THE AI-READY BOARD

by
Rene Schmidli

Rene Schmidli

Rene Schmidli, ein Finanzexperte mit über 30 Jahren Investmenterfahrung, deckte bereits 1993 als Finanzanalyst den Technologiesektor ab und begleitete im Jahre 2000 ein Tech-IPO in der Schweiz. Heute arbeitet er selbstständig in verschiedenen Verwaltungsrats- und Beratungsfunktionen. Im Dezember 2024 schrieb er, motiviert von der rasanten Entwicklung bei AI, seine CAS-Arbeit über Generative AI bei Mateusz Dolata an der Universität Zürich, um eine praxisnahe Betrachtung von AI-Strategie- und Governance-Themen in Verwaltungsräten vorzunehmen.

«Menschen optional?»: Was Agentic AI für Unternehmen bedeutet

Professor Dr. Oliver Gassmann

Oliver Gassmann ist Professor für Technologie und Innovationsmanagement und Geschäftsführender Direktor des Instituts für Technologiemanagement der Universität St. Gallen. Er ist Co-Gründer von „Seconds", ehemals BMI Lab, sowie Vice-Chairman und Partner von Zühlke.

Er ist Koautor des globalen Bestsellers "The Business Model Navigator" sowie „Collaborative Advantage: How Open Organizations Thrive in Volatility".

«The Agentic Enterprise» - Aspekte, die ein Verwaltungsrat wissen muss

Rene Schmidli: Oliver, herzlichen Dank, dass Du Dir Zeit nimmst. Im breiten, allgemeinen Verständnis assoziiert man AI vor allem mit Chatbots oder Tools wie ChatGPT, die Fragen beantworten oder Empfehlungen abgeben. Dann gibt es AI Agents, die autonomer daherkommen und bereits etwas «beängstigender», weil nicht ganz durchschaubar, wirken. Aber was genau ist Agentic AI, und warum sprichst Du in Deinen aktuellen Publikationen vom „nicht-menschlichen Unternehmen"? Für viele Führungskräfte ist das noch sehr abstrakt. Kannst Du kurz erklären, was ein agentisches Unternehmen ausmacht und warum das insbesondere für Verwaltungsräte jetzt zunehmend relevant wird?

Oliver Gassmann: Guten Tag, Rene. Gerne. Bisher war AI für die meisten Unternehmen eine Hilfskraft: Algorithmen geben Empfehlungen; Systeme bringen Vorschläge oder regen zum Denken an, **Chatbots** beantworten Fragen. Die eigentliche Entscheidung trifft aber immer noch der Mensch.

AI Agents sind der nächste Schritt: Das sind autonome Software-Entitäten, die selbständig Ziele verstehen, (Teil-)Aufgaben planen und ausführen, ohne dass ein Mensch bei jedem Schritt eingreifen muss. Wir sind mitten in einer neuen Technologie, die Entscheidungen nicht nur unterstützt, sondern ersetzt.

Agentic AI geht noch einen entscheidenden Schritt weiter. Hier arbeiten mehrere solcher Agenten als echtes digitales Team zusammen, als Multi-Agenten-System. Jeder Agent hat seine spezifischen Aufgaben und Fähigkeiten. Man kann sich das als ein Team aus smarten digitalen Kollegen vorstellen, die genau wie Menschen zusammenarbeiten, nur viel schneller und ohne Pausen. Sie folgen dabei grob quasi immer demselben Muster, fast wie ein Mensch, der eine Aufgabe löst:

Think: Sie schauen sich die Welt an: Sie analysieren nicht nur ihr internes Wissen, sondern zapfen (live) externe Quellen an (über APIs greifen sie auf CRM-, ERP-, Web-Daten, Social-Media-Feeds oder Sensoren zu). Es ist, als würden sie ihre „Augen" öffnen und die aktuelle Lage prüfen.

Plan: Dann überlegt und «denkt» der Agent mittels seines grossen «Hirns» (dem LLM-Teil, also den mächtigen Foundation Models): „Was ist der beste Schritt-für-Schritt-Plan, um das Ziel zu erreichen?" Wie ein Schachspieler, der mehrere Züge vorausdenkt.

Act: Das Wesentliche kommt aber erst jetzt; er handelt wirklich, d.h. entscheidet und setzt um. Dabei benutzt der Agent Tools als seine «Hände». Er schreibt E-Mails, ändert Preise, passt Lagerbestände an, steuert Maschinen oder nimmt Netz-Konfigurationen vor, alles direkt über Schnittstellen zu den echten Systemen. Kein „nur vorschlagen", sondern echtes Tun.

Reflect: Zum Schluss schaut er in den Spiegel: „Hat es funktioniert? Wo war ein Fehler? Was lerne ich daraus?" Er korrigiert sich selbst und wird mit jedem Durchlauf besser. Dieser Schritt ist immens wichtig.

Ein Agentisches Unternehmen, provokant habe ich es in einem frühen Beitrag «the non-human enterprise» genannt, ist genau das: ein Verbund solcher autonomer Agenten, die ganze Wertschöpfungsketten fast ohne ständige menschliche Eingriffe steuern. Das Agentische Unternehmen ist eine Vision der Automatisierung, ähnlich wie man in den 80er Jahren mit dem Aufkommen von Robotern die erste Beiträge einer mannlosen Fabrik hatte – heute bereits eine verbreitete Realität in einigen chinesischen Unternehmen.

Die Grenze zwischen Mensch und System verschwimmt: Software wird zum nicht-menschlichen Akteur im Unternehmen. Wer das ignoriert, riskiert, dass Wettbewerber Organisation, Effizienz, Skalierbarkeit und Kundenerlebnis komplett neu definieren und man über kurz oder lang abgehängt wird.

Rene Schmidli: Konzeptionell ist das nun gut erklärt. Erläutere doch gerne einige reale Beispiele, um das Theoretische zu konkretisieren.

Oliver Gassmann: Das mache ich gerne, weil es eben längst nicht mehr Fiktion oder Theorie allein ist, sondern sehr real. Neben operativen Aspekten sind es insbesondere strategische Gesichtspunkte, welche dermassen relevant sein können, dass ein Nichtbeachten geschäftskritisch wird.

Da wäre zum einen die **Deutsche Telekom**. Sie begegnet in der Steuerung moderner Mobilfunknetze einer zentralen Hürde: unvorhersehbare Lastspitzen bei „Grossevents", von Konzerten über Stadionbesuche bis zu Verkehrsstaus, überfordern lokal die Netzkapazität. Bisher mussten Experten jede Funkzelle über etwa 60 Minuten manuell optimieren, was nur rund 1.000 Ereignisse pro Jahr erlaubte. Diesen Engpass löst die Telekom mit Agentic AI. Ein Multi-Agenten-System übernimmt den gesamten Prozess: Ein Event-Agent erkennt Lastspitzen proaktiv über Web-Daten, ein Monitoring-Agent prognostiziert Kapazitätsprobleme, und ein Remediation-Agent setzt Netzkonfigurationen in Echtzeit um. Dadurch sinkt die Reaktionszeit von einer Stunde auf unter 60 Sekunden, das System bewältigt 40.000 Ereignisse jährlich; eine Vervierzigfachung der Effizienz. Mit 75 % Autonomie wandelt sich die Netzwerksteuerung von reaktiv zu proaktiv und erreicht eine Skalierbarkeit und Geschwindigkeit, die menschlich nicht mehr darstellbar wäre.

Mit der neuen Funktion „Buy for Me" demonstriert **Amazon** die strategische Stärke agentischer AI im Endkundenmarkt. Das zentrale Problem vieler Konsumenten liegt in der Fragmentierung des Online-Handels: Produkte müssen auf verschiedenen Plattformen gesucht, verglichen und einzeln gekauft werden. Amazon beseitigt diese Reibungsverluste, indem ein AI-Agent als autonomer digitaler Einkäufer agiert. Er überschreitet Plattformgrenzen, wählt Varianten, zahlt verschlüsselt und integriert alle Schritte nahtlos in die vertraute Amazon-Oberfläche. Diese Innovation verändert die Marktlogik fundamental: Innerhalb von sechs Monaten stieg das Angebot durch diesen Ansatz von 65.000 auf über 500.000 Produkte. Eine fast achtfache Skalierung. Indem Amazon externe Käufe direkt in die eigene App einbindet, etabliert sich der Konzern als Meta-Plattform des globalen Handels und sichert Zugriff auf Kundenschnittstellen und Datenströme jenseits des

eigenen Marktes. Für Markenhersteller bedeutet das eine neue Realität: Nicht mehr sie, sondern intelligente Agenten entscheiden, welche Produkte sichtbar bleiben und im Warenkorb des Kunden landen.

Rene Schmidli: Die konkreten Beispiele haben gezeigt: Der entscheidende Sprung ist somit von «passiver Intelligenz» zu aktiver Handlungsfähigkeit. Agenten sind keine reinen Sprachmodelle mehr. Sie sind autonome Systeme mit Gedächtnis, Planung, Tool-Nutzung und anschliessender Reflektion. Gibt es eine gängige Taxonomie zu Agentenstrukturen oder andere Möglichkeiten, sich zu orientieren, wenn man das abtiefen will?

Oliver Gassmann: Ja, es gibt verschiedene Frameworks, welche Orientierung liefern und sehr detailliert sein können. Ich möchte hier aber nur auf die wichtigsten Übergruppen von Agenten eingehen. Die Bandbreite reicht von simplen **Reflex-Agenten**, die ohne Gedächtnis unmittelbar auf Reize reagieren (Strassenampeln, Spamfilter), bis hin zu **deliberativen Systemen**, die dank eines Gedächtnisses aus Erfahrungen lernen (komplexe Routen, etwa für Lieferdrohnen) und vorausschauend planen. Während **ziel- und nutzenbasierte Agenten** darauf programmiert sind, knappe Vorgaben wie eine GPS-Route oder eine Gewinnmaximierung eines Handelssystems präzise zu erfüllen, entwickeln **intelligente Agenten** durch stetiges Lernen eine eigene Anpassungsfähigkeit, wie wir sie heute von modernen Empfehlungssystemen (E-Commerce) kennen.

Interface-Agenten dienen als personalisierte Schnittstelle zum Menschen und interagieren direkt mit Nutzern, lernen häufig aus deren Verhalten, um personalisierte Unterstützung zu bieten (smarte Sprachassistenten wie Alexa), während **kollaborative** und **hierarchische Agenten** in vernetzten Ökosystemen zusammenarbeiten. Sie koordinieren als Team digitale Prozesse oder steuern in Fabriken komplexe Produktionsabläufe über mehrere Ebenen hinweg. Hier verschwimmen die Grenzen zwischen einfacher Software und einem „digitalen Kollegen", der eigenständig kommuniziert und delegiert.

Besonders entscheidend für die strategische Führungsebene sind jedoch die **Guardian Agents**, die Wächter des Systems. Sie fungieren als unverzichtbare Instanz für Compliance, Risikokontrolle und Transparenz, indem sie sicherstellen, dass alle Akteure innerhalb definierter Leitplanken und ethischer Standards agieren. Während andere Agenten auf Effizienz und Zielerreichung getrimmt sind, sorgen die Guardian Agents für die notwendigen Guardrails. Sie sind das regulatorische Rückgrat einer agentischen Organisation: Ohne ihre ständige Validierung würde aus produktiver Autonomie unkontrollierbares Chaos entstehen. Man sieht bei Open Claw, wie Agenten auch völlig aus dem Ruder laufen können, wenn es keine klare Governance und konkrete Kontrollloops gibt. Letztere müssen nicht der berühmte Human-in-the-Loop sein, es könnten eben auch spezialisierte Agenten übernehmen.

Erfolgreiche Implementierungen kombinieren diese Typen bewusst je nach Prozesskomplexität, Risiko und Umfeld. So entsteht ein robustes, anpassungsfähiges Multi-Agenten-Ökosystem.

Rene Schmidli: Wo liegen nun die grössten Wettbewerbsvorteile, die sich Unternehmen, welche Agentic AI forcieren, erarbeiten?

Oliver Gassmann: Die zwei genannten Beispiele gaben einen ersten Eindruck. Allgemeiner gefasst entfalten Agentische AI-Systeme ihre Wirkung entlang fünf strategischer Dimensionen.

Das erste Motiv ist **radikale Effizienz**: Agenten operieren kontinuierlich, ohne die biologischen Grenzen menschlicher Arbeitskraft. Sie komprimieren Entscheidungszyklen, erhöhen den Durchsatz und ermöglichen eine neue Taktung operativer Prozesse, von der Planung über die Ausführung bis zur Qualitätssicherung.

Das zweite Motiv ist **Kostenreduktion** und **Reallokation**: Automatisierung senkt den Ressourcenaufwand für Routineprozesse strukturell. Die freiwerdenden Mittel, Budget wie Aufmerksamkeit, können in höherwertige Tätigkeiten umgeschichtet werden, sofern Unternehmen diesen Spielraum bewusst nutzen.

Das dritte Motiv ist **Skalierbarkeit** über **Komplexitätsgrenzen hinweg**: Agentische Systeme sind nicht auf einfache Wiederholungsaufgaben beschränkt. In orchestrierten Verbünden koordinieren sie komplexe, systemübergreifende Prozessketten und werden dabei mit jeder Iteration lernfähiger.

Das vierte Motiv ist **Kontextadaptivität** («Hyperpersonalisierung»): Agentische Systeme ersetzen generische Regeln und Standardprozesse durch kontextspezifische Entscheidungen. Sie analysieren situative Parameter in Echtzeit: Zustand, Nachfrage, Profil, Ressourcenlage und leiten daraus maßgeschneiderte Reaktionen ab (z.B. Preise, Aktivitäten, Timing). Das Prinzip gilt gleichermassen im Kundenkontakt wie in der Fertigung, der Wartung oder der Angebotsgestaltung: Überall dort, wo Einheitslösungen systematisch Wert verschenken, wird Adaptivität zum Wettbewerbsvorteil. Damit werden Geschäftsmodelle profitabel, die auf individuelle Ansprache in grossem Masstab angewiesen sind.

Das fünfte Motiv ist **Sicherheit** und **Risikoreduktion**: In hochsensitiven Umgebungen (Chemie, der Energieversorgung, der Logistik oder im Bergbau) übernehmen agentische Systeme kontinuierliche Überwachungs- und Steuerungsaufgaben. Sie erkennen kritische Zustände frühzeitig (predictive maintenance), reagieren autonom und reduzieren sowohl operative als auch regulatorische Risiken.

Rene Schmidli: Die gezeigten Beispiele regen den unternehmerischen Appetit an. Welches Drehbuch empfiehlst Du, wenn nun ein Verwaltungsrat denkt, er wolle beginnen, weiss aber nicht wie und wo?

Oliver Gassmann: Gerne. Zuallererst gilt festzuhalten: Strategie und Kundenwert muss an oberster Stelle stehen. Daraus abgeleitet kann man Bereiche identifizieren, bei denen der Einsatz von datenbasierter, automatisierter Wertschöpfung Sinn macht. Dies ist wichtig, da Technologie nur Mittel zum Zweck ist.

Hat man diese strategischen Felder identifiziert, so hat sich aus meiner Erfahrung in der Praxis folgende dreistufige Vorgehensweise bewährt:

Stufe 1: Der wirksamste Einstieg in agentische AI beginnt nicht mit der grossen Vision, sondern mit dem richtigen ersten Schritt: kleinen, klar abgegrenzten Prozessen mit hohem Volumen und geringer Mehrdeutigkeit. Standardisierte Supportanfragen, Bestellprozesse oder Basisdisposition bieten ideale Bedingungen, weil dort Fehler früh sichtbar werden und der Mensch noch eng eingebunden bleibt. Viele Industrieunternehmen haben genau so angefangen, mit einzelnen Agenten für Qualitätskontrolle oder Anomalieerkennung und dabei das Entscheidende gelernt: nicht die Technologie ist die erste Hürde, sondern das Vertrauen der Organisation in das Zusammenspiel von Mensch und Maschine.

Stufe 2: Sobald erste Agenten stabil laufen, folgt der strategisch bedeutsamere Schritt: die Verbindung zu End-to-End-Prozessketten. Von der Bestellung über die Lagerdisposition bis zur Auslieferung entsteht so ein kohärentes System, das nicht mehr punktuell, sondern durchgängig wirkt. DHL hat diesen Weg bereits beschritten. Routenplanung, Computer-Vision-Anwendungen und Robotik sind dort zu integrierten Logistikketten verwoben. Damit ein solches System verlässlich bleibt, braucht es den erwähnten Guardian-Agenten, der Risiken überwacht und Regelkonformität sichert, sowie klare Eskalationspfade: Der Verwaltungsrat muss wissen, wer verantwortet wann, wenn das System an seine Grenzen stösst, also eine klare Governance-Frage.

Stufe 3: Die dritte Stufe ist eine strategische Frage, keine operative: Welche Teile des Geschäftsmodells können prinzipiell ohne kontinuierliches menschliches Eingreifen funktionieren, und welche neuen Wertversprechen werden dadurch möglich? Spezialisierte Trading-Units, automatisierte Servicezentren oder personalisierte Produktwelten im E-Commerce sind keine Zukunftsszenarien mehr, sondern heute realisierbar. Der entscheidende Unterschied zu bisherigen Automatisierungslogiken: Es geht nicht primär um Kostensenkung, sondern um Leistungsmerkmale, die menschliche Organisationen strukturell nicht erreichen, in Geschwindigkeit, Verfügbarkeit und Individualisierung. Damit agentische Geschäftsmodelle skalieren und Vertrauen gewinnen, müssen Governance, Compliance und klare Verantwortlichkeiten von Beginn an mitgedacht werden, nicht als Bremse, sondern als Grundlage nachhaltiger Handlungsfähigkeit.

Rene Schmidli: Was sind z.T. bereits heute aber sicher künftig die Implikationen auf die Führung von Unternehmen, insbesondere der Verwaltungsrat im Zusammenhang mit Agentic AI?

Oliver Gassmann: Agentische AI verändert nicht nur Prozesse, sie verschiebt, wer im Unternehmen handelt und wer dafür verantwortlich ist. Wer heute führt, führt ein hybrides System aus Menschen und digitalen Agenten. Das erfordert vom Verwaltungsrat keine technische Expertise, aber ein klares Verständnis dafür, wie Entscheidungsrechte verteilt sind, wo Agenten autonom handeln dürfen und wo menschliches Eingreifen zwingend bleibt. Klassische Aufsicht, periodische Audits, nachträgliche Kontrolle, greift nicht mehr, wenn AI-Systeme täglich Tausende von Handlungen in Echtzeit ausführen. Der Verwaltungsrat muss sich fünf Fragen stellen können und präzise Antworten verlangen: Haben wir ein vollständiges Inventar aller Agenten und ihrer Verantwortlichen? Ist Autonomie nach Risikoklassen abgestuft? Können wir Entscheidungen lükkenlos rekonstruieren? Und haben wir einen echten Notfallplan, wenn etwas schiefgeht?

Die tiefere Frage ist strategischer Natur: Agentische AI ist kein IT-Thema, das man delegiert: sie ist eine Frage der Unternehmensidentität. Der Verwaltungsrat muss entscheiden, ob agentische AI primär der Kostensenkung dient oder als Quelle von Differenzierung und Erneuerung verstanden wird. Diese Entscheidung bestimmt Struktur, Governance und Talentstrategien. Am Ende trägt der Verwaltungsrat die Verantwortung, nicht für jeden einzelnen Agenten, aber dafür, dass das System als Ganzes kontrollierbar, rechenschaftspflichtig und strategisch ausgerichtet bleibt.

Rene Schmidli: Damit schliesst sich der Kreis. Am Ende ist der Mensch, sprich das oberste Organ einer Unternehmung in der Verantwortung. Aufgrund der Komplexität kann das zu einer zurückhaltenden Sichtweise zur Materie führen, welcher einer Firma am Ende aber nicht dienlich ist. Bezogen auf Risiko-, Governance- und Haftungsfragen: wie lassen sich Risiken managen und Verantwortlichkeiten klar und sinnvoll regeln, um das Nutzenpotenzial von Agentic AI dennoch zu erschliessen?

Oliver Gassmann: Zuallererst muss man die Risiken verstehen und einordnen lernen, dann mit dem Risikoappetit und der Strategie abgeglichen werden, um sie entsprechend zu mitigieren. Für Verwaltungsräte liegt die zentrale Herausforderung bei Agentic AI in der wachsenden Haftungslücke: Agenten handeln autonom, doch „The AI did it" ist keine Verteidigung. Die Organisation und damit das Board bleiben uneingeschränkt haftbar, sei es durch Caremark-Klagen in den USA oder die Directors' Duties, welche zum Beispiel in der Schweiz, Deutschland und Australien greifen. Unsauber aufgesetzte Systeme gelingen schnell die Umgehung klassischer Kontrollen: Agenten schließen eigenständig Verträge ab, binden Ressourcen oder geben Daten weiter, ohne dass herkömmliche Sicherheits- und Compliance-Regeln greifen. Operationale und systemische Risiken verstärken das Bild, von gleichzeitigen Aktionen über mehrere Funktionen über Multi-Agenten-Konflikte, Goal Misalignment und Behavioral Drift bis hin zu Tool Misuse. Reputations- und Finanzrisiken entstehen durch direkte Kunden- und Partnerinteraktionen ohne menschliche Kontrolle sowie unvorhersehbare Kaskadeneffekte in Lieferketten. Vendor- und Supply-Chain-Risiken verschärfen die Lage zusätzlich: Black-Box-Verhalten bei Drittanbietern, begrenzte Sichtbarkeit und neue Angriffsvektoren wie Prompt Injection, Data Poisoning oder Model Inversion. Regulatorisch droht ab August 2026 die volle Wucht des EU AI Act mit seinen High-Risk-Pflichten sowie zunehmendes Enforcement durch FTC und SEC.

Wer diese Risiken nicht frühzeitig einordnet, riskiert nicht nur finanzielle Schäden, sondern auch den Verlust von Handlungsfähigkeit und Vertrauen, gegenüber der Öffentlichkeit, Kunden und den eigenen Mitarbeiter. Die gute Nachricht: Ein klares Verständnis ist die unverzichtbare Grundlage für jede wirksame Massnahmen.

Doch, wie können solche Massnahmen das gewünschte Risikoprofil handhabbar werden lassen?

Für Verwaltungsräte liegt die Antwort in einer klaren, mehrschichtigen Governance-Architektur, die Autonomie fall- resp. use-case-spezifisch ausgestaltet und gleichzeitig Transparenz schafft. Human Oversight-Modelle bilden die erste Verteidigungslinie: Bei High-Risk-Aktionen bleibt der Mensch im Loop oder zumindest on-the-Loop, ergänzt durch definierte Eskalationsmatrizen, die klare Zuständigkeiten schaffen. Technische Guardrails sorgen für kontrollierte Handlungsfähigkeit: Durch Least-Privilege-Zugriffe, eindeutige Agenten-

Identitäten, eng gefasste Berechtigungen, Sandbox-Tests und die Möglichkeit einer sofortigen Systemunterbrechung.

Vollständige Audit Trails, Agent Cards, Echtzeit-Observability und eingebettete Compliance-Prüfungen stellen sicher, dass jede Entscheidung nachvollziehbar und regelkonform bleibt. Gleichzeitig stärkt ein professionelles Vendor-Management die Lieferkette: Robuste Due Diligence, Model Cards, Audit-Rechte, Indemnities und klare Daten-Nutzungsverbote schützen vor Black-Box-Risiken Dritter. Die kontinuierliche Überwachung rundet das System ab, und zwar mit adaptiven Risiko-Assessments und regelmässiger Neuklassifizierung der Agenten je nach Autonomiegrad.

Zusammen verwandeln diese Massnahmen Agentic AI von einem unkontrollierbaren Risiko in ein steuerbares Instrument. Sie reduzieren Haftungslücken, minimieren systemische Drift-Effekte und erfüllen die kommenden regulatorischen Anforderungen des EU AI Act. Für den Verwaltungsrat bedeutet das: Governance wird zur echten Wertschöpfung. Sie sichert nicht nur das Unternehmen, sondern schafft Vertrauen und strategischen Handlungsspielraum.

Schliesslich noch ein paar Bemerkungen, wie solche Governance-Ansätze aus Verwaltungsratssicht aussehen können. Aus Sicht des Verwaltungsrats geht es nicht mehr um punktuelle Kontrollen, sondern um eine dynamische und adaptive Aufsicht: Weg von jährlichen Audits hin zu kontinuierlichem Echtzeit-Monitoring und geschlossenen Feedback-Loops, die jede Agenten-Entscheidung unmittelbar nachvollziehbar machen. Das alles natürlich in einer kumulierten, stufengerechten Art und Weise, welche in verabschiedete Reglemente und entsprechenden Weisungen festgehalten wird. Verantwortlichkeiten müssen klar geregelt sein. In der ausgeprägtesten Form bei grösseren Unternehmen mit einem dedizierten AI Governance Committee, AI Risk Officers und konkreten Agent Owners, wobei das Board selbst die oberste Instanz bleibt. Die Governance sollte proportional und risikobasiert ausgestaltet werden: klare „Bright Lines“ als nicht verhandelbare Verbote, ergänzt durch eine abgestufte Autonomie je nach Risikoklasse.

Ein durchgängiger Lifecycle-Ansatz ist unverzichtbar, der die gesamte Wertschöpfungskette der Agenten von Design über Deployment und Monitoring bis zum Retirement umfasst. Gleichzeitig muss diese neue Governance nahtlos in bestehende Strukturen integriert werden, wie in Risk-, Cyber-, Procurement- und Compliance-Frameworks und als festes Agenda-Item in jeder Verwaltungsratssitzung stehen. Entscheidend bleibt schliesslich die eigene Board-Kompetenz: durch gezielte Zusammensetzung, kontinuierliche Weiterbildung und externe Beratung sowie eine explizit definierte Risk Appetite, die den strategischen Spielraum der Agenten klar vorgibt.

So wird Governance nicht zur Bremse, sondern zum eigentlichen Enabler: Sie schützt das Unternehmen, erfüllt die Sorgfaltspflicht des Verwaltungsrats und verwandelt Agentic AI in einen kontrollierten, wertschöpfenden Wettbewerbsvorteil. Wir dürfen nicht vergessen, das grösste Risiko besteht, dass wir den Sprung in ein neues Zeitalter verpassen und das Unternehmen seine Wettbewerbsfähigkeit verliert. Der Verwaltungsrat muss sicherstellen, dass Innovation auf der Agenda des Managements bleibt.