Daten. Unterstützung Risikoklassifizierung („Warum ist die Marge gesunken, obwohl der Umsatz stieg? Wer ist eigentlich wirtschaftlich Berechtigter?“).
- **Decision Support:** Erstellung eines formatierten Word-Dokuments für den Kreditausschuss inkl. SWOT-Analyse und Risikoeinschätzung.



Potenziale

- **Zeit:** Reduktion der "Time-to-Decision" um 25–40%. Dies ist ein enormer Wettbewerbsvorteil im Kampf um Firmenkunden.
- **Produktivität:** Relationship Manager können sich auf die Kundenbetreuung konzentrieren, statt Daten abzutippen.
- **Markt:** Studien zeigen, dass Agenten die End-to-End-Effizienz im Kreditprozess um ca. 30% steigern können.



Risiken

- **Risiko:** Bias in den Trainingsdaten könnten zu Diskriminierung führen (Verstoß gegen EU AI Act "High Risk" Anforderungen).

Use Case 8: Cash Management & Liquidity Planning

Der **Cash Management & Liquidity Planning Agent** transformiert das Corporate Treasury von einer reaktiven Berichtsfunktion zu einem proaktiven, autonomen Profit-Center. Traditionelle Treasury Management Systeme (TMS) basieren oft auf statischen Regeln und retrospektiven Berichten. Im Gegensatz dazu überwacht dieses agentenbasierte System kontinuierlich die Cash-Positionen über globale Tochtergesellschaften, mehrere Währungen und disparate Bankpartner hinweg in Echtzeit.

Dieser Agent besitzt die Autonomie, sogenannte „Smart Sweeps“ auszuführen. Er prognostiziert den täglichen Liquiditätsbedarf mittels prädiktiver Analytik, die Daten aus Vertriebsprognosen, Debitoren- und Kre-

ditorenbuchhaltungen (AP/AR) sowie makroökonomische Indikatoren integriert. Basierend auf dieser Prognose konzentriert der Agent autonom überschüssige Liquidität von Unterkonten auf ein Master-Konto, um Zinserträge zu maximieren (Cash Pooling).

Über das reine Pooling hinaus führt der Agent autonome Absicherungsgeschäfte (Hedging) durch. Erkennt er eine steigende FX-Volatilität, die den Risikoappetit des Unternehmens (definiert in der „Treasury Constitution“) übersteigt, kann er Termingeschäfte oder Optionen ausführen, um das Währungsrisiko abzusichern, ohne auf das Eingreifen eines menschlichen Händlers warten zu müssen. Er nutzt „What-If“-Szenariomodellierungen (z.B. Monte-Carlo-Simulationen), um die Liquidität gegen potenzielle Marktshocks, wie einen plötzlichen Kreditstopp oder den Ausfall eines Großkunden, zu stresstesten.



Potenziale

- **Ertragsoptimierung (Yield Optimisation):** Durch die Eliminierung von ungenutztem Bargeld ("Idle Cash") und die Ausführung von Sweeps rund um die Uhr (auch an Wochenenden dank Instant Payment Rails) stellt der Agent sicher, dass jeder Euro in Overnight-Funds oder Geldmarktinstrumenten investiert ist. Dies steigert das Zinsergebnis signifikant.
- **Reduktion von Sicherheitsbeständen:** Corporate Treasurer halten oft übermäßige Liquiditätspuffer vor, bedingt durch Unsicherheiten über tägliche Abflüsse. Die hohe Präzision KI-gestützter Prognosen (durch Integration von Echtzeit-ERP-Daten) erlaubt es Unternehmen, diese Puffer sicher zu reduzieren und das Kapital in renditestärkere strategische Investitionen umzuleiten.
- **Operative Resilienz:** In Momenten von Marktstress (z.B. Liquiditätsengpässe) kann menschliche Entscheidungsfindung langsam oder panikgetrieben sein. Ein Agent, der auf vorvalidierter Logik operiert, kann Einlagen sofort über mehrere Depotstellen diversifizieren, um das Kontrahentenrisiko zu minimieren.
- **Strategische Beratung:** Der Agent verschiebt die Rolle des Treasurers vom Datenaggregator zum strategischen Berater. Anstatt Stunden mit der Abstimmung von Cash-Positionen zu verbringen, prüft der Treasurer strategische Vorschläge des Agenten, wie etwa "Empfehlung zur Anpassung der Schuldenduration basierend auf der Zinskurvenanalyse des Agenten".



Risiken

- **Flash Crashes und Feedback-Schleifen:** Autonome Trading-Agenten, die auf dieselben Marktsignale reagieren, können Feedback-Schleifen erzeugen, die zu Flash Crashes in Währungs- oder Geldmärkten führen. Die Bank für Internationalen Zahlungsausgleich (BIS) warnt explizit vor der systemischen Fragilität durch KI-gesteuertes Liquiditätsmanagement.

- **Fragilität durch Überoptimierung:** Ein Agent, der darauf trainiert ist, den Ertrag zu maximieren, könnte Liquiditätspuffer auf ein gefährlich niedriges Niveau senken. Ohne ein umfassendes Verständnis für „Black Swan“-Risiken, die in seinen Trainingsdaten nicht vorhanden sind, könnte der Agent das Unternehmen zwar rechtlich solvent, aber in einer Krise illiquide zurücklassen.
- **Model Drift und Datenqualität:** Wenn zugrundeliegende Datenfeeds (z.B. aus einem ERP-System bezüglich erwarteter Zahlungseingänge) korrupt oder verzögert sind, trifft der Agent fehlerhafte Investitionsentscheidungen. Anders als ein Mensch, der einen plötzlichen Rückgang der Forderungen hinterfragen würde, könnte ein Agent blind auf die Daten reagieren, sofern keine spezifischen „Common Sense“-Leitplanken programmiert sind.

Use Case 9: Smart Audit & Internal Control Agent (Governance)

Der Smart Audit & Internal Control Agent markiert den Übergang von der periodischen, stichprobenbasierten Prüfung hin zum Continuous Control Monitoring (CCM). Dieser Agent residiert innerhalb der digitalen Infrastruktur der Bank und überwacht kontinuierlich Transaktionen, Nutzerverhalten und Systemprotokolle.

Im Gegensatz zu traditionellen Skripten, die nach einfachen Schwellenwertüberschreitungen suchen, nutzt dieser Agent semantisches Verständnis (Reasoning), um den Kontext von Kontrollen zu verstehen. Er kann beispielsweise neue regulatorische Richtlinien (z.B. ein Update zu Basel III, MaRisk oder SOX-Anforderungen) lesen, interpretieren und autonom Testskripte generieren, um die Einhaltung zu verifizieren.

Der Agent führt „Full-Population Testing“ durch, anstatt nur Stichproben zu ziehen. Er scannt 100% aller Hauptbucheinträge auf Anomalien, wie Buchungen zu ungewöhnlichen Zeiten (Wochenenden), durch ungewöhnliche Nutzer (IT-Mitarbeiter mit temporären Rechten) oder mit vagen Beschreibungstexten. Wird eine Anomalie erkannt, initiiert der Agent eine Untersuchung: Er fragt den Nutzer per E-Mail/ChatOps nach einer Erklärung, referenziert unterstützende Dokumente (Rechnungen, Genehmigungen) und entscheidet, ob der Alarm geschlossen oder mit einem vorbereiteten „Beweispaket“ an einen menschlichen Auditor eskaliert wird.



Potenziale

- **Totale Assurance-Abdeckung:** Der Übergang von der Prüfung von 5% der Transaktionen auf 100% bietet ein Maß an Sicherheit, das mit manuellen Methoden unmöglich ist. Dies reduziert das „Entdeckungsdefizit“, bei dem Betrug oder Fehler oft monatelang unbemerkt bleiben.

- **Prüfungseffizienz und Reduktion von „Alert Fatigue“:** Durch die Automatisierung der Beweiserhebung und der initialen Triage von Ausnahmen reduziert der Agent die manuelle Routearbeit der Revisionsfunktion drastisch. Dies verringert die Ermüdung durch Fehlalarme bei menschlichen Prüfern und erlaubt ihnen, sich auf komplexe Beurteilungen und strategische Risiken zu konzentrieren.
- **Echtzeit-Remediation:** Traditionelle Audits berichten Monate nach dem Vorfall. Ein agentisches System markiert Kontrollschwächen sofort (z.B. „Funktionstrennungskonflikt in der Kreditorenbuchhaltung erkannt“), sodass das Management die Lücke schließen kann, bevor sie ausgenutzt wird.
- **Regulatorisches Vertrauen:** Eine Bank, die nachweisen kann, dass sie kontinuierliches, KI-gesteuertes Monitoring nutzt, kann unter Umständen von geringeren Kapitalanforderungen oder einer weniger invasiven regulatorischen Prüfung profitieren, da die Robustheit des Kontrollumfelds demonstrierbar ist.



Risiken

- **„Wer prüft den Prüfer?“:** Ein signifikantes Risiko ist die „Black Box“-Natur des KI-Agenten selbst. Wenn die Logik des Agenten fehlerhaft oder voreingenommen ist, könnte er systematisch ungültige Transaktionen genehmigen. Die interne Revision muss sich weiterentwickeln, um den Code und die Logik der Agenten zu prüfen, nicht nur deren Outputs.
- **Adversarial Blindness (Gaming):** Sophisticiertere interne Betrüger, die die Parameter des Agenten verstehen, könnten Transaktionen spezifisch so gestalten, dass sie der Entdeckung entgehen (z.B. Stückelung von Transaktionen knapp unterhalb der Anomalieschwelle). Die Vorhersehbarkeit des Agenten wird zur Schwachstelle.
- **Datenschutz und Überwachung:** Das kontinuierliche Monitoring von Mitarbeiterverhalten (Tastenschläge, E-Mail-Kommunikation, Systemzugriffe) zur Erkennung von „Insider Threats“ wirft gravierende Datenschutzfragen auf. In Jurisdiktionen mit strengen Arbeitsgesetzen (wie Deutschland) könnte ein solches granulares Monitoring ohne strikte Governance und Beteiligung des Betriebsrats rechtswidrig sein.

Use Case 10: Der 24/7 HR-Concierge & Policy Agent

Der HR-Concierge Agent dient als „Tier 0“-Support für Mitarbeiter, der immer verfügbar ist. Anstatt statische Intranets oder PDF-Handbücher zu durchsuchen, unterhalten sich Mitarbeiter mit dem Agenten, um Fragen zu Urlaubsrichtlinien, Benefits, Gehaltsabrechnungsdifferenzen und interner Mobilität zu klären.

Dieser Agent nutzt Retrieval-Augmented Generation (RAG), um auf die umfangreiche Bibliothek von Richtlinien dokumenten der Bank zuzugreifen. Er kann komplexe, kontextabhängige Fragen beantworten wie: „Ich bin VP im Londoner Büro und gehe im November in Mutterschutz; wie wirkt sich das auf meine Bonusansprüche aus und welche Formulare benötige ich?“ Der Agent synthetisiert die Mutter-

schutzrichtlinie, die Bonusregeln und lokale Arbeitsgesetze, um eine präzise, personalisierte Antwort zu geben.

Er fungiert auch als transaktionaler Agent: „Trage 5 Tage Urlaub übernächste Woche in unser Urlaubssystem ein.“ Der Agent prüft das Urlaubssaldo, checkt den Teamkalender auf Deckungslücken und reicht den Antrag zur Genehmigung beim Manager ein.



Potenziale

- **Transformation der Employee Experience (EX):** Sofortige, akkurate Antworten auf administrative Fragen entfernen Reibung aus dem Arbeitsalltag. Dies ist besonders wertvoll für globale Banken, wo HR-Support oft in einer anderen Zeitzone sitzt.
- **Reduktion operativer Kosten:** IBMs Implementierung eines solchen Agenten („AskHR“) löste 94% der Anfragen ohne menschliches Eingreifen und sparte Millionen an operativen Kosten. Dies erlaubt HR-Generalisten, sich von der Ticketbearbeitung hin zur strategischen Personalplanung zu bewegen.
- **Richtlinienkonsistenz:** Menschliche HR-Vertreter geben mitunter inkonsistente Ratschläge basierend auf Gedächtnislücken. Der Agent liefert jedes Mal standardisierte, rechtlich geprüfte Antworten, was das Risiko von Falschinformationen bei sensiblen Themen wie Belästigungsmeldungen oder Abfindungen reduziert.



Risiken

- **Haftung für falsche Ratschläge:** Wenn der Agent halluziniert und falsche Ratschläge bezüglich Benefits oder Arbeitsrechten gibt (z.B. falsche Berechnung einer Abfindung), könnte die Bank rechtlich an die Zusage der KI gebunden sein. Es könnten Ansprüche aus sog. „Estoppel“ (Verwirkung) entstehen, wenn Mitarbeiter sich zum eigenen Nachteil auf das Wort der KI verlassen haben.
- **Interne Datenschutz-Leaks:** Mitarbeiter stellen der HR oft sensible Fragen (z.B. zu krankheitsbedingten Auszeiten, Rehabilitation oder Konflikten am Arbeitsplatz). Wenn der Gesprächsverlauf des Agenten nicht strikt segregiert ist oder wenn er aus diesen Interaktionen „lernt“ und Details an andere Nutzer leakt, schafft dies eine toxische Umgebung und rechtliche Haftung.
- **Verlust der menschlichen HR-Verbindung:** Für sensible Themen (Beschwerden, psychische Gesundheit) ist ein KI-Interface unangemessen. Wenn die Bank alle Interaktionen auf den Agenten schiebt, um Kosten zu sparen, riskiert sie, ihrer Fürsorgepflicht gegenüber vulnerablen Mitarbeitern nicht nachzukommen.

Use Case 11: Customer Service & Dispute Resolution Avatar

Über einfache Chatbots hinausgehend, können Agenten komplexe Kundenanliegen Ende-zu-Ende lösen. Beispiel: Ein Kunde meldet eine unberechtigte Lastschrift. Der Agent prüft die Transaktion, vergleicht sie mit vorliegenden Mandaten, leitet die Rückbuchung ein, sperrt ggf. die Karte und sendet eine Bestätigung – alles autonom im Core-Banking-System. Oder der Kunde sendet einen Screenshot der Fehlermeldung an die Bank inkl. einer Beschreibung der Situation.



Potenziale

- Banking Avatare, die rund um die Uhr Fragen beantworten und Kundenanliegen bearbeiten, können bis zu 75% der Anfragen autonom klären, was zu Kosteneinsparungen beim Personalbedarf im Supportbereich in Höhe von 20-50% bei gleichzeitig erhöhter Kundenzufriedenheit führen kann. Darüber hinaus reduziert die schnelle Lösung von Kundenproblemen die Hemmschwelle für Kunden mit Agenten zu interagieren.



Risiken

- Hoher Integrationsaufwand in Backend-Systeme. Risiko des "Uncanny Valley"-Effekts bei Avataren (das unbehagliche Gefühl, das Menschen empfinden, wenn sie auf menschenähnliche Abbildungen treffen) und Reputationsrisiko bei Fehlverhalten.

Use Case 12: Hyper-Personalisierung & „Next Best Action“

Dieser Use Case repräsentiert den Übergang vom generischen Marketing zur autonomen finanziellen Gesundheit (Financial Wellness). Der „Next Best Action“ (NBA) Agent operiert auf dem Kern-Datenlayer der Bank und synthetisiert Transaktionshistorien, Lebensereignisse (erkannt durch Ausgabenmuster, wie Babykleidung oder Hochzeitsanzahlungen) und Marktkontext.

Im Gegensatz zu statischen Regeln (z.B. „Wenn Saldo >10k, biete Festgeld an“) nutzt der Agent Reinforcement Learning, um die optimale Handlung für den langfristigen Wert des Kunden zu bestimmen. Er agiert als 24/7-Concierge.

- *Szenario:* Ein Kunde erhält einen großen Bonus. Der Agent erkennt diesen Geldeingang, analysiert das Sparziel des Kunden (Anzahlung für ein Haus) und initiiert proaktiv einen Chat: „*Ich sehe einen signifikanten Eingang. Basierend auf Ihrem Ziel, 2026 ein Haus zu kaufen, empfehle ich, diesen Betrag in einen hochverzinslichen Spartopf zu verschieben, um dieses Jahr 400 EUR extra zu verdienen. Soll ich das für Sie erledigen?*“.

Der Agent arbeitet kanalübergreifend (App, Web, Filiale) und behält den Kontext bei. Lehnt der Kunde das Angebot in der App ab, stellt der Agent sicher, dass der Filialmitarbeiter ihn nicht später mit demselben Angebot nervt, sondern vielleicht ein anderes, relevanteres Produkt vorschlägt.



Potenziale

- **Ausweitung des Share of Wallet:** Durch das Angebot zeitnaher, relevanter Ratschläge statt generischem Spam können Banken die Cross-Sell-Konversionsraten signifikant steigern. Daten von Salesforce legen nahe, dass Hyper-Personalisierung Umsatzwachstum und Kundenbindung treibt.
- **Finanzielle Inklusion:** Agenten können profitable, personalisierte Beratung auch für Massenmarkt-Kunden anbieten, die sich keinen menschlichen Finanzberater leisten können. Dies „demokratisiert“ das Wealth Management.
- Retention durch „Sticky Utility“: Eine Bank, die autonom die finanzielle Gesundheit eines Kunden managt (ungenutzte Abos kündigen, Sparen optimieren), wird zu einem Versorger („Utility“), den man nur schwer verlässt. Das Wertversprechen verschiebt sich von „Geld lagern“ zu „Leben optimieren“.



Risiken

- **Predatory Optimisation (Raubtier-Optimierung):** Es besteht ein Interessenkonflikt. Empfiehlt der Agent das Produkt, das für den Kunden am besten ist (z.B. Kreditkarte abbezahlen) oder für die Bank (Schulden halten und neuen Kredit aufnehmen)? Wenn Agenten Bankprofit auf Kosten der Kundengesundheit optimieren, lädt dies massive Conduct Risks und regulatorische Strafen ein.
- **Datenschutz und „Creepiness“:** Die Nutzung intimer Ausgabendaten (z.B. Wissen über eine Schwangerschaft vor der Bekanntgabe) kann die Grenze zur Überwachung überschreiten. Verletzungen der DSGVO durch unautorisierte Dateninferenz sind ein Hauptrisiko.
- **Verbraucherabhängigkeit und Atrophie:** Wenn Kunden blind den Finanzratschlägen des Agenten vertrauen, hören sie möglicherweise auf, sich um ihre eigenen Finanzen zu kümmern. Wenn der Agent einen Marktcrash nicht vorhersieht oder schlechten Rat gibt, wird der Kunde die Bank für seinen Ruin verantwortlich machen.

Use Case 13: Der autonome AML-Analyst

Die Bekämpfung von Geldwäsche (AML) bindet in Banken enorme personelle Ressourcen. Herkömmliche, regelbasierte Monitoringsysteme produzieren extrem hohe Raten an „False Positives“ (oft über 90–95%), die alle manuell von Analysten geprüft werden müssen. Dies führt zu „Alert Fatigue“ und hohen Kosten.

Ein Agentic AI System übernimmt hier die Rolle eines First Level-Analysten. Anders als ein statischer Filter „verstehen“ der Agent den Kontext. Er erhält einen Alert, sammelt autonom Zusatzdaten und trifft eine begründete Vorentscheidung.

Der Workflow des Agenten stellt sich wie folgt dar:

1. **Trigger & Kontext:** Der Agent empfängt einen Alert (z. B. „Verdächtige Transaktion über 50.000 EUR nach Panama“).
2. **Data Gathering (Werkzeugnutzung):** Der Agent fragt via SQL die Transaktionshistorie der letzten 12 Monate ab. Parallel ruft er via API externe Datenprovider (z. B. LexisNexis, Schufa) auf, um nach „Adverse Media“ zu suchen und prüft das Handelsregister auf wirtschaftlich Berechtigte.
3. **Reasoning (Graph Analysis):** Der Agent baut einen mentalen Graphen der Beziehungen auf. Er stellt Fragen wie: „Passt diese Transaktion zum Geschäftszweck des Kunden (z. B. Import/Export)?“ oder „Gibt es Verbindungen zu sanktionierten Entitäten über Ecken?“.
4. **Action & Reporting:** Kommt der Agent zum Schluss, dass der Alarm falsch war (z. B. Namensgleichheit, aber unterschiedliches Geburtsdatum), schließt er den Fall mit einer detaillierten Begründung. Bei echtem Verdacht eskaliert er an einen Second Level-Analysten und bereitet den Entwurf einer Verdachtsmeldung (SAR) vor.



Potenziale

- **Effizienz:** Reduktion der manuellen Bearbeitungszeit für Alerts um 40–60%. Ein Analyst, der bisher 20 Minuten pro Fall benötigte, wird auf die komplexen Fälle fokussiert, während der Agent die Masse in Sekunden vorprüft.
- **Kosten:** Bei großen Banken mit Hunderten von Compliance-Mitarbeitern liegen die Einsparpotenziale im zweistelligen Millionenbereich.
- **Qualität:** Senkung der False-Positive-Rate, die den Menschen erreicht, um bis zu 80% durch intelligenten, semantischen Vorfilter.



Risiken

- „Halluzination“ von Fakten in der Begründung. Regulatorische Anforderung an Erklärbarkeit (Explainability) ist extrem hoch. Wenn der Agent einen Geldwäscher übersieht, haftet die Bank.

Use Case 14: Autonomer IT-Operations & Incident Response Agent

Bank-IT-Systeme müssen rund um die Uhr verfügbar sein. Ausfälle kosten Millionen und schädigen das Vertrauen. „AIOps Agents“ überwachen Logs, Metriken und Traces. Bei einem Incident (z.B. Server-Überlastung, Datenbank-Lock) analysiert der Agent die Ursache (Root Cause Analysis), schlägt eine Lösung vor oder führt diese autonom durch (Self-Healing).

1. **Detection:** Der Agent bemerkt Anomalie in den Latenzzeiten.
2. **Diagnosis:** Der Agent korreliert Logs aus verschiedenen Systemen und identifiziert ein fehlerhaftes Deployment als Ursache.
3. **Remediation:** Der Agent führt ein Rollback auf die vorherige Version durch oder startet Services neu.
4. **Documentation:** Der Agent schreibt einen Post-Mortem-Bericht im Ticketsystem (z.B. Service-Now).



Potenziale

- **Stabilität:** Reduktion der Mean Time to Repair (MTTR) um 30–50%.
- **Kosten:** Einsparung von teuren nächtlichen Bereitschaftseinsätzen und Vermeidung von Ausfallkosten (im Banking ca. 10.000 – 15.000 EUR pro Minute Downtime).



Risiken

- Falsche, autonome Entscheidungen des Agenten können hohe Schäden anrichten und müssen über Kontrollmechanismen ausgeschlossen werden.

Use Case 15: Autonomes Onboarding & Employee Lifecycle Management

Der Autonomous Onboarding Agent fungiert als Brücke zwischen HR, IT und Sicherheit. Sobald ein Kandidat ein Angebot annimmt, orchestriert dieser Agent den komplexen Bereitstellungsprozess, der in Banken aufgrund strikter Zugriffskontrollen oft Tage dauert.

Der Agent löst Workflows aus, um E-Mail-Konten zu erstellen, Hardware zu bestellen und Zugriffe auf spezifische Bankensysteme (z.B. Bloomberg-Terminals, Kernbankmodule) strikt basierend auf der Rolle des Mitarbeiters (RBAC - Role Based Access Control) zu gewähren. Er verifiziert Identitätsdokumente (Pässe, Visa) mittels Computer Vision und gleicht diese mit Regierungsdatenbanken ab, um Arbeitserlaubnisse zu prüfen.

Über den Tag 1 hinaus erstellt der Agent einen personalisierten „Lernpfad“. Er identifiziert Lücken in den Fähigkeiten des neuen Mitarbeiters relativ zu seiner Rolle und schreibt ihn automatisch in obligatorische Compliance-Schulungen (AML, KYC) sowie technische Weiterbildungen ein. Er „stupst“ (nudging) den Mitarbeiter zur Erledigung an und berichtet den Fortschritt an das Management.



Potenziale

- **Produktivität ab Tag 1:** In vielen Banken warten neue Mitarbeiter wochenlang auf vollen Systemzugriff. Der Agent stellt „Zero-Day Readiness“ sicher, indem er alle Tools bereitstellt, bevor der Mitarbeiter das Gebäude betritt (oder sich remote einloggt), was zu sofortiger Produktivität führt.
- **Sicherheit und Compliance:** Durch die Automatisierung der Rechtevergabe basierend auf strikten Richtlinien eliminiert der Agent „Permission Creep“ (bei dem Mitarbeiter einfach die Rechte des Vorgängers kopiert bekommen, inkl. unnötiger Altrechte). Er stellt sicher, dass das Prinzip der minimalen Rechtevergabe (Least Privilege) von Anfang an durchgesetzt wird.
- **Skalierbarkeit:** In Phasen rapider Expansion (z.B. Start einer neuen Digitalbank) oder bei M&A-Integrationen kann der Agent tausende Mitarbeiter gleichzeitig onboarden, ohne den HR- oder IT-Service-Desk zu überlasten.



Risiken

- **„Orphaned Identity“ Angriffe:** Ein großes Sicherheitsrisiko ist die Entstehung von Identitäten, die nicht sauber de-provisioniert werden. Wenn der Agent versäumt, Zugriffe bei Kündigung sofort zu widerrufen, oder wenn der Agent selbst kompromittiert wird, kann er zum „Super-User“ werden, der unautorisierten Akteuren Zugriff gewährt.
- **Unpersönliche Integration:** Onboarding ist kulturell, nicht nur logistisch. Ein überautomatisierter Prozess könnte dazu führen, dass sich neue Mitarbeiter isoliert fühlen. Dem Agenten fehlt die emotionale Intelligenz, um zu spüren, wenn ein neuer Mitarbeiter Schwierigkeiten hat, sich einzufinden.
- **Datenschutz-Aggregationsrisiken:** Der Agent verarbeitet extrem sensible persönliche Daten (Steuerformulare, IDs, Biometrie). Wenn der Agent diese Daten durch eine „Prompt Injection“-Attacke oder eine Halluzination in einem Chat-Interface leakt, stellt dies einen massiven DSGVO-Verstoß dar.

4.3 Softwarelösungen für Agentic AI

Für die Umsetzung von Agentic-AI-Vorhaben stehen unterschiedliche Softwarelösungen zur Verfügung, die sich in vier Gruppen einteilen lassen:

1. **Open-Source-Programmierplattformen**, die ein hohes Maß an Flexibilität und Herstellerunabhängigkeit bieten.
2. **Spezialisierte Workflow- und Agentic-Software**, die entweder als Erweiterung bestehender Tools entstanden ist oder von Grund auf als native AI-Agenten-Plattform konzipiert wurde.

3. **LLM-integrierte Lösungen** großer Modellanbieter, die durch die enge Verzahnung von Sprachmodell und Agentenfunktionen überzeugen, zugleich jedoch Abhängigkeiten von einzelnen Anbietern mit sich bringen können.
4. **Große Cloud- und Enterprise-Ökosysteme**, die AI-Agenten nahtlos in bestehende Unternehmenslandschaften integrieren.

Die Auswahl der geeigneten Lösung hängt stets von den individuellen Anforderungen und dem jeweiligen Ausgangskontext ab. In der Praxis kommen häufig unterschiedliche Plattformen parallel zum Einsatz, um verschiedene Anwendungsfälle abzudecken. Es ist sinnvoll, die Auswahl von Agentic Banking Lösungen professionell begleiten zu lassen. Auch hier trennt sich gegenwärtig die Spreu vom Weizen. Nicht jeder Lösungsanbieter hat in allen Feldern Stärken. Speziell für Banken sind Governance Aspekte, Replizierbarkeit und Nachvollziehbarkeit von Ergebnissen schlicht Grundvoraussetzung. Zudem ist der Markt nicht statisch, sondern einzelne Lösungsanbieter punkten mit raschen Weiterentwicklungszyklen.

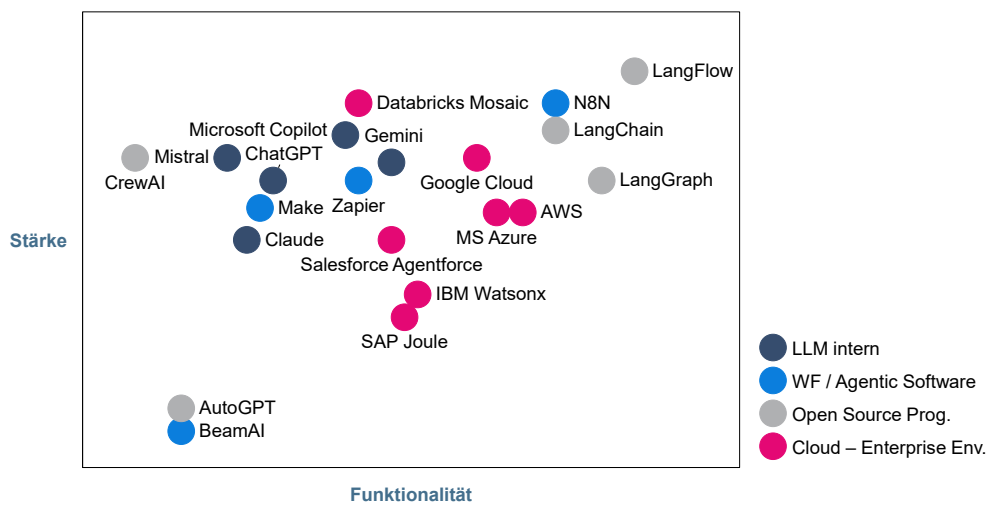


Abbildung 6: Der AI-Agenten Kompass

5. HANDLUNGSEMPFEHLUNG

Agentic AI ist keine ferne Zukunftsvision, sondern eine technologische Realität, die bereits von Vorreitern aktiv pilotiert und eingesetzt wird. Die Technologie markiert den Übergang von der starren Prozessautomatisierung zur flexiblen, kognitiven Prozessbearbeitung. Für Banken ergeben sich daraus vier klare Handlungsempfehlungen:



Starten Sie jetzt, aber fokussiert:

Identifizieren Sie Use Cases mit hohem Volumen und klaren Regeln (z.B. KYC, IT Ops), um erste Erfahrungen mit der Autonomie zu sammeln, bevor Sie sich an komplexe Kundeninteraktionen wagen.



Investieren Sie in die Datenbasis:

Ohne saubere Daten und zugängliche APIs sind Agenten blind und handlungsunfähig. Investitionen in die Modernisierung der Legacy-Schnittstellen und Datenarchitektur sind unumgängliche Voraussetzungen.



Denken Sie „Human-in-the-Loop“:

Agentic AI soll den Banker nicht ersetzen, sondern augmentieren („Bionic Banking“). Bauen Sie Governance-Strukturen auf, die sicherstellen, dass kritische Entscheidungen menschlich validiert bleiben und die KI als Partner agiert.



Setzen Sie ein interdisziplinäres Team auf:

Der Einsatz von KI erfordert viele unterschiedliche Perspektiven und Erfahrungen. Ein integratives und breit aufgestelltes Team mit den notwendigen Vorerfahrungen ist wichtig, um schnell relevante und messbare Ergebnisse erzielen zu können.

Die Bank der Zukunft wird eine hybride Organisation sein, in der Menschen und KI-Agenten kollaborativ zusammenarbeiten.

Wer diesen Wandel jetzt aktiv gestaltet und die Risiken managt, sichert sich signifikante Wettbewerbsvorteile in Effizienz, Geschwindigkeit und Kundenerlebnis. Banking wird aktuell neu definiert. Seien Sie mit dabei!

ÜBER MOONROC

MOONROC ist eine führende Managementberatung. Strategischer Weitblick, Ergebnisorientierung und unternehmerische Umsetzbarkeit sind unsere Leitlinien. Wir verstehen uns als ganzheitlich denkender Partner für Unternehmer und Management. Unsere Berater kennzeichnet ihr führendes fachliches Know-how, langjährige operative Berufserfahrung und die Fähigkeit, innovative Strategien entwickeln und umsetzen zu können. Dabei bauen wir auf drei elementare Grundwerte: Qualität, Engagement und Aufrichtigkeit.

Treten Sie mit uns in Kontakt:



+49 (0) 151 42 20 29 10



company@moonroc.de



Dr. Torsten Stuska

Managing Partner

Strategie | Transformation | M&A



Patrick Natus

Managing Partner

Strategie | IT & Operations | Programm-Management



Thomas Linnemann

Partner

Transformation | Restrukturierung | Programm-Management



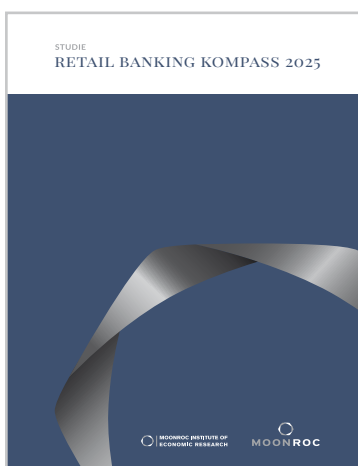
Michael Oettinger

Senior Advisor

Künstliche Intelligenz | Datenanalyse
Dozent für KI (Hochschule der Medien – Stuttgart)

PUBLIKATIONEN

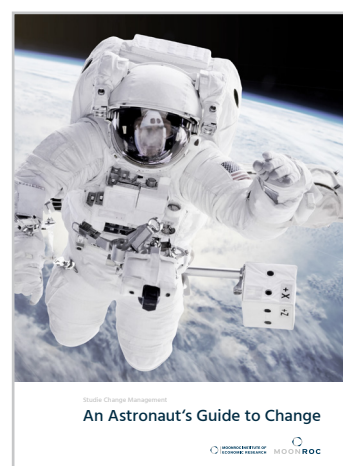
MOONROC veröffentlicht seit 15 Jahren die größte Bankenstudie in Deutschland. Darüber hinaus publiziert MOONROC regelmäßig Artikel und Studien zu markttreibenden Entwicklungen in Financial Services und Travel & Transport sowie in Themengebieten wie Künstliche Intelligenz oder Change-Management.



[Retail Banking Kompass 2025](#)



[Firmenkundenstudie 2025](#)



[An Astronaut's Guide to Change](#)

Diese und weitere Publikationen finden Sie unter: www.moonroc.de/insights/artikel

HAFTUNGSAUSSCHLUSS

Die Darstellungen und Analysen in dieser Publikation stellen, soweit nicht anders vorhanden, Schätzungen dar. Trotz größter Sorgfalt können sich die Inhalte, Daten und Informationen inzwischen verändert haben. Eine Haftung oder Garantie für die Richtigkeit, Aktualität und Vollständigkeit der zur Verfügung gestellten Inhalte, Daten und Informationen kann nicht übernommen werden. Des Weiteren behält sich MOONROC das Recht vor, Änderungen oder Ergänzungen der bereitgestellten Inhalte, Daten und Informationen jederzeit vorzunehmen. Struktur, Inhalt und Daten dieser MOONROC-Publikation sind urheberrechtlich geschützt. Die Vervielfältigung von Informationen oder Daten, insbesondere die Verwendung von Texten, Textteilen oder Bildmaterial, bedarf der vorherigen schriftlichen Zustimmung der MOONROC Advisory Partners GmbH.

