

Zeitschrift für erfolgsorientierte Unternehmenssteuerung

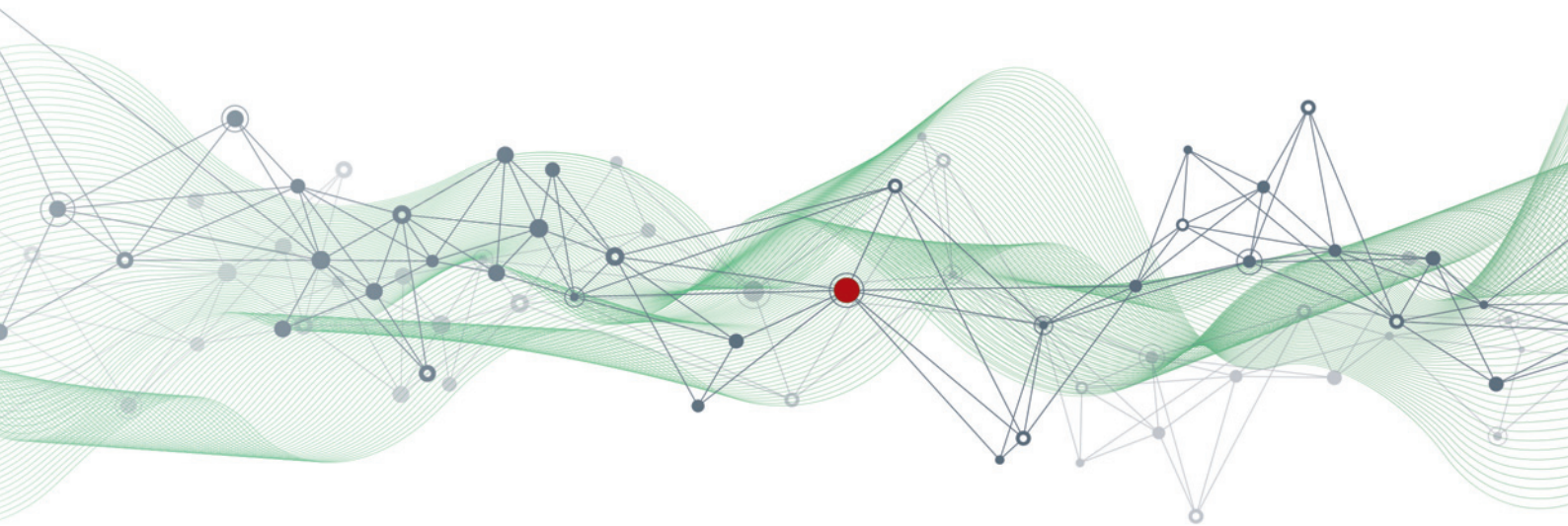
CONTROLLING

Herausgegeben von Ulrike Baumöl, Martin R. W. Hiebl, Andreas Hoffjan, Thorsten Knauer, Klaus Möller, Burkhard Pedell
Gegründet von Péter Horváth und Thomas Reichmann

www.zeitschrift-controlling.de

Oktober 2026 · 38. Jahrgang · Verlage C.H.BECK · Vahlen · München · Frankfurt a.M.

5|2026



SCHWERPUNKT

CONTROLLING VON GROSSEN SOFTWARE-MIGRATIONSPROJEKTEN

Ganzheitliche Steuerung für nachhaltigen Erfolg

Strategisches Projektcontrolling der
ERP-Migration

Wertbeitrag statt nur Go-live –
Ganzheitliches Controlling für
nachhaltige IT-Transformationen

Objectives and Key Results in
der Unternehmenspraxis

Überwindung der KI-Governance Policy-Practice Gap

Ein strukturelles Modell für das regulierte Finanzsystem



Dr. **Holger Harms** wirkt im Swisscom Banking Innovation Lab, um Innovationen im Bankenwesen voranzutreiben.



Dr. **Mena Teebken** ist Postdoktorandin am Lehrstuhl für Business Engineering der Universität St. Gallen (HSG) mit Fokus auf Data Governance in digitalen Ökosystemen.

Die Governance künstlicher Intelligenz (KI) im Finanzsektor steht vor einer strukturellen Herausforderung: Während FINMA und EU AI Act normative Anforderungen definieren, fehlen Übersetzungsmechanismen zwischen Richtlinien und technischen Systemen weitgehend. Der Beitrag diagnostiziert diesen Policy-Practice Gap und operationalisiert Governance über ein Vier-Quadranten-Modell als geschlossenen Regelkreis.

Holger Harms, Mena Teebken, Denise Gubser und Reinhard Jung

1. KI kontrollieren, aber wie? Die Governance-Lücke im Finanzsektor

Der Finanzsektor durchläuft eine tiefgreifende technologische Transformation. Getrieben durch die Verfügbarkeit großer Datenmengen und Fortschritte im Bereich der generativen KI (GenAI) expandiert der Einsatz algorithmischer Systeme von unterstützenden Back-Office-Tätigkeiten hin zu kritischen Entscheidungsprozessen: Auf KI beruhende Systeme steuern zunehmend die Kreditvergabe, die Betrugserkennung, das algorithmische Trading und die direkte Kundeninteraktion. Diese Transformation erzeugt ein folgenreiches Spannungsfeld. Traditionelle Software liefert bei gleicher Eingabe stets identische Ergebnisse, KI-Systeme hingegen arbeiten stochastisch und weisen oft (als «Black-Box») eine geringe Transparenz respektive Erklärbarkeit auf. Die etablierten Instrumente des Risikomanagements stoßen daher an ihre Grenzen. Sie wurden für lineare, zeitinvariante Modelle entwickelt und versagen oft bei der Überwachung adaptiver, nicht-linearer Systeme. Einerseits zwingt der Wettbewerbsdruck Finanzinstitute zur schnellen Einführung dieser Technologien, andererseits kollidiert die probabilistische, oft intransparente Natur moderner KI-Systeme mit den deterministischen Anforderungen an das Bankwesen und mit den Erwartungen der Regulatoren.

Das eigentliche Problem ist dabei kein Mangel an normativen Grundlagen. Transparenz, Fairness, Robustheit und Rechenschaftspflicht gelten global als Kernprinzipien vertrauenswürdiger KI (vgl. Floridi/Cowls, 2022; Jobin et al., 2019). Die Aufsichts-

erwartungen der FINMA (Eidgenössische Finanzmarktaufsicht, die Schweizer Aufsichtsbehörde für Banken und Finanzinstitute) und Regulierungsrahmen wie der EU AI Act haben diese Anforderungen inzwischen rechtlich verankert, während internationale Standards wie die ISO/IEC 42001 konkrete Leitfäden für deren praktische Umsetzung und Auditierung liefern. Die Frage, wie abstrakte normative Anforderungen in die technische Infrastruktur eines Finanzinstituts übersetzt werden, bleibt weitgehend offen. Dies führt wiederum zu Herausforderungen bei der Governance der KI. Normative Prinzipien («Policy») bleiben wirkungslos, solange sie nicht in die technischen Produktionsprozesse («Practice») integriert werden. Diese Diskrepanz zwischen normativen Vorgaben und technischer Wirklichkeit stellt einen «Policy-Practice Gap» dar, welcher Ausgangspunkt des vorliegenden Beitrags ist.

Die Praxis im Finanzsektor zeigt, dass normative Führungsmechanismen etabliert werden, diese jedoch oft von der technischen Validierung entkoppelt bleiben (vgl. Batool et al. 2025). Ein effektives Governance-Modell muss daher Mechanismen beinhalten, die diese Entkopplung aktiv verhindern und normative Anforderungen zwingend mit der technischen Umsetzung verbinden. Gelingt diese Kopplung, entstehen strukturierte Regelkreise, durch die Abweichungen zwischen normativen Vorgaben und technischer Realität frühzeitig sichtbar werden und eine Korrektur ermöglichen. Dieser Beitrag entwickelt ein Vier-Quadranten-Modell der KI-Governance, das die Governance-Aufgabe entlang zweier Achsen strukturiert: Auf der horizontal-

len Achse wird zwischen Organisation und KI-System unterschieden, weil bestehende Regulierungsrahmen diese beiden Ebenen getrennt adressieren und eine integrierte Steuerung beider Ebenen in der Praxis bislang fehlt. Auf der vertikalen Achse wird zwischen qualitativer und quantitativer Bewertung differenziert, weil normative Prinzipien erst dann operativ wirksam werden, wenn sie in messbare, technisch durchsetzbare Kriterien übersetzt sind. Das Modell disaggregiert Governance in vier klar definierte Steuerungsbereiche, verbunden durch explizite Schnittstellen und Kopplungsmechanismen.

Der Beitrag ist wie folgt aufgebaut: Kapitel 2 analysiert die theoretischen Ursachen des Policy-Practice Gap. Kapitel 3 entwickelt das Vier-Quadranten-Modell und legt seine Praxisherkunft dar. Kapitel 4 leitet Implikationen für Führungskräfte ab. Kapitel 5 schliesst mit Fazit und Ausblick. Obwohl der vorliegende Beitrag sich auf den Finanzsektor als Anwendungskontext konzentriert, ist die Grundarchitektur des Vier-Quadranten-Modells sektorunabhängig. Die Trennung von normativer Vorgabe, operativer Umsetzung und technischer Kontrolle ist eine strukturelle Anforderung überall dort, wo KI-Systeme in regulierten oder sicherheitskritischen Umgebungen eingesetzt werden.

2. Zwischen Norm und Code: Warum Prinzipien allein scheitern

Die wissenschaftliche Auseinandersetzung mit KI-Governance hat in den letzten Jahren erheblich an Breite gewonnen, jedoch nicht an operativer Tiefe. Batool et al. (2025) zeigen in einer systematischen Analyse des aktuellen Forschungsstands, dass die Mehrheit der Governance-Artefakte normative Anforderungen formuliert und Richtlinien entwickelt, diese jedoch meist isoliert und ohne technische Operationalisierung bleiben. Nur wenige Ansätze decken alle Phasen des KI-Lebenszyklus ab. Konsistente Durchgängigkeit und explizite Rückkopplungsmechanismen fehlen fast vollständig. Die zentrale Frage «How is it governed?» bleibt in der Literatur und in der Praxis weitgehend abstrakt. Ethische KI wird formuliert, aber ohne messbare Kriterien, ohne systematische Übersetzung in technische Kontrollen und ohne automatisierte Durchsetzung. Die meisten Governance-Lösungen sind entweder organisatorisch-strategisch oder technisch punktuell, aber selten beides in systemischer Kopplung.

Die frühe KI-Governance-Forschung hat einen breiten normativen Konsens geschaffen: Jobin et al. (2019) identifizierten fünf globale Kernprinzipien: Transparenz, Gerechtigkeit, Nicht-Schädigung, Verantwortung und Privatsphäre. Floridi und Cowls (2022) ergänzten die Erklärbarkeit. Was fehlt, ist nicht der normative Rahmen, sondern seine technische Operationalisierung. Begriffe bleiben abstrakt und liefern keine verbindlichen Übersetzungsver-

fahren von der Regulation oder Norm zum Code (vgl. Mittelstadt, 2019). Finanzinstitute reagieren darauf oft mit formalen Strukturen, die Konformität signalisieren, ohne die technischen Kernprozesse zu steuern (vgl. Meyer/Rowan, 1977). Das Resultat hiervon ist eine reine «Papier-Compliance».

Das Ergebnis ist der diagnostizierte Policy-Practice Gap: Banken verfügen über KI-Governance-Strategien, aber nicht über Mechanismen, die sicherstellen, dass diese Strategien das tatsächliche Verhalten der KI-Systeme beeinflussen. Was fehlt, ist keine weitere Richtlinie, sondern eine operative Architektur, die normative Anforderungen zwingend mit technischer Umsetzung verbindet und Entkopplung strukturell verhindert. Genau diese Architektur entwickelt das nachfolgende Kapitel.

3. Die Lücke schliessen: Wie ein strukturiertes Modell Norm und Code verbindet

Praxisherkunft und Forschungsansatz

Ausgangspunkt des Modells war der Austausch mit Schweizer Banken, Verbänden und weiteren Providern, gestützt auf Selbstauskünfte von 18 Instituten im Rahmen einer strukturierten Umfrage zur «KI Governance, Risk und Compliance». Die gewonnenen Einsichten wurden in mehreren Runden mit Praktikern validiert und anschliessend mit der Literatur zu Data Governance und KI-Governance konzeptionell verdichtet. Es kristallisierten sich drei Beobachtungen heraus:

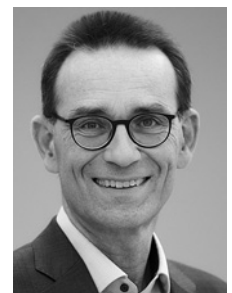
- Die heute im Kontext der KI-Governance angewendeten Vorgaben und Standards setzen eine organisations- oder systembezogene Perspektive voraus. Risiken werden entweder auf Ebene der Organisation als operationelle, rechtliche und reputationsbezogene Risiken des Instituts erfasst (etwa in der FINMA-Aufsichtsmitteilung 08/2024 oder in ISO 42001) oder auf Ebene eines einzelnen KI-Systems mit definiertem Zweck über dessen Lebenszyklus hinweg bewertet (EU AI Act).
- Die Aussagen der Befragten sind überwiegend qualitativer, seltener quantitativer Natur.
- Die Übersetzung qualitativer Aussagen in quantitative Metriken gelingt umso eher, je höher die Maturität der befragten Person oder Organisation ist.

Zentrale Aussagen

- Der Policy-Practice Gap entsteht nicht durch fehlende Regulierung, sondern durch das Fehlen einer Architektur, die Normatives mit Prozessen und Technik verbindet.
- Das Vier-Quadranten-Modell strukturiert KI-Governance als geschlossenen PDCA-Regelkreis und wirkt der Entkopplung von Strategie sowie prozessualer und technischer Realität strukturell entgegen.
- Governance-as-Code und Boundary Objects überführen abstrakte Compliance-Anforderungen in automatisierbare, messbare Kontrollmechanismen.



Denise Gubser, M.A., befasst sich im Swisscom Banking Innovation Lab mit der Identifikation und Bewertung strategisch relevanter Innovationsfelder im Bankensektor.



Prof. Dr. Reinhard Jung ist Ordinarius für Business Engineering an der Universität St. Gallen (HSG) sowie Akademischer Direktor des Executive MBA HSG in Business Engineering.

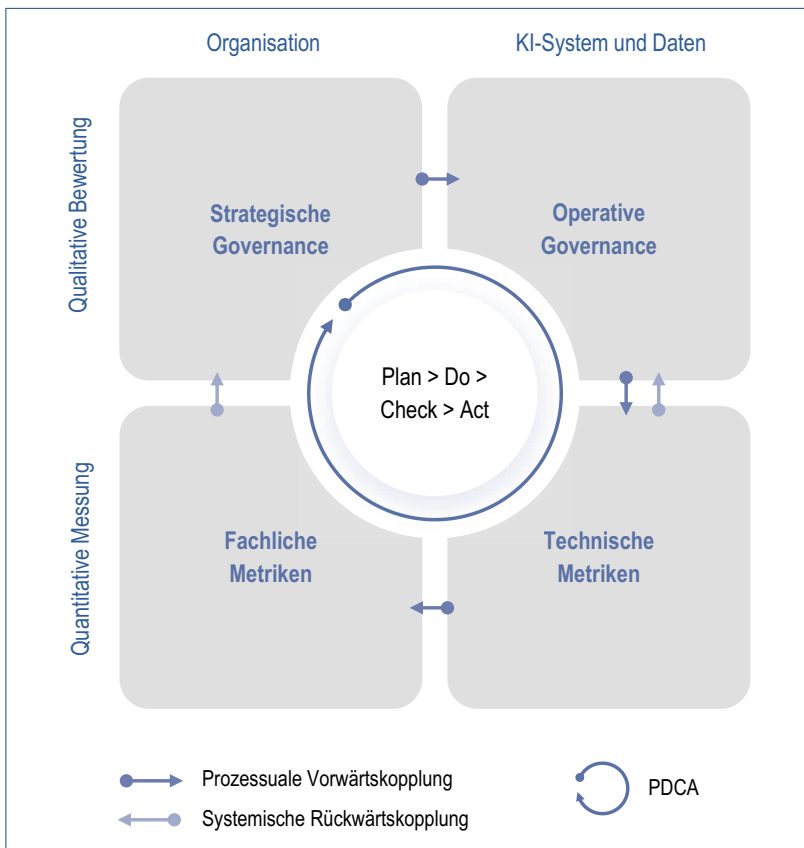


Abb. 1: Das Vier-Quadranten-Modell der KI-Governance

Die dritte Beobachtung ist für das Modell zentral: Sie verweist auf die Kernherausforderung der Governance, normative Setzungen in messbare Kriterien zu überführen. Das ist genau jene Übersetzungsleistung, die in der Literatur weitgehend fehlt.

Herleitung des Modells

Der hier vorgestellte Lösungsansatz liegt in der Disaggregation des Governance-Problems in zwei Dimensionen, die getrennt bearbeitet, aber über definierte Schnittstellen koordiniert werden. Der wesentliche Beitrag dieses Ansatzes liegt im Verständnis von Governance als konfigurierbarem System aus Mechanismen statt als monolithischem Block. Damit KI-Governance funktioniert, müssen zwei Differenzierungen explizit gemacht werden: «Was wird bewertet?» und «Wie wird bewertet?». Diese beiden Fragen spannen die Achsen des Modells auf.

- **Die horizontale Dimension** (Geltungsbereich) greift die erste Beobachtung auf: Da bestehende Regulierungsrahmen entweder eine organisations- oder eine systembezogene Perspektive einnehmen, differenziert das Modell entsprechend: Die «Organisation» (Makro-Ebene) verortet im Modell die aggregierte juristische und ökonomische Verantwortung sowie die strategische Steuerung. Das «KI-System» (Mikro-Ebene) legt den Fokus auf das spezifische KI-Artefakt, also jene technische Instanz, auf der sich regulatorische Verstöße operativ manifestieren.

- **Die vertikale Dimension** (Methodik) greift die zweite Beobachtung auf: Da Aussagen in der Praxis überwiegend qualitativer Natur sind, erzwingt das Modell die explizite Unterscheidung zwischen normativem Anspruch und messbarer Evidenz. «Qualitative Bewertungen» umfassen wertbasierte Einschätzungen wie Risikoappetit-Erklärungen, abstrakte Begriffe wie Transparenz, Robustheit, Erklärbarkeit oder juristische Interpretationen. Diese sind notwendig für normative Setzungen, die sich noch nicht messen lassen. «Quantitative Bewertungen» umfassen objektive, datengetriebene Messungen wie Logs, Metriken und statistische Tests, die essenziell für reproduzierbare Beweisführung und technische Kontrolle sind.
- Die dritte Beobachtung, dass die Übersetzung qualitativer in quantitative Aussagen mit steigender Maturität gelingt, motiviert schließlich die **Schnittstellen** zwischen den Quadranten als zentrales Steuerungselement des Modells.

Abb. 1 visualisiert das Vier-Quadranten-Modell als dynamischen Regelkreis. Die vier Quadranten – Strategische Governance (Q1), Operative Governance (Q2), Technische Metriken (Q3) und Fachliche Metriken (Q4) – sind entlang der Achsen angeordnet. Die dunkelblauen Pfeile zeigen die prozessuale Vorwärtskopplung (Q1 → Q2 → Q3 → Q4), die hellblauen Pfeile die systemische Rückkopplung (Q4 → Q1 und Q3 → Q2). Das zentrale PDCA-Symbol (Plan → Do → Check → Act) verdeutlicht, dass das Modell keine statische Matrix, sondern ein geschlossener Regelkreis ist.

Quadrant 1: Strategische Governance

Der erste Quadrant beinhaltet die normative Setzung für KI-Einsatz in der Organisation. In diesem strategischen Bereich werden der gewünschte Soll-Zustand definiert und die ethische Wertebasis festgelegt. Die Umsetzung erfolgt primär über strukturelle Maßnahmen, wie die Etablierung spezifischer Rollen sowie die klare Zuweisung von Verantwortlichkeiten. Ein wesentlicher Aspekt ist zudem der Aufbau von KI-Kompetenz («AI Literacy») im Management, um fundierte Entscheidungen zu ermöglichen. Zu den zentralen Ergebnissen dieses Quadranten gehören die KI-Strategie, die Risikoappetit-Erklärung sowie Leitlinien oder Weisungen für den Einsatz von KI. Wichtig ist, dass qualitative Aussagen über den Einsatz von KI getroffen werden und diese die Organisation betreffen.

Die größte Herausforderung besteht hier in der Gefahr der Entkopplung, bei der Strategien reine Theorie bleiben, wenn sie nicht operativ verankert werden. Dieser Quadrant schafft zwar Legitimität, bleibt aber ohne die nachfolgenden Schritte wirkungslos.

Quadrant 2: Operative Governance

Im zweiten Quadranten findet die prozedurale Übersetzung der abstrakten Strategie in konkrete Projekte statt. Dies ist das Feld der klassischen Compliance-Prüfung und des Risikomanagements, wobei die Bewertung typischerweise als ex-ante Kontrolle vor der Inbetriebnahme eines Systems erfolgt. Zu den Kernaktivitäten gehören die Durchführung von Folgenabschätzungen, die Klassifizierung von KI-Systemen in verschiedene Risikokategorien sowie die Benennung konkreter Risikoverantwortlicher für das jeweilige System. Die Aussagen betreffen das KI-System und sind qualitativer Natur.

Ein kritischer Punkt dieses Quadranten ist, dass er sich häufig auf manuelle Selbstauskünfte stützt. Dies macht den Prozess anfällig für subjektive Fehleinschätzungen oder übertriebenen Optimismus. Ohne eine technische Validierung bleibt dieser Schritt oft ein formeller Akt, der keine Garantie für die tatsächliche Sicherheit der Systeme bietet.

Quadrant 3: Technische Metriken

Der dritte Quadrant adressiert die Lücke zwischen Vorschrift und Technik, indem er Governance von einer administrativen Anforderung zu einer intrinsischen Systemeigenschaft transformiert. Der Fokus liegt hier auf der kontinuierlichen und automatisierten Messung von technischen Eigenschaften des KI-Systems, sowie der Durchsetzung von Regeln während der Entwicklung und des laufenden Betriebs. Insbesondere kann und muss überwacht werden, ob sich Eigenschaften von Daten, dem KI-System oder der Nutzung über die Zeit ändern.

Durch das Konzept der «Governance-as-Code» können Vorschriften in maschinenlesbare Regeln übersetzt werden. Einerseits ist es wichtig, auf der Vorwärtskopplung qualitative Aussagen in quantitative Aussagen zu übersetzen. Eine qualitative Vorgabe wie «Mitarbeitende sollen Zugriff auf einen sicheren und benutzerfreundlichen Chatbot erhalten» lässt sich etwa so in maschinenlesbare Regeln überführen: «KI-System A der Risikokategorie B soll Anwendern der Rolle C den Zugriff auf Daten D mit Kritikalität E erlauben und dabei Kontrollen der Kategorie F anwenden». Mindestens so wichtig ist die Übersetzung quantitativer Aussagen in qualitative Aussagen. Während des laufenden Betriebs eines KI-Systems müssen schleichende Verhaltensänderungen eines KI-Systems («Drifts») quantifiziert werden und in qualitative Aussagen überführt werden. Beispielsweise kann die Robustheit eines KI-Systems von «Very Good» auf «Fair» sinken, wenn ein höherer Satz künstlich injizierter Angriffe auf das KI-System nicht abgeblockt wird. In beiden Fällen (qualitativ zu quantitativ und vice versa) wird zur Schließung der Policy-Practice Gap die Governance als maschinenlesbare Regel im Code umgesetzt und deren Einhaltung systematisch sichergestellt.

Quadrant 4: Fachliche Metriken

Der vierte Quadrant schliesst den Kreis, indem er den Nutzen von KI für die Organisation quantifiziert. Hier erfolgt eine rückblickende Gesamtbewertung fachlicher Metriken auf Organisationsebene. Im Mittelpunkt stehen die Messung der Rendite von KI-Initiativen, die Überwachung der Betriebskosten sowie die Prüfung der Ressourceneffizienz. Ein (internes oder externes) Audit überprüft zudem, ob das gesamte Governance-System wirksam arbeitet.

Die Funktion dieses Quadranten ist essenziell für die Regelung, denn er liefert die objektive Datenbasis für das Management. Zeigen die Daten, dass Kosten steigen, Risiken zunehmen oder der Nutzen sinkt, muss die strategische Ausrichtung in entsprechenden Quadranten angepasst werden.

Schnittstellen zwischen den Quadranten

Ein statisches Modell aus isolierten Quadranten würde der Komplexität adaptiver KI-Systeme nicht gerecht werden (vgl. Abraham et al., 2019; Gasser & Almeida, 2017), das gilt insbesondere im Finanzumfeld. Die Effektivität der Governance entscheidet sich an den Schnittstellen zwischen den Quadranten, die den Informationsfluss zwischen den Dimensionen sicherstellen und das Risiko der Entkopplung minimieren. An diesen Schnittstellen werden Artefakte übergeben, die von verschiedenen Akteuren gleichermaßen verstanden und genutzt werden können. Solche übergebenen Artefakte werden «Boundary Objects» genannt. Besonders relevant für die Schließung des Policy-Practice Gap sind die Übergänge zwischen qualitativer und quantitativer Bewertung: zum einen die Vorwärtskopplung, die normative Vorgaben in technische Realität überführt, zum anderen die Rückkopplung, die Messergebnisse zurück an die Governance-Ebene spielt. Beispiele für beide Richtungen zeigen [Abb. 2](#) und [Abb. 3](#).

Prozessuale Vorwärtskopplung

Dieser Pfad beschreibt die Durchsetzung normativer Vorgaben in technische Realität und deren anschließende ökonomische Bewertung. Er folgt der Logik von Q1 bis Q4 und ist in [Abb. 2](#) dargestellt.

Systemische Rückkopplung

Die Rückkopplung von Informationen ist für eine reflexive Managementpraxis essenziell. Es ergeben sich zwei dominante Pfade für die Rückkopplung von Informationen an den Übergängen in der Methodik, welche in [Abb. 3](#) abgebildet sind.

4. Was Führungskräfte jetzt tun sollten

Die Erkenntnisse des Vier-Quadranten-Modells lassen sich in vier konkrete Handlungsfelder übersetzen, die Führungskräfte im Finanzsektor priorisieren sollten. Eine Gap-Analyse entlang der einzel-

Banken verfügen über KI-Governance, aber nicht über Mechanismen, die sicherstellen, dass diese Strategien das tatsächliche Verhalten der KI-Systeme regeln.

Mechanismus	Quadrant	Beispiele
Normative Umsetzung	Q1 → Q2	Dieser Übergang beschreibt den Schritt von der abstrakten Strategie zur konkreten Projektplanung. Hier werden die in Q1 definierten, unternehmensweiten strategischen Vorgaben (wie Risikoappetit, Verantwortlichkeiten, Richtlinien) auf den spezifischen Anwendungsfall in Q2 heruntergebrochen. Auf Basis der allgemeinen «KI-Richtlinie» aus dem Q1 werden beispielsweise Assessments abgeleitet, die zur Risikoklassifizierung eines KI-Systems im Q2 nötig sind. Dieser Schritt stellt sicher, dass kein Projekt ohne Klärung der normativen Rahmenbedingungen in die Umsetzung geht. Ein Boundary Object im Kontext der KI-Governance ist beispielsweise eine Definition von Rollen und Verantwortlichkeiten, die als Artefakte aus dem Q1 im Q2 genutzt werden, um die Verantwortlichkeiten in Freigabeprozessen von konkreten KI-Systemen umzusetzen.
Technische Umsetzung	Q2 → Q3	Der Übergang von qualitativen Anforderungen (Q2) zu quantitativer technischer Durchsetzung (Q3) stellt eine anspruchsvolle Herausforderung dar, da hier abstrakte juristische und ethische Konzepte in konkrete Anweisungen übersetzt werden müssen. Die Übersetzungsleistung geschieht wieder mit Boundary Objects. An diesem Übergang werden insbesondere prozedurale Definitionen aus dem Q2 in maschinenlesbare Kontrollen im Q3 übertragen. Zuvor wurde dies als «Governance-as-Code» eingeführt. Ein einfaches Beispiel ist die Definition, wie oft, wie umfangreich und mit welchen Toleranzbändern ein KI-System während des Betriebs (Q3) entsprechend einer zugeteilten Risikokategorie (Q2) evaluiert wird.
Ökonomische Validierung der technischen Systeme	Q3 → Q4	Während Q3 rohe Telemetriedaten und technische Metriken liefert, benötigen Entscheidungsträger in Q4 aggregierte Informationen über den geschäftlichen Einfluss. Dieser Übergang leistet eine Übersetzungsarbeit von technischen Metriken in geschäftsrelevante Risikokennzahlen und finanzielle Metriken. Dies ermöglicht es dem Management, den technischen Zustand ökonomisch zu bewerten. Die Boundary Objects können an dieser Stelle eine Liste von zu übertragenden Metriken sein. Für ein KI-System können dies Aussagen sein wie Anzahl Nutzer, Anzahl Aufrufe, Anzahl verbrauchter Token, Antwortzeiten, Anzahl Folgefragen, Anzahl blockierter Zugriffe, Anzahl von Support-Fällen und so weiter.

Abb. 2: Beispiele für Vorwärtsskopplung entlang der Quadranten

Mechanismus	Quadrant	Beispiele
Strategische Anpassung	Q4 → Q1	Dieser (Makro-)Rückfluss schließt den großen Regelkreis des Managementsystems. Erkenntnisse aus der ökonomischen Validierung in Q4 fließen zurück an die strategische Ebene in Q1. Dies entspricht dem «Act»-Schritt im PDCA-Zyklus: Das System lernt evidenzbasiert auf organisationaler Ebene aus der Summe seiner Projekte.
Operative Adjustierung	Q3 → Q2	Neben dem strategischen Zyklus existiert eine kontinuierliche (Mikro-)Rückkopplung zur dynamischen Risikoadjustierung. Die operative Messung von Metriken der KI-Systeme in Q3 liefert Echtzeitdaten zu deren Performance. Treten plötzliche Anomalien auf oder wird eine schleichende Änderung des Modellverhaltens («Drift») gemessen, werden diese Informationen unmittelbar an Q2 zurückgespielt. In Q2 kann dann die Neubewertung des sogenannten Modellrisikos erfolgen und schließlich eine Anpassung des operationellen Risikos vorgenommen werden. Die Stakeholder der operativen Governance aus Q2 haben somit ein aktuelles Risikobild. Durch eine programmatische Umsetzung der Governance-as-Code Methodik kann auch eine Abschaltung des KI-Systems bei einem gemäß Governance inakzeptablen Risikos erfolgen.
Es können weitere Kopplungen definiert werden, jedoch sind zur Schließung der Policy-Practice Gap jene Schnittstellen bei Übergängen in der Methodik (qualitativ und quantitativ) am relevantesten.		

Abb. 3: Beispiele für Rückkopplung entlang der Quadranten

nen Quadranten liefert die Basis für eine priorisierte Roadmap.

- **Governance als Regelkreis verankern, nicht als Dokumentationspflicht:** Das Modell entfaltet seine Wirkung erst durch den geschlossenen PDCA-Regelkreis: Von der normativen Setzung (Q1) über die operative Übersetzung (Q2) und technische Kontrolle (Q3) bis zur ökonomischen Validierung (Q4) und zurück. Der vierte Quadrant schließt dabei den Regelkreis, indem er die technische Leistung der KI-Systeme in betriebswirtschaftlichen Nutzen ausdrückt und so die Datenbasis für strategische Anpassungen in Q1

liefert. Strategien, die nicht operativ verankert werden, bleiben wirkungslos.

- **Boundary Objects als Übersetzungsbrücken einsetzen:** Insbesondere der Übergang von Q2 nach Q3 ist eine anspruchsvolle Schnittstelle, an der abstrakte juristische und ethische Konzepte in technisch durchsetzbare Artefakte überführt werden müssen. Dies erfordert interdisziplinäre Teams mit ausgeprägten Übersetzungskompetenzen, also Fachpersonen, die sowohl die normative Sprache der Risikoexperten als auch die formale Logik der Data Scientists verstehen. Diese Investition in «Boundary Objects»

ist keine weiche Maßnahme, sondern eine strukturelle Voraussetzung dafür, dass die in Q2 definierten Anforderungen in Q3 überhaupt wirksam werden können.

- **Governance-as-Code als regulatorische Notwendigkeit betrachten:** Wer Governance-Anforderungen konsequent in technische Kontrollmechanismen überführt, schafft damit die strukturellen Voraussetzungen zur Erfüllung regulatorischer Pflichten. Finanzinstitute sollten die dafür notwendigen Investitionen in interdisziplinäre Kompetenzen und technische Infrastruktur entsprechend nicht als Kostenfaktor, sondern als strategische Absicherung gegenüber wachsendem regulatorischen Druck sowie gegenüber finanziellen und reputationsbezogenen Risiken einordnen.
- **KI-Kompetenz im Management aufbauen:** Q1 funktioniert nur, wenn das Management fundierte Entscheidungen über den KI-Risikoappetit treffen kann. Der Aufbau von KI-Kompetenz («AI Literacy») im Management und in der Organisation ist dafür unabdingbar. Dies ist als zentrales Ergebnis von Q1 beschrieben und vom EU AI Act (Art. 4) als explizite Pflicht verankert. Das erfordert kein tiefes technisches Verständnis, aber ein belastbares Bild davon, was KI-Systeme können, wo sie versagen und welche spezifischen Risiken ihre probabilistische Natur mit sich bringt.

5. Vom Policy-Practice Gap zur Systemeigenschaft: Fazit und Ausblick

Das entwickelte Vier-Quadranten-Modell adressiert den Policy-Practice Gap durch eine strukturierte Disaggregation der Governance-Aufgabe entlang zweier Achsen. Zentraler Beitrag des Modells ist die Schließung der Lücke zwischen strategischer Absicht und operativer Realität: Durch den Einsatz von «Boundary Objects», insbesondere «Governance-as-Code» wird das Phänomen der «Entkoppelung» technisch unterbunden. Normative Anforderungen werden so in reproduzierbare, quantifizierbare technische Evidenz übersetzt. Dieser Ansatz schafft die grundlegende Voraussetzung und liefert eine belastbare Compliance-Architektur, um die Auditierbarkeit sowohl gemäß gesetzlichen Rahmenwerken (wie von der FINMA oder dem EU AI Act) als auch nach internationalen Standards wie der ISO/IEC 42001 sicherzustellen. Für Führungskräfte im Finanzsektor bedeutet das Modell vor allem eines: KI-Governance wirkt nur als geschlossener Regelkreis, von der normativen Setzung über die technische Kontrolle bis zur ökonomischen Validierung. Wer Governance lediglich als Dokumentationspflicht versteht, wird den regulatorischen Anforderungen langfristig nicht gerecht.

Das Modell ist im Kontext bestehender Forschung als Brücke zu verstehen: Es schließt die von

Implikationen für die Praxis

- Governance als Regelkreis verankern: KI-Governance wirkt nur als geschlossener PDCA-Zyklus, von normativer Setzung über operative Übersetzung und technische Kontrolle bis zur ökonomischen Validierung.
- Boundary Objects als Übersetzungsbrücken: Interdisziplinäre Teams müssen juristische Anforderungen in technisch durchsetzbare Artefakte überführen – strukturelle Voraussetzung, keine weiche Maßnahme.
- Governance-as-Code als Notwendigkeit: Die Überführung von Governance-Anforderungen in technische Kontrollen ist strategische Absicherung gegen Regulierungs- und Reputationsrisiken, kein Kostenfaktor.
- KI-Kompetenz im Management aufbauen: AI Literacy im Management und in der Organisation ist notwendig (EU AI Act, Art. 4): kein Tiefen-Know-how, aber ein belastbares Bild der Risiken probabilistischer KI-Systeme.

Batool et al. (2025) diagnostizierte Lücke zwischen isolierten Governance-Artefakten und konsistenter Lifecycle-Abdeckung und übersetzt die von Mittelstadt (2019) identifizierten strukturellen Defizite in konkrete organisationale und technische Gegenmaßnahmen. Damit ergänzt es die bestehende Literatur nicht durch ein weiteres normatives Framework, sondern durch ein operatives Strukturierungsinstrument. Das Vier-Quadranten-Modell schafft damit die konzeptuellen Voraussetzungen für die nachfolgende Etablierung von Boundary Objects und die Operationalisierung durch Governance-as-Code-Mechanismen. Für die Forschung eröffnet dies mehrere Anschlusspunkte: insbesondere die Entwicklung standardisierter Metriken je Quadrant sowie die Untersuchung der Übertragbarkeit auf andere regulierte Sektoren. Eine empirische Validierung, auch im Hinblick auf Agentic AI und generative KI, ist in Vorbereitung.

Literatur

- Abraham, R./Schneider, J./Vom Brocke, J., Data governance: A conceptual framework, structured review, and research agenda, in: International Journal of Information Management, 49. Jg. (2019), S. 424–438.
- Batool, A./Zowghi, D./Bano, M., AI governance: a systematic literature review, in: AI and Ethics, 5. Jg. (2025), S. 1–15.
- Floridi, L./Cowls, J., A unified framework of five principles for AI in society, in: Carta, S. (Hrsg.), Machine learning and the city: Applications in architecture and urban design, Hoboken 2022, S. 535–545.
- Gasser, U./Almeida, V. A., A layered model for AI governance, in: IEEE Internet Computing, 21. Jg. (2017), H. 6, S. 58–62.
- International Organization for Standardization, Information technology – Artificial intelligence – Management system (ISO/IEC 42001:2023), 2023.
- Jobin, A./Ienca, M./Vayena, E., The global landscape of AI ethics guidelines, in: Nature Machine Intelligence, 1. Jg. (2019), H. 9, S. 389–399.

- Meyer, J. W./Rowan, B., Institutionalized organizations: Formal structure as myth and ceremony, in: American Journal of Sociology, 83. Jg. (1977), H. 2, S. 340–363.
- Mittelstadt, B., Principles alone cannot guarantee ethical AI, in: Nature Machine Intelligence, 1. Jg. (2019), H. 11, S. 501–507.

Literaturtipps auf inlibra.com:

- AI-Governance als strategisches Instrument, Richard Sentinella, Victoria Honsel, Maël Schnegg, 2024/6, S. 39–42
- Controlling von KI, Valentin Wittmann, Aljoscha Roloff, 2025/5, S. 43–51
- Lösungsansätze für den erfolgreichen Einsatz von KI im Controlling, Niklas Gebert, Christoph Ertl, 2025/6, S. 46–54

Stichwörter

AgenticAI # AI-Act # FINMA # Governance-as-Code # Policy-Practice Gap

Keywords

AgenticAI # AI-Act # FINMA # Governance-as-Code # Policy-Practice Gap

Summary

AI governance in financial institutions faces a structural challenge: while FINMA and the EU AI Act define normative requirements, translation mechanisms between policy and technical systems are largely absent. This paper diagnoses this as the Policy-Practice Gap and develops a four-quadrant model that operationalises governance as a closed control loop.