
# Aufbau einer widerstandsfähigen KI

## Bewältigung von KI Risiken durch Governance, Sicherheit und Resilienz

In Partnerschaft erstellt mit S-RM

# Inhalt

# Vorwort

**Vertrauen ist der rote Faden, der sich durch jedes erfolgreiche Unternehmen zieht. Es bildet die Grundlage von Beziehungen, ermöglicht Innovation und gibt Organisationen die Sicherheit, Veränderungen anzunehmen. Heute wird dieses Vertrauen zunehmend in Künstliche Intelligenz (KI) gesetzt. Die dafür erforderliche Governance hat jedoch Mühe, Schritt zu halten.**

KI ist weit über vereinzelte Pilotprojekte oder reine Produktivitätswerkzeuge hinausgewachsen. Sie wird rasch zu einem festen Bestandteil der Systeme und Prozesse, auf die sich Organisationen täglich stützen, um Entscheidungen zu treffen, Kunden zu bedienen, die Produktivität zu steigern und Innovation voranzutreiben. Die Geschwindigkeit der Entwicklungen hat erhebliche Chancen geschaffen, aber auch eine völlig neue Risikokategorie für Unternehmen mit sich gebracht.

Da KI zunehmend in kritische Geschäftsfunktionen eingeflochten wird, geraten Daten Governance, der Schutz der Integrität von KI Modellen, das Management von Drittparteirisiken und die Einhaltung von Regulierung zunehmend unter Druck.

Diese Entwicklung ist überall spürbar, und KI wird inzwischen als eine der bedeutendsten geschäftlichen Herausforderungen weltweit angesehen. Während Organisationen ihre Investitionen in die Fähigkeiten der KI weiter ausbauen, ist klar, dass die heute getroffenen Entscheidungen die Resilienz, das Kundenvertrauen und die Wettbewerbsposition auf Jahre hinaus prägen werden.

Für Vorstände und Geschäftsleitungen muss KI Sicherheit mehr sein als ein reines Technologie Thema. Sie erfordert starke Führung, eindeutige Verantwortlichkeiten, robuste Governance und einen konsequenten Fokus auf die Widerstandsfähigkeit des Unternehmens.
Den größten Nutzen aus ihren KI Investitionen werden diejenigen Unternehmen ziehen, die ihre Einsatzbereiche genau kennen, eine umfassende Kontrolle über den gesamten Lebenszyklus der KI sicherstellen und von Anfang an die notwendigen Sicherheitsvorkehrungen treffen.

Dieser Bericht beschreibt die sich wandelnde Landschaft der KI Risiken und zeigt praktische Schritte auf, mit denen sich KI schon heute mit Zuversicht einsetzen lässt. Aufbauend auf Erkenntnissen von AXA XL, S RM und führender Branchenforschung wird erläutert, wie Unternehmen KI zuverlässig und verantwortungsvoll skalieren können.

**Jonathan Salter**
Head of Risk Consulting

**Rebiah Bardot-Girard**
Head of Cyber Risk

# Zusammenfassung

Die Sicherheitslandschaft rund um KI tritt in eine neue Phase ein. Die Diskussion löst sich von einzelnen Modellen und rückt die Systeme, die Governance und die Abhängigkeiten in den Mittelpunkt, die bestimmen, wie KI heute im Unternehmen eingesetzt wird. Gleichzeitig beeinflussen schnelle Fortschritte in agentischer KI, sich wandelnde Regulierung und immer ausgefeiltere Cyberbedrohungen die Art und Weise, wie Organisationen über Risiken nachdenken.

**Fünf Entwicklungen prägen derzeit die Prioritäten für Unternehmen:**

## Zentrale Erkenntnis

KI schafft neue Chancen und gleichzeitig neue Formen von Risiken. Organisationen, die KI Governance als strategische Geschäftspriorität und nicht als reines Compliance Thema betrachten, sind am besten aufgestellt, um KI sicher zu skalieren, sich an die sich an neue regulatorische Anforderungen anzupassen und ihren langfristigen Wert zu auszuschöpfen.

## Neue Kategorien von Cyberrisiken entstehen

Für Cyberteams ist KI ein zweischneidiges Schwert. Einerseits trägt sie zur Stärkung von Abwehrmaßnahmen bei, andererseits verschafft sie Angreifern neue Möglichkeiten. Unternehmen sehen sich zudem mit Risiken konfrontiert, die spezifisch für KI sind: Datenlecks, vergiftete oder manipulierte Modelle, promptbasierte Angriffe, Modell Outputs, denen nachgelagerte Systeme ohne eigene Validierung vertrauen, Retrieval Systeme, die Informationen über die regulären Zugriffsrechte eines Nutzers hinaus offenlegen, und die Sicherheit autonomer Agenten, die mit eigenen Zugangsdaten handeln. Diese Risiken sind nicht länger theoretisch. Synthetische Sprach  und Videoaufnahmen werden bereits genutzt, um betrügerische Zahlungen zu autorisieren, und Organisationen wurden für Aussagen haftbar gemacht, die ihre eigenen KI gestützten Kundensysteme getätigt haben.

## Die Regulierung von KI beschleunigt sich weltweit

Regierungen und Aufsichtsbehörden arbeiten mit Hochdruck daran, konkrete Erwartungen für die verantwortungsvolle Entwicklung und Nutzung von KI zu definieren. Obwohl die Ansätze regional unterschiedlich sind, gibt es eine Gemeinsamkeit: Unternehmen müssen nachweisen, dass KI verantwortungsvoll eingesetzt wird.

## Governance entwickelt sich zu einem Wettbewerbsvorteil

Da KI heute in eine Vielzahl von Geschäftsabläufen eingebettet ist, wandelt sich Governance von einer reinen Compliance Disziplin zu einer strategischen Unternehmenskompetenz. Organisationen mit klaren Verantwortlichkeiten und starker Aufsicht sind weitaus besser in der Lage, Technologien erfolgreich zu skalieren und mit neuen Risiken Schritt zu halten – und dadurch stärkere Vertrauensbeziehungen zu ihren Zielgruppen aufzubauen.
Die Aufsicht muss auch jene KI Anwendungen einschließen, von deren Einsatz die Unternehmen nichts wissen. Die Nutzung öffentlicher KI Tools durch Mitarbeitende sowie aktivierte KI Features in bestehender Software stellen heute die am weitesten verbreitete Quelle von Exposition dar.

## KI muss über ihren gesamten Lebenszyklus gesteuert werden

Das Management von KI Risiken erfordert mehr als die Absicherung einzelner Modelle. Es braucht Sichtbarkeit über den gesamten Lebenszyklus — von der Datenerhebung und Modellentwicklung bis zur Einführung und Überwachung. Dazu gehören auch Drittanbieter, denen bewusst sein muss, dass KI Ökosysteme miteinander vernetzt sind und Verantwortung nicht ausgelagert werden kann. Lebenszyklus Management bedeutet auch, dass man in der Lage sein muss, Ereignisse zu rekonstruieren. Ohne gespeicherte Protokolle von Prompts, Antworten und Tool Aufrufen können Vorfälle mit KI Systemen nicht mit derselben Sicherheit untersucht werden wie klassische IT Vorfälle.

## Klarheit hinsichtlich Minderung und Versicherung von KI Risiken ist erforderlich

Unternehmen, die KI einführen, benötigen Unterstützung, um die Verwundbarkeiten zu verstehen, die sie unbeabsichtigt schaffen könnten. Risikomanagement und Versicherungen spielen eine wichtige Rolle dabei, Unternehmen Klarheit über ihre Risiken zu verschaffen, Resilienz aufzubauen, bevor Vorfälle eintreten, und bei einer effektiven Wiederherstellung zu unterstützen, wenn Störungen nicht vermieden werden können. Zudem ist Klarheit darüber erforderlich, wie KI bedingte Schäden mit bestehenden Versicherungssparten interagieren. Eine betrügerische Zahlung, die über einen gefälschten Videoanruf autorisiert wurde, ein fehlerhafter KI generierter Output, der einem Dritten einen Schaden verursachte sowie ein durch einen KI Agenten ermöglichter Einbruch betreffen jeweils unterschiedliche Policen.

# KI hat Einzug in die Unternehmen gehalten

Branchenübergreifend integrieren Organisationen KI in zentrale Geschäftsprozesse und nutzen sie, um Kundeninteraktionen zu unterstützen, Abläufe zu verschlanken, Daten zu analysieren und fundierte Entscheidungen zu treffen.

**Die jüngste „State of AI"-Umfrage von McKinsey ergab, dass 88 % der Organisationen KI inzwischen regelmäßig in mindestens einer Geschäftsfunktion einsetzen – ein Anstieg gegenüber 78 % im Vorjahr. Dies zeigt, wie schnell KI Teil der Technologien geworden ist, auf die sich Organisationen täglich verlassen.[1]**

KI wird zudem autonomer: Unternehmen gehen über reine Content Generatoren hinaus und setzen Systeme ein, die Informationen abrufen, mit anderen Anwendungen interagieren und mit begrenztem menschlichem Input handeln. Das kann erhebliche Effizienzgewinne bringen, erhöht aber auch das potenzielle Schadensausmaß von Sicherheitsfehlern und betrieblichen Fehlentscheidungen.

[1] McKinsey & Company, The State of AI, 2026

Da KI nun integraler Bestandteil vieler Geschäftsabläufe ist, können Fehler sich rasch über Systeme ausbreiten und länger unentdeckt bleiben, bevor sie Konsequenzen verursachen. Der Erfolg in der nächsten Phase der KI Einführung wird davon abhängen, wie gut Organisationen das breitere Ökosystem rund um ihre Modelle managen. Zu verstehen, wo KI genutzt wird, wie sie mit Prozessen interagiert und wer für ihre Ergebnisse verantwortlich ist, wird zunehmend entscheidend für den Aufbau von Resilienz im Zusammenhang mit ihrer Nutzung.

Während Unternehmen immer stärker von KI getriebenen Ökosystemen abhängig werden, die neue Abhängigkeiten zwischen Menschen, Technologien und Drittanbietern schaffen, signalisiert diese Entwicklung einen grundlegenden Wandel — sowohl beim Ausmaß der Chancen als auch beim Ausmaß möglicher Schäden.

**88%**

der Organisationen setzen KI regelmäßig in mindestens einer Geschäftsfunktion ein — McKinsey 2026

## Zentrale Erkenntnis

KI wird zum festen Bestandteil der Betriebsabläufe moderner Unternehmen und ist in zunehmend vernetzte Technologie Ökosysteme eingebunden. Unternehmen sehen sich rasch mit einer Komplexität konfrontiert, für die nur wenige Governance Modelle ursprünglich ausgelegt waren. Sicherheit muss sich daher über den Schutz einzelner Modelle hinaus erstrecken und Daten, Systeme, Lieferanten und Geschäftsprozesse einbeziehen, die einen sicheren KI Betrieb in großem Maßstab ermöglichen.

# Die Risikolandschaft im Bereich KI

Unternehmen sind heute einer verstärkten Form früherer Cyberrisiken ausgesetzt. Diese Risiken sind keine isolierten technischen Probleme, sondern beeinflussen Governance, Sicherheit und Resilienz gleichermaßen. Gleichzeitig werden bestehende Herausforderungen rund um Identität, Daten, Lieferketten und operative Widerstandsfähigkeit laufend komplexer.

Die Risiken sind nicht neu. Datendiebstahl, böswillige Insider und Software Schwachstellen sind seit Langem bekannte Probleme. Was KI verändert, ist die Größenordnung und Komplexität. Heutige Systeme verarbeiten mehr Informationen, interagieren mit mehr Anwendungen und treffen oder beeinflussen mehr Entscheidungen als je zuvor — und das mit größerer Autonomie.

Unternehmen beginnen zu erkennen, dass sie dieses neue Umfeld aktiv gestalten müssen. Der aktuelle „Global Cybersecurity Outlook“ des Weltwirtschafts-forums zeigt, dass *64 % der Organisationen inzwischen Prozesse etabliert haben, um die Sicherheit von KI Tools vor dem Einsatz zu bewerten*[2] — ein deutlicher Anstieg gegenüber 37 % im Vorjahr. Für die Unternehmensführung ist die Konsequenz klar: KI Sicherheit muss von Anfang an berücksichtigt werden, und zwar aus einer globalen Governance Perspektive, nicht nur als lokal begrenztes technisches Thema.

Der erste Schritt ist zu verstehen, wie sich die KI Risiko-landschaft verändert, wo neue verwundbare Stellen entstehen und was sie für das Unternehmen bedeuten.

**64%**

der Organisationen haben inzwischen Prozesse etabliert, um die Sicherheit von KI Tools vor dem Einsatz zu bewerten

**„Aus unserer Arbeit mit Organisationen, die auf Cybervorfälle reagieren und ihre Resilienz stärken, wird eine Erkenntnis zunehmend klarer:**

**KI Risiken entstehen nicht isoliert. Sie werden auf bestehende Schwächen in der Identitätsverwaltung, Daten Governance, Lieferantenaufsicht und Incident-Bereitschaft aufgesetzt. Für viele Organisationen erhöht KI die Gefährdung schneller, als sich die Betriebsmodelle anpassen können.“**

**Joani Green,**
Global Technical Director,
Cyber Security at S-RM

[2] World Economic Forum, Global Cybersecurity Outlook, 2026

# Bekämpfung von Datenlecks und unbefugter Zugriff

KI Systeme benötigen Zugang zu großen Datenmengen, um genaue Ergebnisse zu liefern. Häufig greifen sie dabei auf kommerziell sensible Informationen und geistiges Eigentum zu. Je tiefer KI im Alltag verankert wird, desto wertvoller werden diese Daten, und in vielen Fällen sind sie breiter zugänglich als jemals zuvor.

Ohne starke Governance können sensible Informationen leicht in Prompts, Outputs oder Drittanwendungen gelangen und Risiken erzeugen, die weit über reine Cybersicherheit hinausgehen. Da KI mehr Systemen und Anwendungen Zugang zu sensiblen Daten verschafft, wird die Kontrolle darüber, wer oder was diese Informationen nutzen darf, immer wichtiger. Angreifer zielen zudem auf Identitäten und Zugriffsrechte, die ihnen den Weg zu diesen Daten ebnen.

**Der IBM X Force Threat Intelligence Index 2025 ergab, dass über 30 % der untersuchten Vorfälle den Diebstahl oder Missbrauch von Zugangsdaten betrafen, was einen Wandel weg von klassischer Softwareausnutzung hin zu identitätsbasierten Angriffen widerspiegelt.[3]**

[3] IBM, X-Force Threat Intelligence Index, 2025

Unternehmen benötigen mehr denn je ein klares Verständnis darüber, wo Daten genutzt werden, wie sie zwischen Systemen fließen und wer Zugriff hat. Diese Transparenz ist essenziell für ein wirksames Risikomanagement, insbesondere bei sensiblen oder personenbezogenen Daten. Aus Sicht der Versicherungsbranche sind Organisationen mit nachweislich starker Daten Governance, robusten Zugriffskontrollen und klarer KI Aufsicht weitaus besser aufgestellt, um Risiken zu minimieren.

Für Unternehmensleitungen ist der Schutz von Daten längst mehr als ein Thema der Informationssicherheit. Er ist entscheidend für die Aufrechterhaltung des Kundenvertrauens und dafür, dass KI gestützte Entscheidungen verlässlich bleiben.

## Zentrale Erkenntnis

Wirksame KI Governance beginnt mit einem Verständnis der Daten, auf die KI Systeme zugreifen können, wo sie liegen und wie sie geschützt sind — unabhängig davon, wo sie verwendet werden.

# Data Poisoning

In der Architektur von KI gehören Daten zu den zentralen Bestandteilen eines Modells. Data Poisoning („Datenvergiftung“) tritt während der Trainingsphase auf, wenn böswillige Akteure absichtlich manipulierte Datenfragmente in Trainingssets einschleusen, um Ausgabeergebnisse zu steuern und das Verhalten des Modells zu beeinflussen. Ziel ist es, die Gesamtleistung zu verschlechtern oder versteckte Funktionen (Hintertüren) zu aktivieren, die unter bestimmten Bedingungen zum Tragen kommen.

Wenn KI Outputs von Beginn an manipuliert werden, ist dies nach der Implementierung oft schwer zu erkennen und nur mit erheblichem Aufwand zu beheben, da das Modell vollständig mit sauberen Daten neu trainiert werden muss. Die Auswirkungen betreffen nicht nur die Performance: Sie untergraben Vertrauen, schwächen Sicherheit und Governance und können regulatorische oder geschäftliche Risiken mit sich bringen.

Bereits in den frühen Entwicklungsphasen eines Projekts müssen Unternehmen sicherstellen, dass eine strenge Rückverfolgung der Herkunft der KI-Daten erfolgt, dass robuste Trainingsverfahren definiert und umgesetzt werden und dass der gesamte Trainingsprozess kontinuierlich überwacht wird, um Anzeichen einer Manipulation frühzeitig zu erkennen, einschließlich menschlicher Überwachungsschritte.

## Zentrale Erkenntnis

Gute Daten Governance muss bereits in den frühen Entwicklungsphasen eines KI Projekts verankert werden und sich bedarfsgerecht über den gesamten Projektlebenszyklus weiterentwickeln.

# Prompt Injection und böswillige Angriffe

Die Möglichkeit, über Prompts die Anweisungen zu manipulieren, die KI Systeme erhalten, oder das Modell gezielt mit manipulierten, böswilligen Eingabedaten (Bilder, Texte, Audio) zu falschen Vorhersagen zu verleiten, ist ein weiterer Bereich, den Unternehmen im Auge behalten müssen. Die Beeinflussung des Verhaltens oder die Umgehung vorgesehener Schutzmechanismen zur Erzeugung unbeabsichtigter oder schädlicher Ergebnisse zu erzeugen, kann erheblichen Schaden anrichten.

Werden KI generierte Ergebnisse manipuliert, können die Folgen von der Offenlegung vertraulicher Informationen über die Beeinflussung geschäftlicher Entscheidungen bis hin zur Störung kundenorientierter Dienste reichen. Dies gilt insbesondere dann, wenn KI eng in die täglichen Abläufe eingebunden ist.

Unternehmen müssen daher sicherstellen, dass sich Datensicherheit, Systemtests, Monitoring und Kontrolle durch Menschen parallel zur Nutzung KI basierter Technologien weiterentwickeln.
Das bedeutet, KI Systeme mit derselben Sorgfalt zu behandeln wie jedes andere kritische Unternehmenssystem.

Da KI eine aktivere Rolle in der Kundeninteraktion spielt, können Unternehmen es sich nicht mehr leisten, Prompt Injection als isolierte technische Schwachstelle zu betrachten. Sie wird zu einem Unternehmensrisiko, das eine kontinuierliche Aufsicht erfordert.

## Zentrale Erkenntnis

KI Outputs sollten überprüft, überwacht und durch angemessene Governance abgesichert werden, anstatt davon auszugehen, dass sie standardmäßig korrekt oder sicher sind.

## Manipulation und Diebstahl von KI-Modellen

Für viele Unternehmen werden KI Modelle selbst zu wertvollen Unternehmenswerten. Sie spiegeln erhebliche Investitionen wider und enthalten wertvolles proprietäres Wissen. Mit ihrer wachsenden Bedeutung steigt auch ihre Attraktivität für Cyberkriminelle.

Der Schutz von KI Modellen muss ebenso strategisch wichtig eingestuft werden wie der Schutz von Kundendaten oder kritischer Infrastruktur. Werden KI Modelle manipuliert, kann die Integrität KI gestützter Prozessabläufe gefährdet sein. Kommt es zum Diebstahl, können Angreifer Zugang zu wertvollem geistigem Eigentum erhalten oder Fähigkeiten replizieren, die jahrelange Entwicklung erfordert haben. Dies kann das Vertrauen in KI gestützte Dienste schwer beschädigen und Innovation nachhaltig hemmen.

Schutz bedeutet hier, über rein technische Kontrollen hinauszugehen. Organisationen sollten wissen, wo Modelle eingesetzt werden, wer Zugriff hat, wie Änderungen verwaltet werden und welche Mechanismen existieren, um unbefugte Aktivitäten zu erkennen.

### Zentrale Erkenntnis

KI Modelle sollten als kritische Unternehmenswerte geschützt und gesteuert werden.

## Halluzinationen und unzuverlässige Ergebnisse

Generative KI ist zu außergewöhnlichen Leistungen fähig, kann aber auch mit großer Überzeugung falsch liegen. Halluzinationen entstehen durch Lücken im Trainingsdatensatz, unklare Prompts oder inhärente Modellgrenzen.

Jüngste Untersuchungen des Stanford University AI Index 2026 zeigen, dass bei 26 führenden KI Modellen die Halluzinationsraten zwischen 22 % und 94 % liegen.[4]

Eine einzelne falsche Antwort mag für sich genommen keine große Rolle spielen. Doch wenn KI dazu beiträgt, geschäftliche Entscheidungen zu treffen, Kunden zu unterstützen oder operative Prozesse zu steuern, steigt das Risiko deutlich. Fehler können sich schnell verbreiten und behördliche Untersuchungen, finanzielle Verluste und nachhaltigen Vertrauensverlust nach sich ziehen.

Unternehmen sollten KI Ergebnisse nicht als von Natur aus verlässlich einstufen. Sie brauchen regelmäßige — nicht einmalige — Validierungsprozesse und klare Regeln, wann menschliche Kontrolle erforderlich ist und wie sich dies mit der Zeit verändert.

Unternehmen brauchen Vertrauen nicht nur in das, was KI produzieren kann, sondern auch darin, wann ihre Ergebnisse als belastbar gelten und wann menschliches Urteilsvermögen Vorrang haben sollte.

### Zentrale Erkenntnis

Vertrauen in KI setzt voraus, dass Outputs geprüft werden — nicht, dass ihre Genauigkeit unterstellt wird.

[4] Stanford University, AI Index Report, 2026

## Abhängigkeit von nicht verifizierten Modellen oder Modellen von Drittanbietern

Die Nutzung von Subunternehmern oder externen Anbietern für KI Modelle bringt Herausforderungen für Lieferkette und Governance mit sich. Begrenzte Transparenz darüber, wie ein Modell trainiert wurde, welche Daten verwendet wurden und wie Updates gemanagt werden, erhöht das Risiko unerwünschten Verhaltens und von Richtlinienverstößen. Wie bei jedem anderen IT Dienstleister kann die Abhängigkeit von einem KI Anbieter bei Ausfällen, Strategiewechseln oder Preisänderungen zu Engpässen führen und die Einhaltung interner Standards einschränken.

Darüber hinaus können nicht verifizierte oder schlecht geprüfte Modelle Organisationen gegenüber potenziellen Hintertüren oder unsicheren Verhaltensweisen des Modells aussetzen. Eine weitere große Herausforderung sind Abweichungen von Richtlinien, Vorschriften oder ethischen Grundsätzen, insbesondere wenn Modelle nach der Bereitstellung Drifterscheinungen aufweisen oder ohne gründliche Tests aktualisiert werden. Unklarheiten bei der Lizenzierung und mangelnde Transparenz über Trainingsdaten können zudem die Einhaltung von Vorschriften und die Nachprüfbarkeit erschweren.

Anstatt davon auszugehen, dass externe Modelle von Natur aus sicher sind, müssen robuste Governance und Due Diligence Prozesse für alle Modelle und Daten etabliert werden. Klare Herkunftsnachweise und nachvollziehbare Aktivitäten sollten verlangt, Sicherheits und Funktionsprüfungen vor der Bereitstellung durchgesetzt und starke vertragliche Schutzmechanismen (SLAs, Transparenzklauseln, Offenlegungspflichten für Updates) vereinbart werden.

### Zentrale Erkenntnis

KI Anbieter sollten wie kritische externe Partner behandelt werden; sowohl der Anbieter als auch das KI Modell müssen einem Due Diligence Prozess unterzogen werden.

## Bekämpfung von „Shadow AI“

Shadow AI bezeichnet Situationen, in denen Mitarbeitende oder Geschäftsbereiche KI Tools oder Dienste nutzen, die keiner formalen Sicherheits , Datenschutz und Governanceprüfung unterzogen wurden. Diese Tools können sensible Daten verarbeiten oder mit Unternehmenssystemen interagieren — häufig unter Umgehung von Beschaffungsprozessen und Risikoanalysen.

Zu den Risiken zählen Datenlecks oder Datenabflüsse sowie die Einführung unsicherer Konfigurationen oder versteckter Hintertüren, die die Angriffsfläche des Unternehmens vergrößern. Auf operativer Ebene kann Shadow AI unkontrollierte Datenfströme, Lizenz und Kostenprobleme, inkonsistente Ergebnisse und Herausforderungen bei der Revision verursachen. Strategisch untergräbt sie das Risikomanagement, verstärkt die Abhängigkeit von Anbietern und erschwert die Reaktion auf Vorfälle.

Um dem entgegenzuwirken, sollten Unternehmen nicht autorisierte Tools standardmäßig blockieren und eine klare Richtlinie sowie einen Genehmigungsprozess für KI Tools festlegen. Zusätzlich sollten sie die Prinzipien der Datenklassifizierung und des Zugriffs mit geringst-möglichen Berechtigungen („Least Privilege“) anwenden. Regelmäßige Schulungen der Mitarbeiten-den und wiederkehrende Cybersecurity Kontrollen der Angriffsfläche sind ebenfalls entscheidend, um solche Situationen zu vermeiden.

### Zentrale Erkenntnis

Mehr denn je ist die Eindämmung von Shadow AI entscheidend.

**„Die schwierigsten Risiken sind oft nicht die offensichtlichsten. Unternehmen verfügen zwar möglicherweise über eine formale Governance für strategische KI Programme haben, während unkontrollierte Nutzung von KI über öffentliche Tools, integrierte Software Features oder Dienste von Drittanbietern weiterläuft.**
**Das schafft eine Lücke zwischen wahrgenommenem und tatsächlichem Kontrollgrad.**
**Um diese Lücke zu schließen, muss zunächst eine praktische Bestandsaufnahme darüber erfolgen, wo KI eingesetzt wird, auf welche Daten sie zugreifen kann und wo sie Maßnahmen ergreifen oder Entscheidungen beeinflussen kann.“**

**Joani Green,**
Global Technical Director,
Cyber Security at S-RM

# Autonome KI Agenten

Anstatt nur Inhalte zu generieren oder Prompts zu beantworten, sind agentische KI Systeme heute in der Lage, Aufgaben zu planen und mit Anwendungen zu interagieren, wobei sie Handlungen mit minimaler menschlicher Intervention ausführen. Das Potenzial ist enorm und ermöglicht Unternehmen die Automatisierung komplexer Arbeitsabläufe.

Mit diesem steigenden Autonomiegrad gehen jedoch eine Reihe neuer Herausforderungen im Bereich der Governance einher.

KI Systeme benötigen klar definierte Berechtigungen und angemessene Schutzmechanismen, um sicherzustellen, dass sie innerhalb der richtigen Grenzen agieren. Ohne wirksame Aufsicht riskieren Unternehmen, dass auf falsche Daten zugegriffen wird oder dass Interaktionen mit verbundenen Systemen unbeabsichtigt neue Schwachstellen schaffen.

**Eine Umfrage von McKinsey ergab, dass 23 % der Organisationen agentische KI bereits in mindestens einem Geschäftsbereich in großem Maßstab einsetzen, während weitere 39 % mit KI Agenten experimentieren.[5]**

Die Geschwindigkeit, mit der diese Systeme hier Einzug halten, verdeutlicht, wie schnell diese Systeme zum Bestandteil des Tagesgeschäfts werden. Unternehmen müssen die Vorteile von Automatisierung mit angemessenen Verantwortlichkeits und Kontrollniveaus in Einklang bringen. Je mehr Autonomie Organisationen an KI übertragen, desto wichtiger wird es, klar festzulegen, wer für deren Handlungen die Verantwortung trägt.

## Zentrale Erkenntnis

Je mehr Autonomie Unternehmen der KI einräumen, desto größer wird der Bedarf an wirksamer Governance, klar definierten Berechtigungen und einer angemessenen Aufsicht durch den Menschen.

Für sich betrachtet können Datenlecks und Datenvergiftung, Shadow AI, Prompt Injection, Modellmanipulation und Diebstahl, Halluzinationen und autonome Agenten als separate technische Herausforderungen erscheinen. Zusammengenommen weisen sie jedoch auf einen viel größeren Wandel in der Risikolandschaft von Unternehmen hin.

Es besteht ein Bedarf an einer Governance, die das gesamte KI Ökosystem abbildet, statt einzelne Risiken isoliert anzugehen.

Risiken zu verstehen ist nur ein Teil der Aufgabe. Angesichts der zunehmenden Verbreitung von KI müssen sich Unternehmen zudem in einem regulatorischen Umfeld zurechtfinden, das die Erwartungen neu definiert. Beim Risikomanagement ist heute ein stärker integrierter Ansatz als je zuvor erforderlich, der berücksichtigt, wie sich Technologie, Menschen, Prozesse und Drittanbieter gegenseitig beeinflussen.

[5] McKinsey & Company, The State of AI 2026

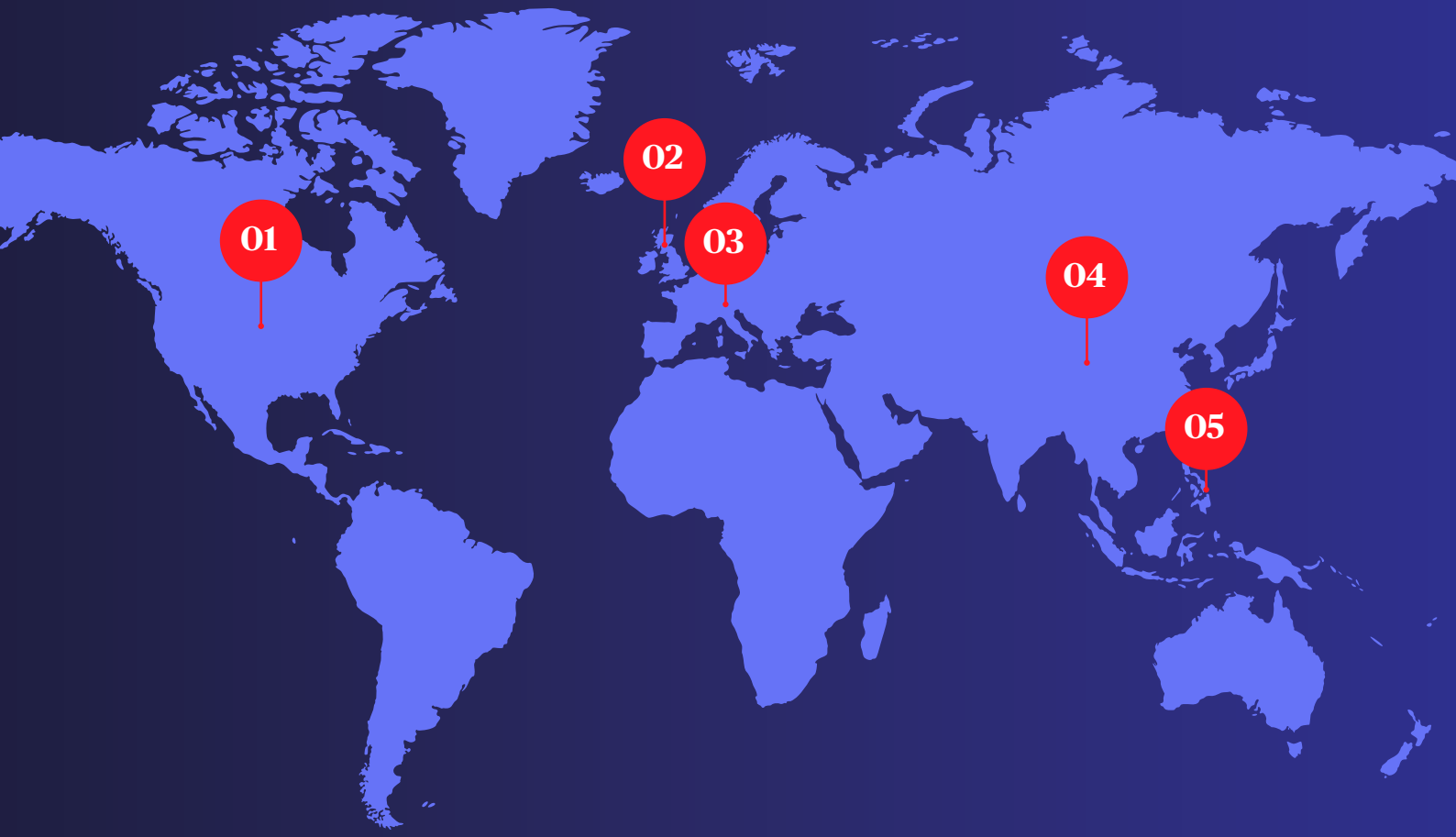
# Umgang mit aktuellen und künftigen regulatorischen Rahmenbedingungen

Das globale regulatorische Umfeld für KI entwickelt sich rasant, während politische Entscheidungsträger daran arbeiten, konkrete Leitplanken festzulegen, die bestimmen, wie KI praktisch gesteuert und überwacht wird. Die OECD[6] hat diesen Wandel hervorgehoben und darauf hingewiesen, dass Regierungen sich von breit angelegten KI Strategien hin zu klareren Regeln mit größerer Verantwortlichkeit bewegen, um eine sichere Einführung zu unterstützen.

Obwohl die Ansätze im Einzelnen variieren, wird die Richtung immer deutlicher. Unternehmen werden zunehmend dazu angehalten, zu verstehen, wo KI eingesetzt wird, passende Governance zu etablieren und Verantwortung über den gesamten Lebenszyklus hinweg nachzuweisen.

Anstatt auf jede neue Vorschrift isoliert zu reagieren, sollten sich Organisationen darauf konzentrieren, Governance Rahmenwerke zu schaffen, die flexibel genug sind, um sich an wandelnde Anforderungen anzupassen.

[6] OECD, Governing with Artificial Intelligence




# Globale regulatorische Entwicklungen

Unternehmen, die international tätig sind, müssen sich in einem Flickenteppich an KI Vorschriften zurechtfinden. Viele Regierungen verfolgen ähnliche Ziele, aber Tempo, Umfang und Fokus der Regulierung unterscheiden sich deutlich zwischen den Regionen:

**01** **USA** In den Vereinigten Staaten herrscht ein stärker fragmentiertes und unsicheres regulatorisches Umfeld, da sich die KI Politik sowohl auf Bundes als auch auf Staatsebene weiterentwickelt. Unterschiede zwischen diesen Ansätzen und offene Fragen zu ihrem Zusammenspiel bedeuten, dass Unternehmen sich auf ein Umfeld vorbereiten müssen, das sich weiterhin erheblich verändern könnte.

**02** **Vereinigtes Königreich** Das Vereinigte Königreich hat einen prinzipienbasierten Ansatz gewählt, der Innovation fördern und gleichzeitig existierende regulatorische Rahmenbedingungen auf KI anwenden soll. Der Schwerpunkt liegt auf verantwortungsvoller Governance, Transparenz und Verantwortlichkeit statt auf völlig neuen Regeln.

**03** **Europa** Europa gibt mit dem EU KI Gesetz („AI Act“) weiterhin das Tempo vor. Es stuft KI Systeme nach dem potenziellen Risiko für Individuen, einschließlich Sicherheit und Grundrechten ein. Anwendungen mit höherem Risiko unterliegen verstärkter Aufsicht, Transparenz und Verantwortlichkeitsanforderungen. Obwohl die Gesetzgebung innerhalb der EU gilt, reicht ihr Einfluss bereits über ihre Grenzen hinaus und veranlasst Unternehmen dazu, ihre KI-Governance in ihren internationalen Geschäftsaktivitäten zu stärken.

**04** **China** China hat einen eigenen regulatorischen Rahmen für KI entwickelt, mit Anforderungen, die Bereiche wie generative KI Dienste, Algorithmen, Daten und Inhalte betreffen. Der Ansatz entwickelt sich parallel zum rasch wachsenden KI Sektor des Landes weiter, weshalb Entwicklungen in China zunehmend relevant für Unternehmen werden, die international tätig sind oder auf chinesische KI Technologien und -Anbieter zurückgreifen.

**05** **Asien Pazifik** In der gesamten asiatisch-pazifischen Region reifen die regulatorischen Ansätze weiterhin in unterschiedlichem Tempo, wobei sich gemeinsame Themen rund um verantwortungsvolle KI, sicheres Datenmanagement und wirksame Aufsicht abzeichnen. International tätige Unternehmen benötigen einen Ansatz, der sich an unterschiedliche Anforderungen anpassen lässt, während sich das regulatorische Umfeld weiterentwickelt.

# Was die Regulierung von KI für Unternehmen bedeutet

Auch wenn sich die regulatorischen Ansätze unterscheiden, laufen sie auf ähnliche Erwartungen hinaus. Unternehmen müssen verstehen, wo sie KI einsetzen, Anwendungen mit hohem Risiko identifizieren, klare Verantwortlichkeiten festlegen und über den gesamten Lebenszyklus hinweg lückenlos dokumentieren.

Erklärbarkeit und Verantwortlichkeit werden mindestens ebenso wichtig wie technische Performance, insbesondere dort, wo KI Entscheidungen beeinflusst, die Kunden, Mitarbeitende oder kritische Geschäftsabläufe betreffen. Für Unternehmensleitungen unterrstreicht dies die Notwendigkeit, KI Governance als unternehmensweite Verantwortung zu betrachten.

# Compliance als Wettbewerbsvorteil

Unternehmen können Regulierung als Einschränkung der Innovation betrachten, doch in Wirklichkeit kann eine effektive Governance zum Wettbewerbsvorteil werden.

Die aktuelle Studie von Deloitte zum Stand der KI in Unternehmen[7]hat ergeben, dass nur eines von fünf Unternehmen ein reifes Governance Modell für autonome KI Agenten besitzt — ein klarer Vorteil für Organisationen, die frühzeitig robuste Governance etablieren.

**„KI verändert auch die Beweislage nach Vorfällen. Herkömmliche Protokolle reichen möglicherweise nicht aus, um zu verstehen, was passiert ist – insbesondere, wenn Prompts, Outputs, Modellverhalten, Abrufquellen oder Agentenaktionen eine Rolle spielen.**

**Unternehmen sollten sich überlegen, welche Informationen sie benötigen, um ein KI bezogenes Ereignis zu rekonstruieren, Verantwortlichkeit zu demonstrieren und juristische, regulatorische oder versicherungsbezogene Prozesse zu unterstützen.“**

**Joani Green,**
Global Technical Director,
Cyber Security at S-RM

[7] Deloitte, State of AI in the Enterprise

# Vom Risiko zur Resilienz

Da sich diese Technologie weiter verbreitet, benötigen Unternehmen praktische Ansätze, um Risiken im Zuge der Weiterentwicklung konsequent zu managen. Das bedeutet, über einzelne technische Kontrollen hinauszugehen und Governance Modelle zu etablieren, die verschiedene Unternehmensbereiche auf eine gemeinsame Linie bringen.

Kein einziges Rahmenwerk kann alle Herausforderungen rund um KI adressieren. Bewährte Standards wie das NIST AI Risk Management Framework, ISO/IEC 42001, die OWASP Top 10 für Anwendungen mit großen Sprachmodellen[8] und die Top 10 für agentische Anwendungen[9] bilden jedoch eine wertvolle Grundlage.

Anstatt konkrete technische Maßnahmen vorzuschreiben, bieten sie Unternehmen eine einheitliche Methode zur Risikobewertung, zur Zuweisung von Verantwortlichkeiten und zur Steuerung von KI. Zusammen unterstützen sie einen einheitlicheren Ansatz zur Identifikation von KI Anwendungen mit hohem Risiko, zum Management von Abhängigkeiten von Drittparteien, zur Überwachung der KI Performance und zur Reaktion auf Vorfälle, während sich Systeme weiterentwickeln.

Letztlich hängt Resilienz weniger von der Wahl eines bestimmten Rahmenwerks ab als von der Verankerung guter Governance in alltäglichen Entscheidungen. Die Aufrechterhaltung der Transparenz über alle KI Systeme hinweg und die kontinuierliche Leistungsüberprüfung versetzen Unternehmen in die Lage, neue Risiken zu managen und gleichzeitig weiterhin selbstbewusst Innovationen voranzutreiben.

## Der Blick nach vorn

Governance Rahmenwerke geben Orientierung, entfalten aber erst dann Wert, wenn sie in gelebte Praxis überführt werden. Die nächste Herausforderung für Unternehmen wird sein, diese Prinzipien in die Gestaltung, Entwicklung, Implementierung und das Management von KI Systemen zu übersetzen — also Sicherheit und Resilienz durch den gesamten KI Lebenszyklus hindurch mitzudenken, anstatt sie erst nach der Einführung zu ergänzen.

[8] OWASP, Top 10 for Large Language Model Applications

[9] OWASP, Top 10 for Agentic Applications for 2026

**„In der Praxis geht es nicht darum, alle KI Risiken vollständig zu eliminieren, sondern sie beherrschbar zu machen. Das bedeutet, klare Verantwortlichkeiten zu definieren, Grenzen für akzeptable Nutzung fest-zulegen, KI gestützte Workflows zu testen und Reaktionspläne für Szenarien vorzubereiten, in denen KI Systeme Daten offenlegen, fehlerhafte Empfehlungen ausgeben oder über ihre eigentlichen Befugnisse hinaus handeln."**

**Joani Green,**
Global Technical Director,
Cyber Security at S-RM

# Sichere KI „by Design“ aufbauen

Unternehmen, die Sicherheit von Anfang an in ihre KI integrieren, werden langfristig besser aufgestellt sein, um Einführung in großem Maßstab zu bewältigen und Resilienz zu stärken, während sich die regulatorischen Rahmenbedingungen weiterentwickeln. Technologie allein reicht dafür nicht aus.

Die folgenden fünf Prioritäten bieten eine praktische Grundlage, um Risiken frühzeitig zu erkennen und den vertrauensvollen Einsatz von KI zu ermöglichen:

## Bessere Daten Governance

Starke KI Governance beginnt mit einem Verständnis der Daten, auf denen KI Systeme basieren. Unternehmen sollten wissen, auf welche Informationen KI zugreifen kann, woher sie stammen und wie sie geschützt werden, um Sicherheits und Regulierungsrisiken zu verringern.

## Sicherheit von Modellen und Anwendungen

KI Modelle sollten als kritische Unternehmenswerte behandelt werden. Sicherheitstests, regelmäßiges Monitoring und effektives Change Management können helfen, Vertrauen in KI gestützte Dienste zu erhalten und das Risiko von Manipulation oder unautorisiertem Zugriff zu reduzieren.

## Stärkung der Identitäts und Zugriffskontrollen

Mit zunehmender Autonomie von Systemen gewinnt die Identitätsprüfung an Bedeutung. *Das deckt sich mit der OWASP Empfehlung in den Top 10 Listen für LLM Anwendungen[8] und agentische Anwendungen[9], die übermäßige Handlungsmacht („excessive agency“) und zu weitreichende Berechtigungen als wichtige aufkommende Sicherheitsrisiken identifizieren.* Unternehmen sollten sicherstellen, dass sowohl Nutzer als auch KI Systeme nur Zugang zu den Daten und Anwendungen haben, die sie für ihre vorgesehene Rolle benötigen — dies stärkt Governance und begrenzt die Auswirkungen kompromittierter Konten.

## Stärkung der Resilienz im gesamten KI Ökosystem

Die meisten Unternehmen verlassen sich auf ein Netzwerk aus Cloud Providern, Technologiepartnern und KI Anbietern. Diese gegenseitigen Abhänigkeiten zu verstehen hilft, das Netzwerk zu steuern und potenzielle Schwachstellen früh zu erkennen.

## Kontinuierliche Überwachung und Anpassung

KI ist nicht statisch: Modelle entwickeln sich laufend weiter, Vorschriften ändern sich und neue Bedrohungen entstehen. Regelmäßiges Monitoring, Governance Reviews und Tests helfen Unternehmen, Probleme früh zu erkennen, fortlaufende Einhaltung der Vorschriften nachzuweisen und sich an wandelnde Technologien und Risiken anzupassen.

„Security by Design“ zielt letztlich darauf ab, Organisationen mehr Sicherheit bei der Innovation und Skalierung von KI zu geben — sicher und verantwortungsvoll, mit Vertrauen als integraler Bestandteil des Prozesses. Dies hängt davon ab, dass Governance, Sicherheit und Resilienz während des gesamten Einführungsprozesses verankert werden, unterstützt von einer Unternehmenskultur und, wo erforderlich, durch vertrauenswürdige Partner, die dabei helfen können, sich in einer zunehmend komplexen Risikolandschaft zurechtzufinden.

[8] OWASP, Top 10 for Large Language Model Applications

[9] OWASP, Top 10 for Agentic Applications for 2026

# Der Ansatz von AXA XL

**Ein resilienter Ansatz beginnt mit Transparenz. Unternehmen müssen wissen, wo KI eingesetzt wird, auf welche Daten sie zugreifen kann, welche Entscheidungen sie beeinflusst und von welchen Drittparteien sie abhängig ist. Dazu gehören formale KI Initiativen ebenso wie weniger sichtbare Verwendungen in öffentlichen Tools, eingebetteten Software Features und autonomen Agenten.**

AXA XL ist überzeugt, dass KI Risikomanagement in praktischen Geschäftsszenarien verankert sein sollte. Unternehmen sollten sich vor Augen führen, was passiert, wenn ein Modell einen unzuverlässigen Output erzeugt, ein KI Agent über seine Befugnisse hinaus handelt, sensible Daten durch einen Prompt offengelegt werden oder ein kritischer KI Provider ausfällt.

Solche Szenarien helfen dabei, technische Schwachstellen in geschäftliche Konsequenzen wie finanzielle Verluste, Betriebsstörungen, Haftungsrisiken, behördliche Überprüfungen und Reputationsschäden zu übersetzen.

Sie ermöglichen zudem klarere Diskussionen über Resilienz und Versicherungsdeckung. KI bedingte Schäden lassen sich möglicherweise nicht eindeutig einer einzigen Risikokategorie zuordnen. Ein durch Deepfake ermöglichter Zahlungsbetrug, ein KI bezogener Datenvorfall, ein fehlerhafter Output, der Schäden bei Dritten verursacht, oder ein Ausfall bei einem kritischen Anbieter können jeweils andere Bereiche der Unternehmensrisiken und des und Versicherungsprogramms betreffen.

Diese Szenarien früh zu verstehen hilft, Klarheit darüber zu schaffen, wo bestehende Kontrollen und Deckungen greifen, wo Unsicherheit besteht und wo zusätzliche Maßnahmen zur Risikominderung nötig sind.

AXA XL bringt Risikoberatung, Cyber Expertise und Versicherungswissen zusammen, um diese breitere Sicht auf KI Resilienz zu unterstützen. Gemeinsam mit Spezialpartnern wie S RM liegt der Fokus darauf, Organisationen bei der Identifikation ihrer Risiken, der Stärkung ihrer Governance, der Vorbereitung auf neue Incident Szenarien und bei fundierteren Entscheidungen zum Risikotransfer zu unterstützen.

Das Ziel besteht nicht darin, Innovation zu bremsen, sondern Unternehmen zu befähigen, KI mit Zuversicht einzuführen: Risiken zu verstehen, sie durch starke Governance und Resilienz zu bewältigen und zu beurteilen, wo sie übertragen oder versichert werden können.

Mit der Einbettung von KI in zentrale Geschäftsprozesse müssen Unternehmen verstehen, wie sich ihr Gesamt Risikoprofil verändert.
KI sollte nicht ausschließlich als Technologierisiko gesehen werden sondern als eine Frage der unternehmensweiten Resilienz, die Cybersicherheit, Daten Governance, Abhängigkeiten von Drittanbietern, Betriebskontinuität, regulatorische Verantwortlichkeit und Versicherungsschutz miteinander verbindet.

# Abschließende Überlegungen

**Der Einsatz von KI zeigt keine Anzeichen einer Verlangsamung. Die größte Herausforderung für Unternehmen ist daher heute, sicherzustellen, dass KI im großen Maßstab vertrauenswürdig eingesetzt werden kann.**

Dazu gehört, zu verstehen, wie KI im eigenen Unternehmen eingesetzt wird, Governance über ihren gesamten Lebenszyklus zu verankern und sicherzustellen, dass die Sicherheit mit der Technologie Schritt hält. Organisationen, die diese Grundlagen heute legen, werden besser gerüstet sein, sich an neue Bedrohungen und fortschreitende Regulierung anzupassen.

Vertrauenswürdige KI erfordert zudem eine enge Zusammenarbeit von Unternehmensleitung, Risikomanagement, Rechtsabteilung, Sicherheits  und operativen Funktionen, unterstützt von Partnern, die sowohl die Chancen durch KI als auch die damit einhergehenden Herausforderungen verstehen.

Unternehmen, die Governance, Sicherheit und Resilienz fest in ihre Arbeitsabläufe integrieren, werden das volle Potenzial von KI erschließen und sich mit Zuversicht anpassen können, während sich diese leistungsstarke Technologie weiterentwickelt.

# Haftungsausschluss

Dieser Bericht beruht auf Analysen einer Vielzahl von Quellen, darunter öffentlich zugängliche Berichte, Einsichten und Analysen sowie proprietäre Analysen und Erkenntnisse von AXA XL und S RM, basierend auf ihren internen Daten. Eine nicht erschöpfende Liste öffentlich verfügbarer Quellen ist im Bericht enthalten, stellt jedoch nicht die einzige Grundlage der gewonnenen Einsichten dar.

Die in diesem Bericht dargestellten Analysen basieren auf den zum Zeitpunkt der Erstellung verfügbaren Informationen. Aussagen zu möglichen zukünftigen Entwicklungen sind keine Vorhersagen zu Trends und Bedrohungen, sondern beschreiben den potenziellen Kontext, in dem Organisationen künftig agieren müssen.

Global Asset Protection Services, LLC, XL Catlin Services SE und deren verbundene Unternehmen („AXA XL Risk Consulting“) stellen auf Anfrage Berichte zur Schadenverhütung und Risikobewertung sowie andere Risk Consulting Services zur Verfügung. In diesem Zusammenhang befassen sich unsere Veröffentlichungen, Services und Begehungen zur Sachschadenverhütung nicht mit Fragen der Personensicherheit oder Haftung gegenüber Dritten.

Dieses Dokument darf nicht als Hinweis auf das Bestehen oder die Verfügbarkeit von Versicherungsschutz für eine bestimmte Art von Verlust oder Schaden unter einer konkreten Police ausgelegt werden. Die Erbringung von Leistungen bedeutet nicht, dass jede potenzielle Gefahr an einem Standort identifiziert wurde oder dass es keine weiteren Gefahren gibt. AXA XL Risk Consulting übernimmt keine Verantwortung für Kontrolle, Korrektur, Fortführung oder Veränderung bestehender Bedingungen oder Abläufe.

Wir lehnen ausdrücklich jede Garantie oder Zusicherung ab, wonach die Einhaltung von Ratschlägen oder Empfehlungen in diesem Dokument oder anderen Mitteilungen einen Standort oder Betrieb sicher oder gesund machen oder in Übereinstimmung mit einem Standard, Code, Gesetz, einer Regel oder Vorschrift bringen würde.

Sofern nicht ausdrücklich schriftlich vereinbart, lehnen AXA XL Risk Consulting und verbundene sowie angeschlossene Unternehmen jede Haftung für Verluste oder Schäden ab, die einer Partei im Zusammenhang mit unseren Services entstehen – einschließlich mittelbarer oder Folgeschäden, gleich welcher Art. Jede Partei, die sich in irgendeiner Weise auf den Inhalt dieses Dokuments stützt, tut dies auf eigenes Risiko.

Die hierin enthaltenen Informationen dienen ausschließlich zu Informationszwecken. Der Versicherungsschutz im Einzelfall hängt von der Art der Police, ihren Bedingungen, Klauseln und Ausschlüssen sowie den Umständen des spezifischen Falles ab.

Es wird keinerlei Zusicherung gemacht, dass ein bestimmter Versicherungsschutz unter den hier beschriebenen Umständen greifen würde. Bitte ziehen Sie die einzelnen Policenformulare für spezifische Deckungsdetails heran. Diese Zusammenfassung stellt weder ein Angebot, noch eine Aufforderung oder Werbung in irgendeiner Jurisdiktion dar, noch beschreibt sie Produkte oder Dienstleistungen von AXA XL im Detail.

AXA XL ist eine Division der AXA Gruppe und bietet Produkte und Dienstleistungen über drei Geschäftsbereiche an: AXA XL Insurance, AXA XL Reinsurance und AXA XL Risk Consulting.

In den USA sind die AXA XL Versicherungsgesellschaften:
AXA XL Insurance Company Americas, Greenwich Insurance Company, Indian Harbor Insurance Company, XL Insurance America, Inc., XL Specialty Insurance Company und AXA XL Excess & Surplus Lines Insurance Company.

In Kanada werden Versicherungsdeckungen von XL Specialty Insurance Company — Canadian Branch — gezeichnet.

Auf Bermuda ist XL Bermuda Ltd. die Versicherungsgesellschaft. Deckungen können zudem von Lloyd’s Syndicate Nr. 2003 gezeichnet werden.

Deckungen, die von Lloyd’s Syndicate Nr. 2003 gezeichnet werden, werden im Namen des Mitglieds des Syndicates Nr. 2003 durch Catlin Canada Inc. platziert. Die Ratings von Lloyd’s sind unabhängig von AXA Group.

Nicht alle genannten Versicherer sind in allen Jurisdiktionen tätig, und Deckungen sind nicht überall verfügbar.



**axaxl.com**