Heft 40 | Dezember 2024 | 18. Jahrgang | ISSN 1864-6557

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e.V.



AUSZUG
AUS HEFT 40

Normen und Standards für die KI-Governance

Michael Klotz, Luisa-Elene Pissors, Benjamin Birkmann

ISACA Germany Chapter

dpunkt.verlag | it-governance.dpunkt.de | isaca.de

Heft 40 | 2024

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e.V.

Inhalt

Fachthemen

2 **Bedeutung von IAM vor dem Hintergrund von NIS-2**
Ingo Struckmeyer, Andreas Lehner

8 **IT-Governance bei immersiven digitalen Zwillingen**
Ein erster Eindruck von ihren Herausforderungen
Petra Haferkorn, Christopher R. Healey

Rubriken

14 Zum Thema
»Human in the Loop« und verwandte Konzepte im Rahmen der KI-Governance
Jakob Schneider, Anna Fries, Matthias Goeken

22 Zum Thema
Die Zukunft der KI unter EU-Regulierung: Was erwartet Unternehmen?
Eric Per Vogel

29 IT-Prüfung
Prüfkatalog für das neue IT-Audit-Thema »Gesetzeskonformer Umgang mit IT-Diagnose-Daten«
Stephen Fedtke

37 Standards
Normen und Standards für die KI-Governance
Michael Klotz, Luisa-Elene Pissors, Benjamin Birkmann

41 **Inserenten**

41 **Vorschau**

41 **Impressum**

Standards
Normen und Standards für die KI-Governance

Michael Klotz, Luisa-Elene Pissors, Benjamin Birkmann

Der Einsatz von künstlicher Intelligenz (KI) schreitet in Unternehmen rasch voran. In einer aktuellen Studie von McKinsey setzen 72 % der befragten Unternehmen KI bereits in mindestens einer Unternehmensfunktion ein [Singla et al. 2024, S. 3]. Um im Wettbewerb zu bestehen, sind Unternehmen gefordert, nutzbringende Anwendungsbereiche zu identifizieren, notwendige finanzielle Ressourcen zu allokieren, entsprechendes technisches Know-how aufzubauen, den gesetzeskonformen Einsatz KI-gestützter Systeme sicherzustellen, entstehende Risiken zu minimieren und die Sicherheit dieser Systeme zu gewährleisten. In all diesen Handlungsbereichen besteht für Unternehmen ein Orientierungsbedarf (vgl. [Klotz et al. 2024]). Eine Möglichkeit, diesen Bedarf zu decken, bieten entsprechende Normen und Standards. Diese stehen mittlerweile zahlreich zur Verfügung. Um diesbezüglich Transparenz zu schaffen, wurde an der Hochschule Stralsund im Rahmen des Projekts »Mittelstand-Digital Zentrum Rostock« eine Studie zu den aktuell verfügbaren Normen und Standards für die Governance des KI-Einsatzes durchgeführt und in einem Arbeitspapier dokumentiert (vgl. [Klotz & Pissors 2024]). Die Ergebnisse werden im Rahmen dieses Artikels zusammengefasst.

1 KI-Governance

KI-Governance wird hier – basierend auf dem Verständnis von KI-Systemen als IT-Systeme – als auf KI-Systeme bezogene IT-Governance aufgefasst (nach [Mäntymäki et al. 2022, S. 605]). Dementsprechend wird das IT-Governance-Verständnis der ISO/IEC 38500:2024 zugrunde gelegt [ISO/IEC 38500:2024]. Dieses wird wesentlich durch elf Grundsätze beschrieben, die als Handlungsfelder für eine IT-Governance angesehen werden können. Diese Grundsätze sind: Zweck, Wertschöpfung, Strategie, Aufsicht, Rechenschaftspflicht, Einbindung von Anspruchsgruppen, Führung, Daten und Entscheidungen, Risikobeherrschung, gesellschaftliche Verantwortung sowie langfristige Existenzfähigkeit und Leistung (vgl. [Klotz 2024, S. 20 f.]).

2 Normung und Standardisierung im Bereich der KI

Die im Rahmen der Studie für KI-Governance als relevant identifizierten Normungs- und Standardisierungsorganisationen sind:

- DIN Deutsches Institut für Normung e. V. (DIN)
- International Organization for Standardization (ISO)
- Europäisches Komitee für Normung (CEN)
- International Electrotechnical Commission (IEC)
- Institute of Electrical and Electronics Engineers (IEEE)
- National Institute of Standards and Technology (NIST)
- Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW)

Dass Normierung und Standardisierung für diese Organisationen aktuell eine große Rolle spielen, lässt sich daran erkennen, dass beispielsweise sowohl das DIN als auch das NIST entsprechende umfangreiche Vorhaben aufgelegt haben.

- Das DIN realisiert derzeit ein Projektprogramm zur Umsetzung der Handlungsempfehlungen aus der »Deutschen Normungsroadmap für Künstliche Intelligenz«. Mit Partnern aus Industrie, Forschung und Verwaltung führt das DIN verschiedene Umsetzungsprojekte durch, aus denen konkrete Normungs- und Standardisierungsbedarfe abgeleitet und in Normen und Standards umgesetzt werden (vgl. [DIN 2024]).
- Das NIST richtet aktuell seine Aktivitäten auf ein globales Engagement zur Förderung und Entwicklung von KI-Standards. Das Ziel ist es auch hier, die Entwicklung und Umsetzung von KI-bezogenen Normen und Standards voranzutreiben. Unter Beteiligung von Akteuren des öffentlichen und privaten Sektors veröffentlichte das NIST am 26. Juli 2024 den »Plan for Global Engagement on AI Standards« (vgl. [NIST 2024]).

Diese Bestrebungen werden von den jeweiligen Regierungen unterstützt bzw. beauftragt. Für Unternehmen lohnt es sich, derartige Initiativen zu verfolgen, um einerseits von dem in den entstehenden Normen und Standards enthaltenen Know-how zu profitieren und um sich andererseits auf sich abzeichnende Qualitäts- und Konformitätsprüfungen einstellen zu können.

3 KI-Normen und -Standards

Es konnten insgesamt 16 für KI-Governance relevante Normen und Standards identifiziert werden (vgl. Tab. 1), wobei im Falle der Normen auch technische Reports (TR) und Spezifikationen (TS) berücksichtigt wurden.

Elf Normen (inkl. technischer Reports und Spezifikationen) und Standards stammen aus den Jahren 2023 und 2024, die restlichen fünf Normen und Standards aus den Jahren 2020 und 2022. Lediglich drei Normen befinden sich als Entwurf

Lfd. Nr.	Norm/Standard		Jahr	Gültig	Entwurf
1	DIN SPEC 92001-3	Artificial Intelligence – Life Cycle Processes and Quality Requirements – Part 3: Explainability	2023	X	
2	E DIN EN ISO/ IEC 23894	Informationstechnik – Künstliche Intelligenz – Leitlinien für Risikomanagement (ISO/IEC 23894:2023)	2023		X
3	IDW PS 861	Prüfung von KI-Systemen	2023	X	
4	IEEE 7010-2020	IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being	2020	X	
5	ISO/IEC 5259-1	Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 1: Overview, terminology, and examples	2024	X	
6	ISO/IEC 5259-3	Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 3: Data quality management requirements and guidelines	2024	X	
7	ISO/IEC 5259-4	Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 4: Data quality process framework	2024	X	
8	ISO/IEC FDIS 5259-5	Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 5: Data quality governance framework	2023		X
9	ISO/IEC 22989	Information technology – Artificial intelligence – Artificial intelligence concepts and terminology	2022	X	
10	ISO/IEC 23894	Information technology – Artificial intelligence – Guidance on risk management	2023	X	
11	ISO/IEC TR 24368	Information technology – Artificial Intelligence – Overview of ethical and societal concerns	2022	X	
12	ISO/IEC 24668	Information technology – Artificial intelligence – Process management framework for big data analytics	2022	X	
13	ISO/IEC 38507	Information technology – Governance of IT – Governance implications of the use of artificial intelligence by organizations	2022	X	
14	ISO/IEC 42001	Information technology – Artificial intelligence – Management system	2023	X	
15	ISO/IEC DIS 42005	Information technology – Artificial intelligence – AI system impact assessment	2024		X
16	NIST AI 100-1	Artificial Intelligence Risk Management Framework (AI RMF 1.0)	2023	X	

Tab. 1: Für KI-Governance relevante Normen und Standards

im Normungsverfahren. Hierbei stellt die E DIN EN ISO/IEC 23894 die europäische bzw. deutsche Übernahme der bereits gültigen internationalen Norm ISO/IEC 23894 dar. Nur bei zwei der Normen ist der Governance-Begriff Teil des Titels: bei der ISO/IEC FDIS 5259-5 und der ISO/IEC 38507. Letztere ist Teil der Normenreihe ISO/IEC 385XX.

Die inhaltlichen Schwerpunkte liegen in den Governance-Bereichen Risikobeherrschung, Umgang mit Daten (insb. Datenqualität) und KI-gestützten Entscheidungen sowie der gesellschaftlichen Verantwortung (Auswirkungen von KI-Systemen, ethische und gesellschaftliche Aspekte der KI-Nutzung). Im Arbeitspapier wird der Inhalt jeder Norm bzw. jedes Standards in Bezug zu den elf Governance-Grundsätzen der ISO/IEC 38500 gesetzt, sodass sich Schwerpunkte und Lücken deutlicher erkennen lassen. Aus der Anzahl der von einer Norm bzw. einem Standard adressierten Governance-Bereiche lässt sich zudem ihre Relevanz für KI-Governance erkennen.

4 Beschreibung der KI-Normen und -Standards

Im Rahmen des Arbeitspapieres [Klotz 2024] werden alle KI-Normen und -Standards systematisch dargestellt. Für jede Norm werden

- Titel,
- aktuelle Version,
- herausgebende Institution,
- Status,
- Seitenumfang,
- eine Inhaltsbeschreibung,
- ein Bezug zu Governance-Grundsätzen und
- ein Link zur Fundstelle der jeweiligen Norm bzw. des Standards

angegeben. Tabelle 2 zeigt eine derartige Darstellung für den Entwurf der DIN EN ISO/IEC 23894.

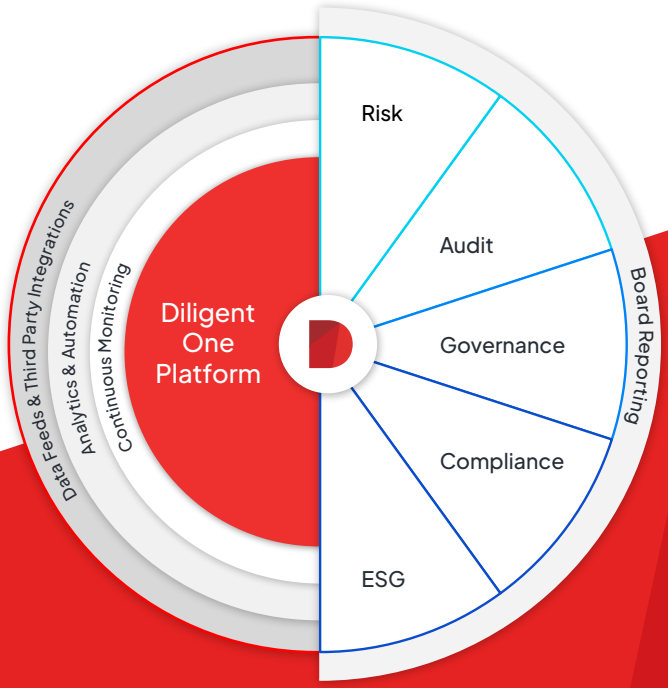
Titel	E DIN EN ISO/IEC 23894 Informationstechnik – Künstliche Intelligenz – Leitlinien für Risikomanagement (ISO/IEC 23894:2023)
Aktuelle Version	Auflage 1, 2023-11
Organisation	DIN Deutsches Institut für Normung e. V.
Status	Entwurf
Umfang	36 Seiten
Inhalt	Die Norm richtet sich an Organisationen, die KI-gestützte Produkte, Systeme und Dienstleistungen entwickeln, herstellen, einsetzen oder nutzen. Für diese Organisationen enthält die Norm Leitlinien für die Integration des Risikomanagements in die KI-bezogenen Aktivitäten und Funktionen. Dementsprechend basiert die ISO/IEC 23894 auf der Risikomanagement-Norm ISO 31000, auf die umfangreich Bezug genommen wird. Im Mittelpunkt der Ausführungen steht ein auf KI-Risiken bezogenes Risikomanagement, das auch viele Aspekte der Risiko-Governance adressiert. Wegen »potenziell weitreichender Auswirkungen der KI auf Stakeholder« sollen diese umfangreich eingebunden werden. Ein weiterer Schwerpunkt bildet die Compliance mit Gesetzen (insb. hinsichtlich Datenschutz), Verträgen, Normen und Leitlinien. Auch soziale und ethische Aspekte der Nutzung von KI werden angesprochen. Drei Anhänge gehen auf Ziele des KI-Einsatzes, Risikoquellen und eine Verbindung des Risikomanagementprozesses mit dem Lebenszyklus eines KI-Systems ein. Hierbei geht es auch um die Risiken, die ausgehend von der eingesetzten KI die Unternehmensumwelt bedrohen, sowie um Bedrohungen der KI-Systeme durch die Umwelt.
Grundsätze	4, 6, 9, 10, 11
Link	DIN: *https://www.dinmedia.de/de/norm-entwurf/din-en-iso-iec-23894/373239039*

Tab. 2: Systematische Beschreibung der E DIN EN ISO/IEC 23894

Anzeige

Diligent

Clarify risk.
Find opportunity.
Elevate governance.



Scan to request a demo

For more information:
info@diligent.com
diligent.com

Die in der Zeile »Grundsätze« genannten Nummern verweisen auf die in der ISO/IEC 38500 genannten Governance-Grundsätze der IT-Governance (vgl. hierzu [Klotz 2024]). Für die E DIN EN ISO/IEC 23894 sind dies Aufsicht, Einbindung von Anspruchsgruppen, Risikobeherrschung, gesellschaftliche Verantwortung sowie langfristige Existenzfähigkeit und Leistung. Die Norm deckt also fünf der elf Governance-Grundsätze ab, was ihre hohe Relevanz für die KI-Governance belegt.

5 Fazit

Die vorliegende Studie zeigt die bereits heute bestehende Vielfalt und Bedeutung von Normen und Standards für die Governance von KI-Systemen auf. Die zunehmende Normierung und Standardisierung in diesem Bereich trägt dazu bei, eine effektive KI-Governance und hierdurch einen verlässlichen, gesetzeskonformen und transparenten Einsatz von KI-Systemen zu gewährleisten. Unternehmen stehen vor der Herausforderung, KI effektiv, sicher und gesetzeskonform in die bestehende IT-Infrastruktur zu integrieren. Hierbei können Normen und Standards eine wertvolle Orientierung bieten. Das im Rahmen der Studie erstellte Arbeitspapier bietet als Handreichung für die Praxis einen aktuellen Überblick über die für KI-Governance relevanten Normen und Standards.

Literatur

[DIN 2024] *DIN Deutsches Institut für Normung e. V.:* Projekte zu KI und Normung; *https://www.din.de/de/forschung-und-innovation/themen/kuenstliche-intelligenz/projekte-zu-ki-und-normung*; Zugriff am 17.10.2024.

[ISO/IEC 38500:2024] *ISO/IEC:* Information technology – Governance of IT for the organization, International Standard ISO/IEC 38500:2024, 3rd edition 2024-02-23.

[Klotz 2024] *Klotz, M.:* IT-Governance genormt – die neue ISO/IEC 38500 (revolutions). IT-Governance 18 (2024), 39, S. 19-24.

[Klotz & Pissors 2024] *Klotz, M.; Pissors, L.-E.:* KI-Normen und -Standards – Unterstützung für die Gestaltung der KI-Governance. SIMAT Arbeitspapiere, Hochschule Stralsund, Jg. 16, 2024, *https://www.researchgate.net/publication/385906684_KI-Normen_und_-Standards_-Unterstutzung_fur_die_Gestaltung_der_KI-Governance*; Zugriff am 17.10.2024.

[Klotz et al. 2024] *Klotz, M.; Adam, W.; Noack-Sandring, L.; Schueschke, N.:* Literaturstudie zu den Handlungsbereichen einer Governance für den Einsatz von KI- Systemen im Unternehmen. In: Klein, M. et al. (Hrsg.): Proceedings INFORMATIK 2024 Lock-in or log out? Wie digitale Souveränität gelingt. 24.-26.09.2024, Wiesbaden, Gesellschaft für Informatik, Bonn 2024, S. 1595-1604, DOI: 10.18420/inf2024_139, Zugriff am 17.10.2024.

[Mäntymäki et al. 2022] *Mäntymäki, M.; Minkkinen, M.; Birkstedt, T.; Viljanen, M.:* Defining organizational AI governance. AI and Ethics 2 (2022), 4, S. 603-609.

[NIST 2024] *National Institute of Standards and Technology (NIST): AI Standards; https://www.nist.gov/artificial-intelligence/ai-standards;* Zugriff am 17.10.2024.

[Singla et al. 2024] *Singla, A.; Sukharevsky, A.; Yee, L.; Chui, M.:* The state of AI in early 2024: Gen AI adoption spikes and starts to generate value, Mai 2024; *https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai#/;* Zugriff am 17.10.2024.



Michael Klotz

ist seit 1999 Professor für Betriebswirtschaftslehre, insb. Informationsmanagement, Organisation und Datenverarbeitung an der Hochschule Stralsund. Davor war er 15 Jahre in der IT-Branche als Berater, Projektmanager und Geschäftsführer tätig. Seine fachliche Arbeit dokumentiert sich in über 100 Publikationen zu IT-Governance, IT-Compliance und Projektmanagement.



Luisa-Elene Pissors

ist wissenschaftliche Mitarbeiterin im Mittelstand-Digital Zentrum Rostock und Masterstudentin der Angewandten Data Science und Künstlichen Intelligenz mit Fokus auf explorative Datenanalyse, Machine Learning und IT-Governance an der Hochschule Stralsund. Sie hat Erfahrung in Python, R und SQL und ist begeistert von der Entwicklung innovativer Lösungen und automatisierter Entscheidungsfindung.



Benjamin Birkmann

studiert Wirtschaftsinformatik an der Hochschule Stralsund. Er sammelte Erfahrungen als Consultant bei OSCAR in der Prozessanalyse. Er ist Gründer der Baltic Student Solutions und arbeitet als studentische Hilfskraft im Mittelstand-Digital Zentrum Rostock.

Prof. Dr. Michael Klotz
Luisa-Elene Pissors
Benjamin Birkmann
Hochschule Stralsund
Fakultät für Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
{michael.klotz, luisa-elene.pissors, benjamin.birkmann}@hochschule-stralsund.de
www.hochschule-stralsund.de

Hinweis
Diese Arbeit wurde im Rahmen des Projekts »Mittelstand-Digital Zentrum Rostock« durchgeführt, gefördert durch das Bundesministerium für Wirtschaft und Klimaschutz in Deutschland.