Holger Reibold

# ISO 42001

## KI verantwortbar steuern

## Executable Compliance umsetzen

## Der Managementleitfaden

BRAIN-MEDIA.DE

Holger Reibold

# ISO 42001

## KI verantwortbar steuern

## Executable Compliance umsetzen

## Der Managementleitfaden

BRAIN-MEDIA.DE

ISBN: 978-3-95444-368-0

Cover: Freepik

Brain-Media.de

Dr. Holger Reibold – Huber-Müller-Str. 52 – 66113 Saarbrücken

info@brain-media.de – www.brain-media.de

# Inhaltsverzeichnis

# Vorwort

*KI-Governance wird zur Führungsaufgabe*

Unternehmen befinden sich mitten in einer technologischen Transformation, deren Dynamik und Tragweite mit früheren Digitalisierungswellen nur bedingt vergleichbar ist. Künstliche Intelligenz entwickelt sich zunehmend zu einer universellen Steuerungs- und Automatisierungstechnologie. Generative KI, große Sprachmodelle, autonome Entscheidungssysteme und datengetriebene Assistenzmechanismen verändern Geschäftsmodelle, Wertschöpfungsketten und Organisationsstrukturen tiefgreifend.

Gleichzeitig steigen die regulatorischen Anforderungen in einem bislang unbekannten Ausmaß. Mit dem EU AI Act etabliert die Europäische Union erstmals einen umfassenden regulatorischen Rahmen für KI-Systeme. Ergänzt wird dieser durch bestehende Vorgaben aus der DSGVO, Anforderungen der NIS-2-Richtlinie, Cybersecurity-Regularien, Produkthaftungsregeln sowie branchenspezifische Aufsichtsanforderungen. Unternehmen müssen heute nicht mehr nur nachweisen, dass KI-Systeme funktional sind, sondern dass sie kontrollierbar, sicher, nachvollziehbar und verantwortbar betrieben werden.

Die regulatorische Entwicklung verändert damit die Rolle von KI grundlegend. KI wird nicht länger ausschließlich als Innovations- oder Effizienztechnologie betrachtet, sondern zunehmend als regulierter Bestandteil unternehmerischer Kernprozesse. Governance wird dadurch zu einer strategischen Voraussetzung für den nachhaltigen KI-Einsatz.

Besonders herausfordernd ist dabei die Geschwindigkeit technologischer Veränderungen. Viele Organisationen verfügen bereits heute über eine Vielzahl isolierter KI-Initiativen, die historisch unabhängig voneinander entstanden sind. Fachbereiche implementieren generative KI-Werkzeuge, Entwicklungsabteilungen integrieren Machine-Learning-Modelle in Produkte, Sicherheitsabteilungen nutzen KI-basierte Analyseverfahren und Managementfunktionen setzen auf automatisierte Entscheidungsunterstützung.

Was zunächst als dezentrale Innovationsdynamik erscheint, entwickelt sich schnell zu einer komplexen Governance-Herausforderung. Unterschiedliche Datenquellen, uneinheitliche Kontrollmechanismen, fehlende Transparenz über Modellnutzung und unklare Verantwortlichkeiten führen zu einer fragmentierten KI-Landschaft. Unternehmen verlieren dadurch häufig die Übersicht darüber, welche KI-Systeme tatsächlich im Einsatz sind, welche Risiken bestehen und welche regulatorischen Anforderungen gelten.

Genau hierin liegt eines der größten strukturellen Probleme moderner KI-Governance: Klassische Compliance-Ansätze reichen für KI-Systeme nicht mehr aus.

Traditionelle Governance- und Compliance-Modelle wurden primär für stabile, deterministische IT-Systeme entwickelt. KI-Systeme hingegen sind dynamisch, probabilistisch und häufig adaptiv. Modelle verändern ihr Verhalten durch neue Daten, generative Systeme erzeugen nicht vollständig deterministische Ergebnisse, und autonome Entscheidungsmechanismen können Risiken erzeugen, die sich nicht allein durch statische Richtlinien kontrollieren lassen.

Dokumentenbasierte Compliance verliert dadurch an Wirksamkeit. Richtlinien allein verhindern weder Halluzinationen generativer Systeme noch diskriminierende Entscheidungen oder Sicherheitsrisiken durch manipulierte Trainingsdaten. Governance muss deshalb wesentlich näher an die technischen Betriebs- und Entwicklungsprozesse rücken.

Unternehmen benötigen ein Steuerungsmodell, das organisatorische Governance, Risikomanagement, technische Kontrollen und kontinuierliche Überwachung integriert. Genau hier gewinnen Managementsysteme für KI an Bedeutung.

Ein Artificial Intelligence Management System (AIMS) nach ISO/IEC 42001 schafft einen strukturierten Rahmen, um KI systematisch zu steuern. Es definiert Verantwortlichkeiten, Governance-Prozesse, Kontrollmechanismen, Risikoanalysen und kontinuierliche Verbesserungsprozesse. Vor allem jedoch schafft ein AIMS Transparenz über den gesamten KI-Lebenszyklus.

Ein integriertes AI Management System ermöglicht Unternehmen:

- KI-Systeme systematisch zu inventarisieren,
- Risiken strukturiert zu bewerten,
- regulatorische Anforderungen kontrolliert umzusetzen,
- technische und organisatorische Kontrollen zu verbinden,
- Governance-Prozesse auditierbar zu gestalten,
- Verantwortlichkeiten klar zu definieren,
- und Vertrauen in KI-basierte Entscheidungen aufzubauen.

Dabei ist entscheidend, dass ein modernes AIMS nicht isoliert betrieben wird. Die eigentliche Stärke entsteht durch die Integration in bestehende Managementsysteme wie Informationssicherheit, Datenschutz, Qualitätsmanagement, Enterprise Risk Management und interne Kontrollsysteme.

KI-Governance wird damit zu einer Querschnittsfunktion der gesamten Organisation.

Besonders relevant ist in diesem Zusammenhang die Verbindung von Governance und technischer Operationalisierung. Unternehmen stehen vor der Herausforderung, regulatorische Anforderungen nicht nur formal zu dokumentieren, sondern technisch wirksam umzusetzen. Governance muss daher zunehmend automatisierbar, kontinuierlich überprüfbar und in operative Plattformen integrierbar sein.

Die Zukunft der KI-Compliance liegt deshalb in steuerbaren und operationalisierten Kontrollmodellen. Continuous Monitoring, Policy

Automation, technische Evidenzketten und Governance-by-Design werden zu zentralen Bestandteilen moderner KI-Steuerung.

Die neue Realität der KI-Governance besteht somit nicht allein aus zusätzlicher Regulierung. Sie markiert vielmehr den Übergang zu einer neuen Form unternehmerischer Steuerung, in der Technologie, Governance, Risiko- und Compliance-Management eng miteinander verschmelzen.

Unternehmen, die diese Entwicklung frühzeitig strategisch adressieren, schaffen nicht nur regulatorische Sicherheit. Sie schaffen die Grundlage für vertrauenswürdige, skalierbare und langfristig resiliente KI-Organisationen.

Ich wünsche Ihnen dabei viel Erfolg!

Herzlichst

Holger Reibold

# 1 Verantwortbare KI-Steuerung

*Warum Responsible AI jetzt entscheidend ist*

Die Einführung künstlicher Intelligenz verändert nicht nur Technologien und Geschäftsmodelle, sondern auch die Art und Weise, wie Unternehmen gesteuert, kontrolliert und reguliert werden. KI-Systeme treffen Entscheidungen, erzeugen Inhalte, analysieren große Datenmengen und beeinflussen operative sowie strategische Prozesse zunehmend autonom. Damit verschiebt sich Governance von einer rein organisatorischen Disziplin hin zu einer Kombination aus Management, Risikoüberwachung und technischer Steuerung.

Verantwortbare KI-Steuerung bedeutet deshalb weit mehr als die Einhaltung regulatorischer Anforderungen. Sie umfasst die Fähigkeit einer Organisation, KI-Systeme transparent, kontrollierbar, nachvollziehbar und langfristig belastbar zu betreiben. Unternehmen benötigen hierfür klare Verantwortlichkeiten, wirksame Kontrollmechanismen, belastbare Governance-Strukturen und eine enge Verzahnung zwischen Management, Compliance und Technologie.

ISO/IEC 42001 schafft erstmals einen international standardisierten Rahmen für ein Artificial Intelligence Management System (AIMS). Die Norm definiert Anforderungen an Governance, Risikomanagement, Dokumentation, kontinuierliche Verbesserung und

organisatorische Verantwortlichkeiten entlang des gesamten KI-Lebenszyklus. Gleichzeitig macht sie deutlich, dass KI-Governance nicht isoliert betrachtet werden kann. Sie muss mit Informationssicherheit, Datenschutz, Qualitätsmanagement und Enterprise Risk Management integriert werden.

Dieses Kapitel erläutert die Grundlagen moderner KI-Governance, die Struktur und Zielsetzung von ISO/IEC 42001 sowie die zentralen Elemente eines wirksamen AI Management Systems. Darüber hinaus wird gezeigt, warum verantwortbare KI zu einer strategischen Managementaufgabe geworden ist und weshalb die Zukunft regulatorisch belastbarer KI in operationalisierten und technisch steuerbaren Governance-Modellen liegt.

## 1.1 Die Entwicklung von KI-Governance

Die Governance technologischer Systeme ist kein neues Thema. Bereits mit der zunehmenden Digitalisierung unternehmerischer Prozesse entstanden Anforderungen an strukturierte Steuerungs- und Kontrollmodelle für Informationssysteme. Frühere Governance-Ansätze konzentrierten sich vor allem auf Stabilität, Verfügbarkeit, Sicherheit und Wirtschaftlichkeit klassischer IT-Infrastrukturen. Frameworks wie COBIT, ITIL oder ISO 27001 entstanden in einer Zeit, in der IT-Systeme überwiegend deterministisch arbeiteten und sich ihre Risiken vergleichsweise klar definieren ließen.

Mit der zunehmenden Nutzung datengetriebener Verfahren und maschinellen Lernens veränderte sich jedoch die Charakteristik technologischer Risiken grundlegend. KI-Systeme treffen Wahrscheinlichkeitsentscheidungen, entwickeln sich durch neue Daten dynamisch weiter und erzeugen Ergebnisse, die selbst für Entwickler nicht immer vollständig nachvollziehbar sind. Gleichzeitig beeinflussen diese Systeme zunehmend kritische Geschäftsprozesse, Kundeninteraktionen, Sicherheitsmechanismen und regulatorisch relevante Entscheidungen.

Dadurch entstand ein grundlegender Wandel von klassischer IT-Governance hin zu AI-Governance.

Während traditionelle IT-Governance primär auf Stabilität und Betriebssicherheit ausgerichtet war, erweitert KI-Governance den Fokus um Transparenz, Nachvollziehbarkeit, Fairness, Verantwortung und kontinuierliche Risikosteuerung. KI-Systeme müssen nicht nur technisch funktionieren, sondern auch regulatorischen, ethischen und gesellschaftlichen Anforderungen genügen. Unternehmen stehen deshalb vor der Herausforderung, technologische Innovation mit kontrollierbarer Governance zu verbinden.

Besonders deutlich wird dieser Wandel durch die internationale regulatorische Entwicklung. Regierungen, Aufsichtsbehörden und Standardisierungsgremien arbeiten weltweit an Rahmenwerken für vertrauenswürdige KI. Die OECD veröffentlichte früh grundlegende AI Principles, die Transparenz, Robustheit und Verantwortlichkeit in den Mittelpunkt stellen. Das NIST AI Risk Management Framework in

den USA adressiert insbesondere Risikosteuerung und Governance-Strukturen. Parallel dazu entwickelt die ISO mit Standards wie ISO/IEC 42001 und ISO 23894 internationale Management- und Risikomodelle für KI-Systeme.

Innerhalb Europas markiert insbesondere der EU AI Act einen regulatorischen Meilenstein. Er definiert erstmals verbindliche Anforderungen an Entwicklung, Einsatz und Überwachung von KI-Systemen. Der Schwerpunkt liegt dabei auf risikobasierten Kontrollmodellen, Transparenzpflichten, menschlicher Aufsicht und dokumentierter Nachweisfähigkeit.

Gleichzeitig reicht regulatorische Compliance allein nicht aus, um vertrauenswürdige KI zu etablieren. Die Diskussion über Responsible AI zeigt, dass Governance zunehmend auch ethische Fragestellungen umfasst. Themen wie Diskriminierung, algorithmische Verzerrungen, mangelnde Transparenz oder der Verlust menschlicher Kontrolle betreffen nicht nur regulatorische Risiken, sondern auch Reputation, gesellschaftliches Vertrauen und langfristige Akzeptanz.

Ethik, Transparenz und Verantwortung entwickeln sich damit zu zentralen Steuerungsprinzipien moderner KI-Governance. Unternehmen müssen sicherstellen, dass KI-Systeme nachvollziehbar, überprüfbar und kontrollierbar bleiben. Governance wird dadurch zu einer interdisziplinären Aufgabe, die Management, Compliance, Technologie, Risikomanagement und Unternehmenskultur miteinander verbindet.

Die Entwicklung von KI-Governance zeigt somit einen klaren Trend: Weg von isolierten technischen Kontrollmodellen hin zu integrierten Governance-Systemen, die regulatorische Anforderungen, operative Steuerung und technische Umsetzung miteinander verschmelzen lassen. Genau diese Entwicklung bildet die Grundlage moderner AI Management Systeme nach ISO/IEC 42001.

## 1.2 Was ISO/IEC 42001 konkret regelt

ISO/IEC 42001 ist der erste international veröffentlichte Managementsystemstandard speziell für künstliche Intelligenz. Ziel der Norm ist es, Unternehmen einen strukturierten Rahmen zur Steuerung, Überwachung und kontinuierlichen Verbesserung von KI-Systemen bereitzustellen. Im Mittelpunkt steht dabei der Aufbau eines Artificial Intelligence Management Systems, das Governance, Risiko- und Kontrollmechanismen organisatorisch verankert.

Die Norm folgt der sogenannten High-Level Structure (HLS), die bereits aus anderen ISO-Managementsystemen bekannt ist. Dadurch wird eine Integration mit bestehenden Standards wie ISO 27001, ISO 9001 oder ISO 22301 erheblich erleichtert. Die HLS definiert einheitliche Kapitelstrukturen für Themen wie Kontext der Organisation, Führung, Planung, Support, Betrieb, Leistungsbewertung und kontinuierliche Verbesserung.

ISO/IEC 42001 adressiert insbesondere die besonderen Eigenschaften von KI-Systemen. Dazu zählen dynamische Modelle,

probabilistische Ergebnisse, datenabhängiges Verhalten sowie Risiken durch mangelnde Transparenz oder unzureichende Kontrolle. Die Norm fordert deshalb, dass Unternehmen Verantwortlichkeiten definieren, Risiken bewerten, Kontrollen implementieren und die Wirksamkeit ihrer Governance-Maßnahmen regelmäßig überprüfen.

Ein wesentlicher Bestandteil der Norm ist der risikobasierte Ansatz. Unternehmen müssen KI-Systeme hinsichtlich potenzieller Auswirkungen auf Menschen, Organisationen und Gesellschaft analysieren. Dabei geht es nicht ausschließlich um technische Risiken, sondern auch um ethische, regulatorische und operative Fragestellungen.

Die Norm unterscheidet außerdem zwischen verbindlichen Anforderungen und ergänzenden Leitlinien. Während die Hauptkapitel konkrete Managementanforderungen definieren, enthalten Anhänge zusätzliche Orientierung zu Governance, Transparenz, Datenmanagement, Monitoring oder Human Oversight.

Im Unterschied zu ISO 27001 liegt der Fokus nicht primär auf Informationssicherheit, sondern auf der umfassenden Steuerung von KI-Systemen. ISO 9001 konzentriert sich auf Qualitätsmanagement und Prozessstabilität, während ISO 31000 allgemeine Prinzipien des Risikomanagements beschreibt. ISO/IEC 42001 verbindet diese Perspektiven speziell für KI und erweitert sie um Governance-, Transparenz- und Kontrollanforderungen. Die strategische Bedeutung der Norm liegt vor allem darin, dass sie einen international anerkannten Rahmen für vertrauenswürdige KI schafft. Unternehmen erhalten damit nicht nur ein Governance-Modell für regulatorische Anforderungen,

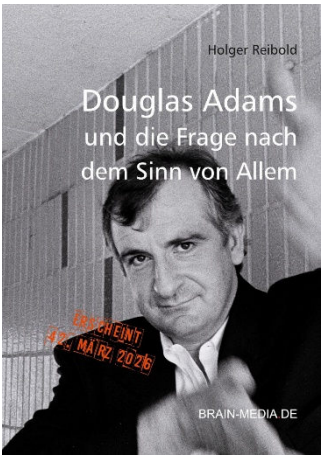
sondern auch eine Grundlage für Skalierbarkeit, Auditierbarkeit und langfristige Vertrauensbildung.


*Abbildung 1: Das Schichtenmodell zeigt, wie strategische Führung, Governance, Risiko- und Kontrollmechanismen sowie technische Operationalisierung innerhalb eines AI Management Systems zusammenwirken.*

## 1.3 Die Kernelemente

Ein Artificial Intelligence Management System bildet die organisatorische Grundlage für die kontrollierte Nutzung künstlicher Intelligenz. Ziel eines AIMS ist es, Governance, Risiko- und Kontrollmechanismen systematisch entlang des gesamten KI-Lebenszyklus zu etablieren. Im Zentrum stehen belastbare Governance-Strukturen. Unternehmen benötigen klare organisatorische Verantwortlichkeiten für

# Mehr von Brain-Media.de




**42 – Douglas Adams und die Frage nach dem Sinn von Allem**

Am 11. Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

Preis: 14,99 EUR

Erscheint: 42. März 2026


**Towelday, das ultimative Handtuch für alle Fans**

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.

100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.

**Executable Compliance**

**Compliance, die läuft.**


Regulierung wird komplexer – klassische Ansätze stoßen an ihre Grenzen. Executable Compliance überführt Anforderungen in eine strukturierte, maschinenlesbare Compliance-Schicht, die direkt in Ihre Systeme integriert wird. Im Zentrum: das Brain-Media Audit Model (BAM):

**Requirement → Gap-Check → Remediation**
**→ Risk → Control → Evidence**

Das Ergebnis: ein durchgängiger, auditfähiger Datenstrom.

- Audit-Ready auf Knopfdruck
- Collect Once, Comply Many
- Nahtlose Integration in GRC & IT
- KI-Ready durch strukturierte Daten

Executable Compliance ist keine Software, sondern eine Infrastruktur. Für mehr Effizienz, Transparenz und Wettbewerbsvorteile.

Compliance als System. Nicht als Projekt.