Klotz, Michael; Pissors, Luisa-Elene

Working Paper

KI-Normen und -Standards – Unterstützung für die Gestaltung der KI-Governance

SIMAT Arbeitspapiere, No. 16-24-043

Provided in Cooperation with:
Hochschule Stralsund, Stralsund Information Management Team (SIMAT)

Suggested Citation: Klotz, Michael; Pissors, Luisa-Elene (2024) : KI-Normen und -Standards – Unterstützung für die Gestaltung der KI-Governance, SIMAT Arbeitspapiere, No. 16-24-043, Hochschule Stralsund, Stralsund Information Management Team (SIMAT), Stralsund

This Version is available at:
https://hdl.handle.net/10419/307147

SIMAT Arbeitspapiere
Herausgeber: Prof. Dr. Michael Klotz

SIMAT AP 16-24-043

KI-Normen und -Standards – Unterstützung für die Gestaltung der KI-Governance

Prof. Dr. Michael Klotz
Luisa-Elene Pissors

Hochschule Stralsund
SIMAT Stralsund Information Management Team

November 2024

ISSN 1868-064X

Klotz, Michael; Pissors, Luisa-Elene: KI-Normen und -Standards – Unterstützung für die Gestaltung der KI-Governance. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: Hochschule Stralsund, SIMAT Stralsund Information Management Team, 2024 (SIMAT AP, 16 (2024), 43), ISSN 1868-064X

Impressum

Hochschule Stralsund
Zur Schwedenschanze 15
18435 Stralsund
www.hochschule-stralsund.de

Herausgeber

Prof. Dr. Michael Klotz
Fakultät für Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
E-Mail: michael.klotz@hochschule-stralsund.de

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

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

Autor/-in

Prof. Dr. Michael 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 150 Publikationen zu IT-Governance, IT-Compliance und Projektmanagement.

Luisa-Elene Pissors ist wissenschaftliche Mitarbeiterin der Fakultät für Wirtschaft an der Hochschule Stralsund. Im Projekt „Mittelstand-Digital Zentrum Rostock“ unterstützt sie kleine und mittlere Unternehmen bei der Einführung und Nutzung von KI-Systemen.

KI-Normen und -Standards – Unterstützung für die Gestaltung der KI-Governance

Prof. Dr. Michael Klotz, Luisa-Elene Pissors[1]

Gliederung

Zusammenfassung: Dieses Arbeitspapier gibt einen Überblick über aktuelle Normen und Standards, die für die Governance des Einsatzes von Künstlicher Intelligenz (KI) im Unternehmen von Bedeutung sind. Es werden Normen der International Organization for Standardization (ISO), der ISO gemeinsam mit der International Electrotechnical Commission (IEC), des Deutschen Instituts für Normung (DIN) sowie europäische Normen (EN) berücksichtigt. Bei den Standards werden solche Organisationen als relevant erachtet, die in der Lage sind, den von ihnen publizierten KI-Standard einem breiten, mit der Anwendung von KI bzw. der Nutzung KI-gestützter Systeme befassten Adressatenkreis zugänglich zu machen und eine Weiterentwicklung des Standards sicherzustellen. Beispiele für derartige Organisa-

[1] Prof. Dr. Michael Klotz, Hochschule Stralsund, michael.klotz@hochschule-stralsund.de; Luisa-Elene Pissors, Wissenschaftliche Mitarbeiterin, Fakultät für Wirtschaft, Zur Schwedenschanze 15, 18435 Stralsund, luisa-elene.pissors@hochschule-stralsund.de

tionen sind das National Institute of Standards and Technology (NIST) und das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW). Insgesamt werden zwölf spezialisierte KI-Normen, fünf Governance-Normen und vier KI-Standards beschrieben, beispielsweise der Entwurf der Norm DIN EN ISO/IEC 23894 zu Leitlinien für das Risikomanagement oder die Norm ISO/IEC 38507 zu den Governance-Implikationen beim Einsatz von KI-Systemen. Als KI-Standard ist z. B. NIST AI 100-1 mit dem Artificial Intelligence Risk Management Framework enthalten. Mit dem IDW PS 861 findet auch ein Standard für die Prüfung von KI-gestützten Systemen Berücksichtigung. Neben den KI-Normen werden fünf allgemeine Governance-Normen beschrieben, die einigen der KI-Normen zugrunde liegen oder von diesen referenziert werden.

Die einzelnen Normen und -Standards werden nach einer einheitlichen Struktur beschrieben: Jede Beschreibung enthält den Titel, die aktuelle Version, die herausgebende Institution, den formalen Status, den Seitenumfang und eine prägnante Inhaltsangabe zu den Governance-Bezügen der Norm bzw. des Standards. Dann wird der Inhalt in Bezug zu den elf Governance-Grundsätzen der ISO 37000 gesetzt, so dass sich Schwerpunkte und Lücken erkennen lassen. Abschließend werden Links für die eigene Recherche angegeben. Insofern soll dieses Arbeitspapier nicht nur eine aktuelle, systematische Zusammenstellung bieten, sondern es stellt auch eine Hilfestellung für ein schnelles Orientieren und Nachschlagen dar.

Schlüsselwörter: DIN – Governance – ISO – ISO/IEC – KI – KI-Governance – Künstliche Intelligenz – Normen – Standards

JEL-Klassifikation: L15, M10, M21, M42

Vorwort

Zu dem in diesem Arbeitspapier versuchten Überblick über aktuelle Normen und Standards zur Governance des Einsatzes Künstlicher Intelligenz (KI) bedarf es keines Anlasses – der Bedarf hierfür liegt auf der Hand. Branchenverbände, Expertinnnen und Experten aus der Wissenschaft sowie Fachleute aus den Unternehmen stufen KI als wichtigen – wenn nicht künftig den wichtigsten – Wettbewerbsfaktor ein. Sie sehen KI als disruptive Schlüsseltechnologie, die neue digitale Geschäftsmodelle ermöglicht und bestehende Prozesse und Produkte erweitern kann. Dementsprechend schreitet der Einsatz von KI in deutschen Unternehmen aller Branchen und Größenordnungen schnell voran. Die nationale und transnationale Politik adressiert mit ihrer Regulierung Risiken, die sich aus dem Einsatz der KI ergeben, und schreibt entsprechend zu ergreifende Maßnahmen vor. Insbesondere der EU AI Act will sicherstellen, dass auf dem EU-Markt eingeführte KI-Systeme sicher sind und die in der EU geteilten Grundrechte und Werte wahren, während gleichzeitig Investitionen und Innovationen im KI-Bereich gefördert werden sollen. Der Handlungsbedarf für Planung, Steuerung und Überwachung des Einsatzes KI-gestützter Systeme im Unternehmen ist somit beträchtlich. Normen und Standards sollen naturgemäß in einem wichtigen Handlungsfeld Orientierung und Anleitung bieten. Insofern ist es nicht überraschend, wenn zahlreiche Normungs- und Standardisierungsorganisationen KI-Normen und -Standards entwickeln. Die diesbezügliche Dynamik ist so groß, dass es sich lohnt, einen ersten Überblick über Normen und Standards zur Governance des KI-Einsatzes zu erlangen. Dies ist das Ziel dieses Arbeitspapiers.

Die im Folgenden vorgenommene Auflistung wird bald nach Erscheinen veraltet sein. Hinweise zu notwendigen Aktualisierungen sowie zu weiterhin aufzunehmenden KI-Normen und -Standards sind jederzeit willkommen und werden in einer Neuauflage berücksichtigt. Wir danken unserer studentischen Hilfskraft, Benjamin Birkmann, für die Recherchearbeit und die Unterstützung bei der tabellarischen Aufbereitung. Bei den Kolleginnen der Bibliothek der Hochschule Stralsund bedanken wir uns für die Bereitstellung der verschiedenen Normen.

Prof. Dr. Michael Klotz
Luisa-Elene Pissors

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abb.	Abbildung
AI	Artificial Intelligence
BDA	Big Data Analytics
CEN	Comité Européen de Normalisation (Europäisches Komitee für Normung)
CEN-CLC/JTC	CEN-CENELEC Joint Technical Committee
DIN	Deutsches Institut für Normung e. V.
DIS	Draft International Standard
E	Entwurf
EN	Europäische Norm
EU	Europäische Union
FDIS	Final Draft International Standard
ID-Nummer	Identifizierungsnummer
IDW	Institut der Wirtschaftsprüfer in Deutschland e. V.
IDW PS	IDW-Prüfungsstandard
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IHK	Industrie- und Handelskammer
ISO	International Organization for Standardization
IT	Informationstechnik / Informationstechnologie
KI	Künstliche Intelligenz
KIMS	KI-Managementsystem
Mio.	Millionen
ML	Machine Learning
MSS	Management System Standard
NIST	National Institute of Standards and Technology
PAS	Publicly Available Specification
SP	Special Publication
SPEC	Specification
Std	Standard
Tab.	Tabelle
TM	Trademark
TR	Technical report
TS	Technical specification
TÜV	Technischer Überwachungsverein
Tz.	Teilziffer

1 Einleitung

Rolle von Normen und Standards

Normen und Standards – gleich in welchem Themenbereich – entstehen vor dem Hintergrund einer breit geteilten Interessenlage; sie bieten Orientierung und Anleitung für wichtige praktische Aufgabenstellungen. Diese richten sich allgemein auf die Sicherstellung der Effektivität und der Effizienz und ggf. weiterer Zielsetzungen (z. B. Sicherheit, Compliance) des in Frage stehenden Anwendungsbereiches – hier des Einsatzes von KI-gestützten Systemen im Unternehmen.[2]

1.1 Abgrenzung von Normen und Standards

Die Begriffe „Normen“ und „Standards“ werden oftmals synonym verwendet. Somit stellt sich die Frage, was unter „Norm“[3] zu verstehen ist und welcher Zusammenhang zwischen den beiden Begriffen „Standard“ und „Norm“ besteht.[4] Da Normen eine Spezialisierung von Standards darstellen, soll zuerst der Begriff des Standards geklärt werden.[5]

Standards

Ein Standard stellt eine grundlegende Beschreibung dar, wie etwas zu tun, zu lösen oder handzuhaben ist. Hierzu werden Handlungsbereiche durch Definitionen, Verfahren, Strukturmodelle, Prozesse, zu ergreifende Maßnahmen u. Ä. strukturiert.

Merkmale von Standards

Aber nicht jede Zusammenfassung von Konzepten und Modellen, Richtlinien, Best Practices, Empfehlungen u. Ä. kann als Standard qualifiziert werden. Zur bloßen Existenz als schriftliches Dokument muss hinzukommen, dass die als Standard beschriebenen Inhalte breit akzeptiert und angewendet werden. Der Akzeptanzbereich kann dabei geographisch (z. B. auf einen Staat oder eine Staatengemeinschaft) oder auf eine nationale, internationale oder globale Anwendergruppe (z. B. Ingenieure, Applikationsentwickler) beschränkt sein. Weiterhin müssen die Mitglieder der Anwendergruppe den Standard nicht nur kennen und akzeptieren, sondern auch wirklich praktisch nutzen. Aus dieser Nutzung sollte sich zudem eine Rückkopp-

[2] Der Text in diesem Kapitel ist im Wesentlichen übernommen aus *Klotz 2013*, S. 10-17, bzw. fasst diesen Text zusammen.
[3] Der hier verwendete Begriff der „Norm“ ist zu unterscheiden vom Begriff der Rechtsnorm, der rechtliche Regelwerke (Gesetze, Verordnungen, Satzungen) und Verwaltungsvorschriften umfasst.
[4] Eine begriffliche Verwirrung kann leicht dadurch entstehen, dass der englische Begriff „standard“ i. d. R. eine Norm bezeichnet.
[5] Im Folgenden nach *Klotz 2020*, S. 872f.

lung für die Weiterentwicklung des Standards ergeben. Hieran ist regelmäßig eine größere Anzahl von Anwendungsexpertinnen und -experten beteiligt.[6]

Anwendergruppe

Als Anwendergruppe für KI-Standards (wie auch für KI-Normen) kommen grundsätzlich alle am KI-Einsatz beteiligte Stakeholder in Frage, z. B. Leitungsorgane, Projektleiterinnen und -leiter, Projektauftraggeber oder Mitglieder von Projektlenkungsausschüssen, betroffene Mitarbeiterinnen und Mitarbeiter in der KI-Systementwicklung oder -nutzung sowie unternehmensinterne und -externe Auditoren, die KI-Systeme prüfen.

Verbreitung von Standards

Die Durchsetzbarkeit eines KI-Standards und damit seine Verbreitung in einer Anwendergruppe ergeben sich zum einen aus der Größe der jeweiligen Organisation, die die Verwertungsrechte an dem Standard innehat. Gewöhnlich handelt es sich um Mitgliederorganisationen, vor allem Vereine, so dass zu erwarten ist, dass die Verbreitung umso umfangreicher ausfällt, je größer die Mitgliederbasis dieser Vereine ist. Die alleinige Verbreitung im Mitgliederkreis reicht jedoch nicht aus. Von einer wesentlichen Verbreitung lässt sich erst dann sprechen, wenn ein Großteil der Anwender, auch ohne Mitglied zu sein, den Standard kennt und nutzt. Dies wird gewöhnlich dadurch erreicht, dass die Organisationen das Know-how für die Nutzung in Weiterbildungsmaßnahmen vermitteln, das erlangte Know-how prüfen und bei erfolgreicher Prüfung Zertifikate als Kompetenz-Nachweis vergeben. Je mehr nun diese Zertifikate in der Praxis anerkannt werden, umso eher ergeben sich der Druck und damit die Motivation, diese Zertifikate zu erlangen. Für die KI-Thematik existieren derzeit zahlreiche Angebote für persönliche Zertifikate, die im Zusammenhang mit einer Teilnahme an einer Weiterbildungsveranstaltung erworben werden. Diese werden vor allem von Universitäten und Hochschulen, Industrie- und Handelskammern (IHKs) sowie den TÜV-Organisationen offeriert. Die diesbezügliche Situation ist momentan unübersichtlich. Dementsprechend können Qualität und Werthaltigkeit dieser Zertifikate nur schwer beurteilt werden.

Normen

Normen beschreiben „wissenschaftlich begründete Arbeitsmethoden zur Bewältigung rationeller, meist wiederholbarer Arbeitsprozesse … bzw. Qualitäts- und Sicherheitsanforderungen“.[7] Sie werden von einer offiziellen Nor-

[6] Bspw. sind am Standard „IEEE Std 7010™-2020“ insgesamt 139 Personen (v. a. als Mitglieder der Arbeits-, Abstimmungs- und Genehmigungsgruppen) beteiligt.
[7] *VOI 2008*, S. 18.

mungsorganisation als Ergebnis eines systematischen, festgelegten Normungsverfahrens beschlossen und veröffentlicht. Eine Norm ist ein „Dokument, das mit Konsens erstellt und von einer anerkannten Institution angenommen wurde und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt, wobei ein optimaler Ordnungsgrad in einem gegebenen Zusammenhang angestrebt wird“.[8]

Verbindlichkeit von Normen

Aufgrund des formalisierten Erstellungsprozesses beinhalten Normen in der Regel nicht den innovativsten Stand eines Anwendungsgebietes. Sie schreiben vielmehr die durch praktische Bewährung allgemein anerkannten Regeln eines bestimmten Anwendungsbereiches fest (sog. „Stand der Technik“). Insofern werden Normen häufig – ggf. von externen Gutachtern – herangezogen um festzustellen, ob Sorgfaltspflichten eingehalten bzw. verletzt wurden. Die Einhaltung von Normen wird zudem mitunter in nationalen und internationalen Vorschriften, d. h. vor allem in Gesetzen und Verordnungen, verbindlich vorgeschrieben. In diesen Fällen erlangt eine Norm eine unmittelbare rechtliche Bindungswirkung.[9] Dies ist auch dann der Fall, wenn die Orientierung an Normen (aber auch an Standards) oder gar ihre strikte Einhaltung vertraglich vereinbart wird.

Normungsorganisation

Eine Norm erhält dadurch einen offiziellen Charakter, dass die jeweilige Normungsorganisation dazu in der Lage ist, die Norm in ihrem Geltungsbereich (fachlich) durchzusetzen. Eine Normungsorganisation ist eine Institution, „die auf nationaler, regionaler oder internationaler Ebene anerkannt ist und als wesentliche Funktion, ..., die Erstellung, Anerkennung oder Annahme von Normen hat, welche der Öffentlichkeit zugänglich sind“.[10] In den folgenden Ausführungen werden Normen folgender Normungsorganisationen berücksichtigt:

- Deutsches Institut für Normung e. V. (DIN),
- International Organization for Standardization (ISO),
- International Electrotechnical Commission (IEC),
- Europäisches Komitee für Normung (CEN).

[8] *DIN EN 45020*, S. 25.
[9] Nach *VOI 2008*, S. 18.
[10] *DIN EN 45020*, S. 31.

1.2 Auswahl der KI-Normen und -Standards

Governance-orientierung

Entsprechend der gewählten inhaltlichen Fokussierung werden im Folgenden prinzipiell nur solche Normen und Standards betrachtet, die für die Governance des KI-Einsatzes im Unternehmen relevant sind. Dies bedeutet jedoch nicht, dass sie sich vollumfänglich und ausschließlich auf KI-Governance beziehen müssen. Es werden auch solche Normen berücksichtigt, die nur einzelne Handlungsbereiche adressieren. Bezüglich der Herkunft der Normen erfolgt eine Fokussierung auf die im vorherigen Abschnitt genannten Normungsorganisationen.

Status

In Bezug auf den Status werden sowohl gültige Normen als auch noch im Entwurf befindliche Normen herangezogen. Bei Normentwürfen wurde darauf geachtet, dass diese sich in einer fortgeschrittenen Normungsphase befinden.[11] Neben Normen wurden auch von den Normungsorganisationen herausgegebene „Technische Reports“ (TR) und „Technische Spezifikationen“ (TS) berücksichtigt.

- Technische Reports fokussieren ein bestimmtes Thema, z. B. Prüfkonzepte, Fallstudien oder Methoden. Sie enthalten Informationen, die für Normenentwickler und andere Zielgruppen nützlich sind. Sie sind jedoch niemals normativ.[12]
- Technische Spezifikationen sind ähnlich detailliert und umfangreich wie Normen, haben aber noch nicht alle Genehmigungsstufen durchlaufen, weil entweder noch kein Konsens erzielt wurde oder weil die Normung noch nicht als ausgereift angesehen wird.[13]

Schwierige Abgrenzung

Gerade bei den Technischen Reports und Spezifikationen ist es im Einzelfall schwer zu entscheiden, ob diese noch der Governance-Ebene zuzurechnen sind. Ein Beispiel hierfür ist die ISO/IEC TS 8200. Die ISO/IEC TS 8200 richtet sich auf die operative Kontrollierbarkeit von KI-Systemen. Dieser Norm können somit Hinweise für IT/KI-Kontrollsysteme entnommen werden – ein Aspekt, der die Governance-Grundsätze der Aufsicht und der Risikobeherrschung adressiert. Wegen der sehr operativen Ausrichtung, die auch Design- und Implementierungsempfehlungen beinhaltet, soll diese TS jedoch nicht den Governance-Normen zugerechnet werden.

[11] Beispielsweise befindet sich die ISO/IEC DIS 5259-5 im Approval-Status 50.20 (Proof sent to secretariat or FDIS ballot initiated).
[12] Nach *IEC 2024a.*
[13] Nach *IEC 2024b.*

ISO/IEC TS 8200

Titel	ISO/IEC TS 8200 Information technology – Artificial Intelligence – Controllability of automated artificial intelligence systems
Aktuelle Version	First edition, 2024-04
Organisation	ISO International Organization for Standardization IEC International Electrotechnical Commission
Status	Stage 60.60 International Standard published
Umfang	34 Seiten
Inhalt	Die ISO/IEC TS 8200 beschreibt Modelle und Ansätze für die Realisierung und Verbesserung der Kontrollierbarkeit von KI-Systemen. Die Norm legt den Fokus auf die Fähigkeit, den Zustand eines KI-Systems zu beobachten und zu steuern, den Prozess der Kontrollübernahme (insb. durch einen menschlichen Akteur), den Umgang mit Unsicherheiten während dieser Übergänge und die Überprüfung und Validierung der Kontrollierbarkeit. Die Norm behandelt verschiedene Kontrollmechanismen, die sicherstellen, dass KI-Systeme sicher, vorhersehbar und unter menschlicher Kontrolle bleiben, auch wenn sie zunehmend automatisierte Entscheidungen treffen.
Link	ISO-Webseite: https://www.iso.org/standard/83012.html

Auch im Umfeld von Standards gibt es weitere Dokumente, die jedoch eher den Charakter einer Fachpublikation haben, als dass sie normativ verbindliche bzw. zumindest empfehlende Aussagen enthalten. Im Einzelfall können derartigen Dokumenten durchaus hilfreiche Ausführungen zur KI-Governance entnommen werden. Ein Beispiel hierfür ist die NIST SP 1270, die sich als „Special Publikation“ mit der Identifizierung von und dem Umgang mit Vorurteilen in KI-Systemen auseinandersetzt.

NIST SP 1270

Titel	NIST Special Publication 1270 Towards a Standard for Identifying and Managing Bias in Artificial Intelligence
Aktuelle Version	Ausgabe 2022-03
Organisation	NIST National Institute of Standards and Technology
Status	Veröffentlicht
Umfang	86 Seiten
Inhalt	Diese NIST Special Publication konzentriert sich auf die Identifikation und das Management von Bias (Vorurteilen) in KI-Systemen. Sie definiert drei Hauptkategorien von Bias (systemische, statistische und menschliche Vorurteile) und analy-

	siert deren Auswirkungen auf Einzelpersonen, Organisationen und die Gesellschaft. Die Publikation bietet Leitlinien zur Minimierung dieser Vorurteile und betont die Wichtigkeit eines sozio-technischen Ansatzes, um sicherzustellen, dass KI-Systeme vertrauenswürdig und fair sind.
Link	NIST-Dokument: https://doi.org/10.6028/NIST.SP.1270

Ein weiterer Sonderfall ist die DIN SPEC 92001-3. Hierbei handelt es sich um eine Spezifikation, wobei das Dokument vom DIN selbst als „Standard“ bezeichnet wird. Ein derartiger Standard, der vom DIN herausgegeben wird, soll von einem Netzwerk relevanter Marktteilnehmer initiiert und erstellt werden, wobei jedoch nicht alle Interessengruppen beteiligt werden müssen. Als Themen für eine DIN SPEC kommen z. B. neuartige Herstellungs- oder Prüfkonzepte oder die Nutzung einer innovativen Technologie in Frage. Das DIN bindet weitere Akteure und die Öffentlichkeit ein, übernimmt das Projektmanagement und klärt die Widerspruchsfreiheit mit nationalen, europäischen und internationalen Normen.[14]

Datenherkunft

Die in diesem Arbeitspapier enthaltenen Daten zu den Normen und Standards wurden den Originaldokumenten bzw. den jeweiligen Webseiten der Normungsinstitute und Standardisierungsorganisationen entnommen.

1.3 KI-Governance

KI-Governance

Für KI-Governance finden sich in der Literatur spezifische Definitionen. So verstehen Mäntymäki et al. unter AI governance ein “system of rules, practices, processes, and technological tools that are employed to ensure an organization’s use of AI technologies aligns with the organization’s strategies, objectives, and values; fulfills legal requirements; and meets principles of ethical AI followed by the organization.”[15] Zweifellos werden hier zahlreiche Facetten der KI-Governance abgedeckt. Es stellt sich jedoch die Frage, ob es wirklich eines eigenen Governance-Begriffs für den KI-Einsatz bedarf.

KI-Systeme als IT-Systeme

Ausgehend vom Verständnis von KI-Systemen als IT-Systeme wird KI-Governance in diesem Arbeitspapier, als auf KI-Systeme bezogene Corpo-

[14] Nach *DIN 2024a.*
[15] *Mäntymäki et al. 2022*, S. 604.

rate bzw. IT-Governance verstanden.[16] Entsprechend wird auf das IT-Governance-Verständnis der ISO 37000 zurückgegriffen. Weiterhin ist die ISO/ IEC 38500:2024 von Bedeutung. Im Zentrum dieser Norm stehen die aus der ISO 37000 übernommenen elf Governance-Grundsätze, die auf die Governance der Unternehmens-IT übertragen werden.

Governance-Grundsätze

Die elf Governance-Grundsätze sind: Zweck, Wertschöpfung, Strategie, Überwachung, Rechenschaftspflicht, Einbeziehung von Interessengruppen, Führung, Daten und Entscheidungen, Risikomanagement, gesellschaftliche Verantwortung sowie langfristige Lebensfähigkeit und Leistungsfähigkeit. Entsprechend der ISO 37000 sind die Grundsätze in drei Kategorien eingeteilt: primär (primary), grundlegend (foundational) und unterstützend (enabling), vgl. Abb. 1. [Klotz 2024], S. 20f.).

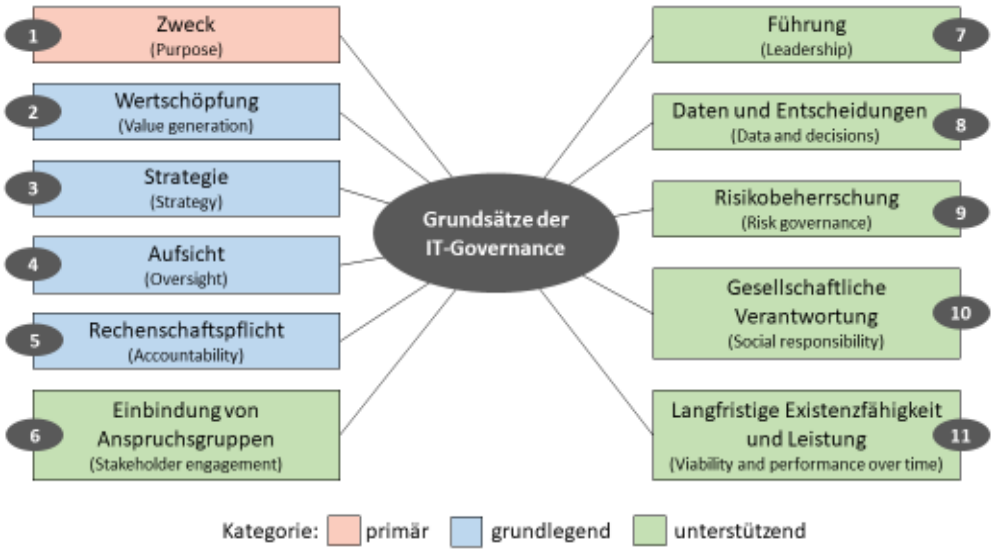

Abbildung 1
Die elf Grundsätze der IT-Governance nach ISO 38500:2024[17]

Die Orientierung an dem Governance-Verständnis der ISO 37000 bzw. der ISO/IEC 38500 erfolgt wegen der Anschlussfähigkeit an diese internationalen Normen. Weiterhin ergibt sich der Vorteil, dass das in den Grundsätzen abgebildete Governance-Verständnis umfassend ist und die verschiedensten Governance-Aspekte integriert. Zudem wird durch den Anschluss deutlich, dass KI-Governance keine eigenständige Disziplin darstellt, sondern inhalt-

[16] In Anlehnung an *Mäntymäki et al. 2022*, S. 605.
[17] Entnommen aus *Klotz 2024*, S. 20. Siehe diesen Aufsatz auch für eine nähere Erläuterung der elf Grundsätze.

lich, methodisch, konzeptionell, prozessual etc. in die IT- bzw. Corporate Governance integriert ist (bzw. in diese zu integrieren ist), vgl. Abb. 2.

Abbildung 2
Corporate, IT- und KI-Governance[18]

Dass der Bedarf an Orientierung in Bezug auf eine KI-Governance hoch ist, zeigt eine aktuelle Studie von Deloitte. Zu den konkreten Maßnahmen, die die befragten Unternehmen derzeit ergreifen, gehören die Einrichtung eines Governance-Rahmens für die Nutzung von generativen KI-Tools und -Anwendungen (51 %), die Überwachung der gesetzlichen Anforderungen und die Sicherstellung der Compliance (49 %) sowie die Durchführung interner Audits/Tests für generative KI-Tools und -Anwendungen (43 %). Hervorzuheben ist, dass trotz ihrer Bedeutung für eine effektive Steuerung und Überwachung des KI-Einsatzes jede dieser Maßnahmen nur von weniger als der Hälfte der befragten Unternehmen ergriffen wird.[19]

[18] Eigene Darstellung.
[19] Nach *Rowan et al. 2024*, S. 18.

2 Normen für KI-Governance

Im Folgenden werden die verschiedenen KI-Normen im Einzelnen dargestellt. Hierzu werden zuerst einige grundlegende Basisdaten (zum Titel, zur aktuellen Version, zur herausgebenden Institution, zum aktuellen Status und zum Umfang) genannt. Daran schließt sich eine kurze Inhaltsangabe an, die die für KI-Governance relevanten Inhalte/Elemente einer Norm fokussieren. Daran schließt sich eine Zuordnung der Inhalte zu den elf Governance-Grundsätzen an. Die Tabellen enden mit Angabe der jeweiligen Weblinks, die zu den Normen oder Standards führen.

Die Auflistung von insgesamt 17 Normen wird in drei Gruppen gegliedert, DIN EN ISO/IEC-Normen, ISO/IEC-Normen und allgemeine Governance-Normen, s. Tabelle 1.

Tabelle 1
Gruppierung der KI-Normen

Gruppe			Anzahl
1	DIN EN ISO-Normen	• E DIN EN ISO/IEC 23894	1
2	ISO/IEC-Normen	• ISO/IEC 5259-1 • ISO/IEC 5259-3 • ISO/IEC 5259-4 • ISO/IEC DIS 5259-5 • ISO/IEC 22989 • ISO/IEC 23894 • ISO/IEC TR 24368 • ISO/IEC 24668 • ISO/IEC 38507 • ISO/IEC 42001 • ISO/IEC DIS 42005	11
3	Allgemeine Normen	• DIN ISO 31000 • DIN ISO 37000 • ISO 31000 • ISO 37000 • ISO/IEC 38500	5
Insgesamt			17

2.1 DIN EN ISO/IEC-Normen

DIN EN-Normen

DIN EN ISO/IEC-Normen entstehen, wenn eine ISO/IEC-Norm als Europäische Norm (EN) übernommen wurde und nun das DIN wiederum diese EN als deutsche Norm übernimmt. Die Übernahme der Norm durch das DIN-Institut hat eine Übersetzung der Norm ins Deutsche zur Folge. Im

Falle der E DIN EN ISO/IEC 23894 hat das Komitee CEN-CLC/JTC 21 „Künstliche Intelligenz“ die ISO/IEC 23894 als Europäische Norm übernommen.

E 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.[20] 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 sich auch auf viele Aspekte der Risiko-Governance richtet. Wegen „potenziell weitreichender Auswirkungen der KI auf Stakeholder“[21] 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, als auch um Bedrohungen der KI-Systeme durch die Umwelt.
Grundsätze	4, 6, 9, 10, 11
Link	DIN-Webseite: https://www.dinmedia.de/de/norm-entwurf/din-en-iso-iec-23894/373239039

[20] Nach *E DIN EN ISO/IEC 23894*, S. 7.
[21] *E DIN EN ISO/IEC 23894*, S. 9.

2.2 ISO/IEC-Normen

Zwei der im Folgenden dargestellten ISO/IEC-Normen tragen den Begriff „Governance“ bereits im Titel. Dies sind die ISO/IEC 38507 zu den Governance-Implikationen beim Einsatz von KI und die ISO/IEC DIS 5259-5, die ein Governance-Framework für die Datenqualität beschreibt. Die weiteren für KI-Governance relevanten Normen befassen sich schon von ihrem Titel her jeweils mit einzelnen Governance-Aspekten. So fokussiert bspw. der Technische Report ISO/IEC 24368 ethische und gesellschaftliche Belange beim KI-Einsatz.

ISO/IEC 5259-Reihe

Ziel der ISO/IEC 5259-Reihe ist die Bereitstellung von Werkzeugen und Methoden zur Bewertung und Verbesserung der Qualität der für Data Analytics und Machine Learning (ML) verwendeten Daten.[22] Ihr Governance-Schwerpunkt liegt im Bereich der Data Governance. Die Normenreihe beinhaltet eine ausdrückliche Governance-Norm, die ISO/IEC 5259-5. Da diese aber auf den anderen Normen der Normenreihe beruht bzw. mit diesen inhaltlich in Zusammenhang steht, werden auch weitere für KI-Governance relevante ISO/IEC 5259-Normen beschrieben.

ISO/IEC 5259-1

Titel	ISO/IEC 5259-1 Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 1: Overview, terminology, and examples
Aktuelle Version	First edition, 2024-07
Organisation	ISO International Organization for Standardization IEC International Electrotechnical Commission
Status	Stage 60.60 International Standard published
Umfang	19 Seiten
Inhalt	Diese Norm bildet die terminologische Grundlage für die gesamte ISO/IEC 5259-Reihe. Sie bietet einen Überblick über die Grundlagen der Datenqualität für Data Analytics/ML. Neben Begriffsdefinitionen beinhaltet sie auch aus Governance-sicht wesentliche Konzepte und Modelle für Datenqualität. Ein Datenqualitätsmodell für Data Analytics/ML bildet die Grundlage für die Festlegung von Qualitätsanforderungen und die Bewertung der Datenqualität.[23] Ein weiteres grundlegendes Modell richtet sich auf den Daten-Lebenszyklus, dessen Pha-

[22] Nach *ISO/IEC 529-1*, S. V.
[23] Nach *ebd.*, S. 7.

	sen mit Prozessen, wie Datenschutz, Datensicherheit und Governance von Datenqualität, verbunden werden.[24]
Grundsätze	8
Link	ISO-Webseite: https://www.iso.org/standard/81088.html

ISO/IEC 5259-3

Titel	ISO/IEC 5259-3 Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 3: Data quality management requirements and guidelines
Aktuelle Version	First edition, 2024-07
Organisation	ISO International Organization for Standardization IEC International Electrotechnical Commission
Status	Stage 60.60 International Standard published
Umfang	28 Seiten
Inhalt	Diese Norm legt Anforderungen und Leitlinien für das Qualitätsmanagement von Daten für Data Analytics/ML fest. Der Fokus liegt auf dem in der ISO/IEC 5259-1 einführend beschriebenen Lebenszyklusmodell für Datenqualität, das acht Stufen umfasst: (1) Motivation und Konzeptualisierung, (2) Datenspezifikation, (3) Datenplanung, (4) Datenakquisition, (5) Datenvorverarbeitung, (6) Datenanreicherung, (7) Datenbereitstellung und (8) Datendeaktivierung abdeckt.[25] Darüber hinaus werden Hinweise für ein auf Datenqualitätsrisiken bezogenes Risikomanagement gegeben.
Grundsätze	8, 9
Link	ISO-Webseite: https://www.iso.org/standard/81092.html

ISO/IEC 5259-4

Titel	ISO/IEC 5259-4 Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 4: Data quality process framework
Aktuelle Version	First edition, 2024-07
Organisation	ISO International Organization for Standardization IEC International Electrotechnical Commission
Status	Stage 60.60 International Standard published
Umfang	28 Seiten
Inhalt	Diese Norm beschreibt ein Prozessmodell für Datenqualität,

[24] Vgl. *ebd.*, S. 13.
[25] Vgl. *ISO/IEC 529-3*, S. 6-8.

	das mit den Lebenszyklusphasen für Datenqualität integriert ist.[26] Das Prozessmodell besteht aus vier Prozessen (Planung der Datenqualität, Bewertung der Datenqualität, Verbesserung der Datenqualität und Validierung des Datenqualitätsprozesses) mit zugeordneten Aktivitäten und Ergebnissen.
Grundsätze	8
Link	ISO-Webseite: https://www.iso.org/standard/81093.html

Die derzeit noch im Entwurf vorliegende Norm ISO/IEC DIS 5259-5 referenziert die Normenreihe ISO/IEC 3850X, insbesondere die Normen ISO/IEC 38505-1 zur Data Governance und ISO/IEC 38507 zur KI-Governance. Im Rahmen der ISO/IEC 5259-Reihe steht sie in Verbindung mit der Managementebene, die von den beiden Normen ISO/IEC 5259-3 und ISO/IEC 5259-4 gebildet und dementsprechend häufig von der ISO/IEC 5259-5 referenziert werden.[27]

ISO/IEC DIS 5259-5

Titel	ISO/IEC DIS 5259-5 Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 5: Data quality governance framework
Aktuelle Version	Draft 2023
Organisation	ISO International Organization for Standardization IEC International Electrotechnical Commission
Status	Stage 50.20 Proof sent to secretariat or FDIS ballot initiated
Umfang	15 Seiten
Inhalt	Die ISO/IEC DIS 5259-5 beschreibt ein Governance-Framework für die Qualität von Daten für Data Analytics/ML. Die Norm fokussiert die Verantwortung der Leitungsorgane und beschreibt im Detail die Verantwortungsteilung zwischen diesen und dem untergeordneten Management, dem hierzu entsprechende Zuständigkeiten zu delegieren sind. Die Leitungsorgane müssen grundlegend die strategische Bedeutung der Datenqualität für Data Analytics/ML verstehen. Ihre darauf aufbauende Verantwortung erstreckt sich insbesondere auf die Formulierung einer Datenqualitätsstrategie, die das Erreichen der Unternehmensziele unterstützt, und ihre Umsetzung. Weiterhin ist durch die Leitungsorgane sicherzustellen, dass die Organisation über geeignete Fähigkeiten zum Risikomanagement verfügt. Mittels Richtlinien zur Datenqualität sind

[26] Vgl. *ISO/IEC 5259-4*, S. 5.
[27] Vgl. *ISO/IEC 5259-5*, S. 5.

	sowohl die Datenqualitätsziele zu erreichen als auch die Anforderungen der Stakeholder zu erfüllen. Um diesen Verantwortlichkeiten nachzukommen, haben die Leitungsorgane angemessene Überwachungsmechanismen zu etablieren.[28]
Grundsätze	4, 5, 7, 8, 9
Link	ISO-Webseite: https://www.iso.org/standard/81093.html

Die ISO/IEC 22989 ist als inhaltliche Basis für alle KI-Normen anzusehen, da sie die Begrifflichkeit festlegt und grundlegende Konzepte beschreibt. Die Norm wird von vielen anderen Normen referenziert, so dass sie auch aus Sicht der KI-Governance von grundlegender Bedeutung ist.

ISO/IEC 22989

Titel	ISO/IEC 22989 Information technology – Artificial intelligence – Artificial intelligence concepts and terminology
Aktuelle Version	First edition, 2022-07
Organisation	ISO International Organization for Standardization IEC International Electrotechnical Commission
Status	Stage 60.60 International Standard published
Umfang	60 Seiten
Inhalt	Diese Norm beinhaltet die wesentlichen Konzepte und Begriffe im Bereich der KI. Eine grundlegende Festlegung der KI-Governance wäre es, die in sich abgestimmte Begrifflichkeit der ISO/IEC 22989[29] und der weiteren KI-Normen zu übernehmen. Weiterhin bietet sich eine Orientierung an dem umfassenden Rollenmodell für die KI-Stakeholder[30] an. Das Lebenszyklusmodell für KI-Systeme[31] wird von anderen Normen referenziert. Es integriert insb. auch Aspekte der Governance, des Risikomanagements, der Sicherheit und des Datenschutzes. Ein weiteres wichtiges Modell der Norm bezieht sich auf das KI-Ökosystem.[32] Dieses bildet in sechs Ebenen den Technologiemix, aus dem sich ein KI-System zusammensetzt, ab. Die hierin enthaltenen Ausführungen zu den von ML-Systemen genutzten Daten[33] sind grundlegend für eine Data Governance.

[28] Vgl. *ISO/IEC 5259-5*, S. 8-12.
[29] Siehe *ISO/IEC 22989*, S. 1-16.
[30] Siehe *ebd.*, S. 32-35.
[31] Siehe *ebd.*, S. 35-40.
[32] Siehe *ebd.*, S. 43-50.
[33] Siehe *ebd.*, S. 46f.

Grundsätze	6, 8, 9
Link	ISO-Webseite: https://www.iso.org/standard/74296.html

Die ISO/IEC 23894:2023 wurde bereits in eine Europäische Norm (ISO/IEC EN 23894) überführt. Demgemäß wird sie derzeit vom DIN übernommen und liegt damit der E DIN EN ISO/IEC 23894 zugrunde.[34]

ISO/IEC 23894

Titel	ISO/IEC 23894 Information technology – Artificial intelligence – Guidance on risk management
Aktuelle Version	First edition, 2023-02
Organisation	ISO International Organization for Standardization IEC International Electrotechnical Commission
Status	Stage 60.60 International Standard published
Umfang	26 Seiten
Inhalt	s. E DIN EN ISO/IEC 23894
Grundsätze	4, 6, 9, 10,11
Link	ISO/IEC-Webseite: https://www.iso.org/standard/77304.html

Der Technische Report ISO/IEC TR 24368 vertieft die Thematik des ethisch vertretbaren Einsatzes von KI-Systemen. Damit ist er auch für die KI-Governance hinsichtlich einer ethischen Führung und der gesellschaftlichen Verantwortung relevant.

ISO/IEC TR 24368

Titel	ISO/IEC TR 24368 Information technology – Artificial Intelligence – Overview of ethical and societal concerns
Aktuelle Version	First edition, 2022-08
Organisation	ISO International Organization for Standardization IEC International Electrotechnical Commission
Status	Stage 60.60 International Standard published
Umfang	48 Seiten
Inhalt	Die ISO/IEC TR 24368 gibt einen Überblick über ethische und gesellschaftliche Themenstellungen im Zusammenhang mit der Entwicklung und dem Einsatz von KI-Systemen, z. B. Transparenz, Erklärbarkeit, Verantwortung, menschliche Kon-

[34] Siehe Abschnitt 2.1.

	trolle, Nachhaltigkeit, Gesetzestreue. Vor allem in den Überlegungen zur Entwicklung und Nutzung ethischer und sozialverträglicher KI werden zahlreiche Fragen gestellt, die als Checkpoints, insbesondere im Hinblick auf eine ethische Führung, genutzt werden können.[35] Mit Aspekten der Sicherheit und der Nachhaltigkeit werden die Beziehungen zwischen dem KI-System und den externen (technischen, sozialen, ökologischen etc.) Systemen der Organisation adressiert.
Grundsätze	7, 10, 11
Link	ISO-Webseite: https://www.iso.org/standard/78507.html

ISO/IEC 24668

Titel	ISO/IEC 24668 Information technology – Artificial intelligence – Process management framework for big data analytics
Aktuelle Version	First edition, 2022-11
Organisation	ISO International Organization for Standardization IEC International Electrotechnical Commission
Status	Stage 60.60 International Standard published
Umfang	50 Seiten
Inhalt	Die ISO/IEC 24668 richtet sich das Prozessmanagement im Bereich Big Data Analytics (BDA). Sie beschreibt ein Modell mit Prozesskategorien und Prozessen, darunter Stakeholder-Prozesse sowie auf Kultur, Kompetenz, Risiken, Technologie und Data Governance bezogene Prozesse.[36] Die Darstellung erfolgt systematisch anhand einer Tabellenstruktur. Jede Prozessdarstellung enthält eine ID-Nummer, eine Prozessbezeichnung, eine Kontextbeschreibung, das Prozessziel und Prozessergebnisse.[37] Für die verschiedenen Governance-Aspekte lassen sich so detaillierte Gestaltungshinweise entnehmen.
Grundsätze	6, 7, 8, 9
Link	ISO-Webseite: https://www.iso.org/standard/78368.html

Die ISO/IEC 38507 ist Teil der Normenreihe ISO/IEC 3850x. Insofern ist sie in Zusammenhang mit der ISO/IEC 38500 zu lesen.[38]

[35] Vgl. *ISO/IEC TR 24368*, S. 17-22.
[36] Vgl. *ISO/IEC 24668*, S. 4f.
[37] Vgl. *ebd.*, S. 6-14.
[38] Siehe Abschnitt 2.3.

ISO/IEC 38507

Titel	ISO/IEC 38507 Information technology – Governance of IT – Governance implications of the use of artificial intelligence by organizations
Aktuelle Version	First edition, 2022-04
Organisation	ISO International Organization for Standardization IEC International Electrotechnical Commission
Status	Stage 60.60 International Standard published
Umfang	28 Seiten
Inhalt	Die ISO/IEC 38507 behandelt die Governance-Auswirkungen der Nutzung von KI in Organisationen. Mit dem KI-Ökosystem und dem KI-Lebenszyklusmodell greift die Norm auf wesentliche Konzepte der ISO/IEC 22989 zurück.[39] Die Norm setzt sich grundlegend mit dem Nutzen, aber auch den Beschränkungen von KI-Systemen auseinander.[40] Für ein Governance-Modell in Bezug auf die Implikationen der KI-Nutzung greift die ISO/IEC 38507 auf der IT-Governance-Modell der ISO/IEC 38500[41] zurück. Die Verantwortung der Leitungsorgane und des Managements richtet sich auf die Etablierung von Überwachungsmechanismen, insbesondere Richtlinien, die die Verantwortlichkeit in Bezug auf den KI-Einsatz regeln. Die Richtlinien sollen die fünf Bereiche (1) Entscheidungsfindung, (2) Datennutzung, (3) Kultur und Werte, (4) Compliance und (5) Risiko umfassen.[42]
Grundsätze	2, 4, 5, 7, 8, 9
Link	ISO-Webseite: https://www.iso.org/standard/56641.html

Die ISO/IEC 42001 richtet sich auf ein KI-Managementsystem und bildet damit i. S. einer Schnittstelle zwischen Governance und Management eine wichtige Ergänzung zur ISO/IEC 38507. Die Norm basiert auf der „harmonisierten Struktur“ der ISO und gliedert sich damit in die Reihe der Managementsystemnormen (MSS – Management System Standard) ein. Sie beinhaltet Leitlinien und Anforderungen und ist damit – genauso wie z. B. die ISO/IEC 27001 – zertifizierbar. Insofern ist die ISO/IEC 42001 ein MSS vom Typ A.[43]

[39] Vgl. *ISO/IEC 38500*, S. 8f.
[40] Vgl. *ebd.*, S. 9-11.
[41] Dem Entstehungsdatum der Norm entsprechend bezieht sich die ISO/IEC 38507 auf die ISO/IEC 38500:2015 und nicht auf die aktuelle Version von 2024.
[42] Vgl. *ebd.*, S. 13-22.
[43] Vgl. *ISO 2024*. Nicht zertifizierbare MSS sind vom Typ B.

ISO/IEC 42001

Titel	ISO/IEC 42001 Information technology – Artificial intelligence – Management system
Aktuelle Version	First edition, 2023-12
Organisation	ISO International Organization for Standardization IEC International Electrotechnical Commission
Status	Stage 60.60 International Standard published
Umfang	52 Seiten
Inhalt	Die ISO/IEC 42001 enthält Leitlinien für und Anforderungen an die Einrichtung, Umsetzung, Aufrechterhaltung, Dokumentation und kontinuierliche Verbesserung eines KI-Managementsystems (KIMS). Grundlegend muss die Organisation den Kontext des KIMS verstehen. Hierzu gehört auch die Berücksichtigung der Interessen der Stakeholder.[44] Das Top-Management muss Führung und Commitment demonstrieren, insb. in Form einer KI-Richtlinie.[45] Die Planung des KIMS umfasst sowohl eine Risiko- als auch eine Folgenabschätzung des KI-Einsatzes. Zur Unterstützung des KMIS muss ein entsprechender Kompetenzaufbau erfolgen, der Betrieb des KIMS muss wiederum umfangreich Risikobewertungen und -behandlungen umfassen. Für die Leistungsmessung sollen interne Prüfprogramme entwickelt und durchgeführt werden und letztlich muss das Top-Management das KIMS einem Review unterziehen. Bei Abweichungen von Zielen und Vorgaben sind entsprechende Korrekturmaßnahmen zu ergreifen. [46] Zwei der vier Anhänge sind aus Sicht der Governance relevant: Der Anhang A enthält die für einen Typ A MSS typische Auflistung von Kontrollzielen und Maßnahmen.[47] Anhang B umfasst umfangreiche Implementierungsleitlinien für jede in Anhang A aufgelistete Maßnahme.[48] Hierbei wird auch die Beziehung zu Third-Party-Akteuren, insb. Kunden und Lieferanten, thematisiert.
Grundsätze	4, 5, 6, 7, 8, 9, 10, 11
Link	ISO-Webseite: https://www.iso.org/standard/81230.html

[44] Vgl. *ISO/IEC 42001*, S. 5f.
[45] Vgl. *ebd.*, S. 7f.
[46] Vgl. *ebd.*, S. 8-16.
[47] Vgl. *ebd.*, S. 17-20.
[48] Vgl. *ebd.*, S. 21-45.

Titel	ISO/IEC DIS 42005 Information technology – Artificial intelligence – AI system impact assessment
Aktuelle Version	Draft 2024
Organisation	ISO International Organization for Standardization IEC International Electrotechnical Commission
Status	Status 50.00 Final text received or FDIS registered for formal approval,
Umfang	36 Seiten
Inhalt	Die ISO/IEC DIS 42005 bietet Unterstützung für die Durchführung von Folgenabschätzungen von KI-Systemen für Personen, Gruppen und Einrichtungen, die von einem KI-System und seinen geplanten Anwendungen betroffen sein können. Es werden Hinweise gegeben, wann und wie derartige Folgeabschätzungen durchgeführt werden sollen. Weiterhin wird die Integration des Prozesses der Folgeabschätzung in das KI-Risikomanagement und das KI-Managementsystem behandelt.[49] Voraussetzung für die Folgeabschätzung ist eine Analyse der relevanten internen und externen Stakeholder.[50] Die Folgenabschätzung richtet sich auf Auswirkungen hinsichtlich Verantwortlichkeiten, Transparenz, Fairness und Diskriminierung, Datenschutz, Verlässlichkeit, Datensicherheit, Erklärbarkeit und ökologische Auswirkungen.[51]
Grundsätze	6, 7, 9, 10, 11
Link	ISO-Webseite: https://www.iso.org/standard/44545.html

2.3 Governance-relevante allgemeine Normen

Außer den KI-spezifischen Normen gibt es weitere relevante Normen, die sich entweder direkt auf Governance beziehen (insb. die ISO 37000 und die ISO/IEC 38500) oder die von den KI-spezifischen Normen referenziert werden. Letzteres gilt für die ISO 31000. Teilweise liegen diese Normen auch als DIN-Norm vor, so dass in dieser Gruppe insgesamt fünf Normen relevant sind.

[49] Nach *ISO/IEC DIS 42005*, S. 1.
[50] Vgl. *ebd.*, S. 12f.
[51] Vgl. *ebd.*, S. 13-16.

DIN ISO 31000

Titel	DIN ISO 31000 Risikomanagement – Leitlinien (ISO31000:2018)
Aktuelle Version	Auflage 1, 2018-10
Organisation	DIN Deutsches Institut für Normung e. V.
Status	Veröffentlicht
Umfang	24 Seiten
Inhalt	Die DIN ISO 31000 beinhaltet Leitlinien für den Umgang mit Risiken in einer Organisation auf Basis von Grundsätzen, eines Rahmenwerkes und eines Risikomanagementprozesses.[52] Die Grundsätze richten sich auf die Schaffung und den Schutz von Werten.[53] Das Rahmenwerk fokussiert Führung und Verpflichtung, insb. der Leitungs- und Aufsichtsorgane. Hierbei steht aus Sicht der Governance die Zuweisung von Befugnissen, Verantwortlichkeiten und Rechenschaftspflichten im Vordergrund. Der Risikomanagementprozess bildet den Kern der Norm und umfasst die Aktivitäten der Kommunikation und Konsultation, die Kontextanalyse, die Risikobeurteilung und -behandlung, die Überwachung bzw. Überprüfung des Prozesses und prozessbegleitend die Dokumentation und das Berichtswesen.[54]
Grundsätze	4, 5, 7, 9
Link	DIN-Webseite: https://www.dinmedia.de/de/norm/din-iso-31000/294266968

Jede Ausgestaltung einer Governance – gleich ob für das gesamte Unternehmen oder einzelne Funktionen – sollte die (DIN) ISO 37000 berücksichtigen. Die ISO/IEC 38500 verweist explizit auf die ISO 37000.

DIN ISO 37000

Titel	DIN ISO 37000 Anleitung für Governance von Organisationen (ISO 37000:2021)
Aktuelle Version	Auflage 1, 2024-08
Organisation	DIN Deutsches Institut für Normung e. V.
Status	Veröffentlicht
Umfang	51 Seiten
Inhalt	Die DIN ISO 37000 beinhaltet einen Leitfaden für die Gover-

[52] Nach *DIN ISO 31000,* S. 7.
[53] Vgl. *ebd.*, S. 9f.
[54] Vgl. *ebd.*, S. 16-23.

	nance von Organisationen. Die Norm richtet sich an die Leitungsorgane, das Top-Management und Stakeholder, „die an der Organisation und ihrer Governance beteiligt sind."[55] Insbesondere richten sich die Ausführungen grundlegend auf die Zusammensetzung, die Struktur und die benötigten Kompetenz des Leitungsorgans.[56] Den Kern der Norm bilden elf Governance-Grundsätze, die in einen primären Grundsatz, vier grundlegende Grundsätze und sechs unterstützende Grundsätze unterteilt sind. Der primäre Grundsatz richtet sich auf die Zweckverfolgung der Organisation. Er bildet den zentralen Angelpunkt für alle anderen Grundsätze. Diese sind im Kontext des primären Grundsatzes zu verstehen und zu befolgen. Die grundlegenden Grundsätze sind wesentlich für die Sicherstellung einer wirksamen IT-Governance. Sie betreffen die Wertschöpfung, die Strategie, die Aufsicht i. S. der Überwachungsverantwortung der Leitungsorgane und deren Rechenschaftspflicht. Die unterstützenden Grundsätze adressieren Governance-Verantwortlichkeiten, die aktuell für Organisationen relevant sind.[57] Hierbei handelt es sich um die Einbindung von Stakeholdern, die Führung, insb. in ethischer Hinsicht, Daten und Entscheidungen, die Risikobeherrschung, die gesellschaftliche Verantwortung der Organisation und ihre langfristige Existenzfähigkeit und Leistungserbringung. Jeder dieser Grundsätze beinhaltet zuerst eine Aussage zur Verantwortung des Leitungsorgans in Bezug auf den Grundsatz mit einer anschließenden Begründung. Daran schließen sich praktische Schlüsselaspekte der Grundsätze, die als Empfehlungen formuliert sind, an. Hierdurch ergibt sich eine Vielzahl von Hinweisen für die Ausgestaltung der Corporate Governance und funktions- oder themenspezifische Ausprägungen, wie die IT- oder KI-Governance.
Grundsätze	1 – 11
Link	DIN-Webseite: https://www.dinmedia.de/de/norm/din-iso-37000/380905283

Die ISO 31000 wurde zuletzt im Jahr 2023 einem Review unterzogen und im Ergebnis als weiterhin für gültig erklärt. Derzeit steht allerdings eine erneute Prüfung der Norm an.

[55] *DIN ISO 37000*, S. 11.
[56] Vgl. *ebd.*, S. 19f.
[57] Vgl. *ebd.*, S. 23ff.

ISO 31000

Titel	ISO 31000 Risk management – Guidelines
Aktuelle Version	First edition, 2021-09
Organisation	ISO International Organization for Standardization
Status	90.92 International Standard to be revised
Umfang	24 Seiten
Inhalt	s. DIN ISO 31000
Grundsätze	4, 5, 7, 9
Link	ISO-Webseite: https://www.iso.org/standard/65694.html

ISO 37000

Titel	ISO 37000 Governance of organizations – Guidance
Aktuelle Version	Edition 2, 2018-02
Organisation	ISO International Organization for Standardization
Status	Stage 60.60 International Standard published
Umfang	36 Seiten
Inhalt	s. DIN ISO 37000
Grundsätze	1 – 11
Link	ISO-Webseite: https://www.iso.org/standard/65036.html

Die ISO/IEC 38500 ist die grundlegende Norm der Normenreihe ISO/IEC 3850x. Sie liegt in einer aktuellen dritten Version aus dem Jahr 2024 vor.[58]

ISO 38500

Titel	ISO/IEC 38500 Information technology – Governance of IT for the organization
Aktuelle Version	Edition 3, 2024-02
Organisation	ISO International Organization for Standardization IEC International Electrotechnical Commission
Status	Stage 60.60 International Standard published
Umfang	21 Seiten
Inhalt	Die ISO/IEC 38500 orientiert sich in ihrem Governance-Verständnis grundlegend an der ISO 37000. Die Auswirkungen einer „guten IT-Governance“ zeigen sich unter Berücksichtigung des Organisationsumfelds und der Erwartungen der Stakeholder in einer effektiven Leistung, einer verantwor-

[58] Einen kompakten Überblick über die ISO/IEC 38500 gibt *Klotz 2024*.

	tungsvolle Leitung und der Förderung einer ethischen IT-Nutzung durch die Leitungsorgane.[59] Für jeden der aus der ISO 37000 übernommenen elf Governance-Grundsätze beschreibt die Norm die spezifischen Governance-Implikationen für die Nutzung von IT. Daran schließt sich die auf die IT-Nutzung bezogene Darstellung der Ergebnisse bzw. Auswirkungen an.[60] Zusätzlich zu den Governance-Grundsätzen beschreibt die Norm ein Framework für die IT-Governance. Dieses beinhaltet sechs für die Praxis der IT-Governance grundlegende Elemente: (1) Ausrichtung für die Nutzung der IT, (2) Identifizierung der aktuell und künftig erforderlichen digitalen Fähigkeiten, (3) Festlegung und Fortschreibung von IT-bezogenen Regelungen, (4) Delegation von Befugnissen und Verantwortlichkeiten für die Nutzung von IT, (5) Leistung der IT, (6) Rechenschaft.[61] Das Framework wird in ein Modell der IT-Governance integriert. Dieses betont die Unterscheidung zwischen IT-Governance und IT-Management. Die Governance-Ebene umfasst die vier übergeordneten Governance-Aufgaben Evaluieren, Steuern und Überwachen der Unternehmens-IT sowie Stakeholder-Einbindung.[62]
Grundsätze	1 – 11
Link	ISO-Webseite: https://www.iso.org/standard/81684.html

[59] Vgl. *ISO/IEC 38500*, S. 3f.
[60] Vgl. *ebd.*, S. 6-14.
[61] Vgl. *ebd.*, S. 17-20.
[62] Vgl. *ebd.*, S. 15f.

3 Standards für KI-Governance

Im Folgenden werden verschiedene Standards für die KI-Governance in derselben Beschreibungsstruktur dargestellt. Folgende vier Standards werden beschrieben:

- DIN SPEC 92001-3,
- IDW PS 861,
- IEEE Std 7010™-2020,
- NIST AI 100-1.

Die DIN SPEC 92001-3[63] wurde nach dem vom DIN definierten und überwachten PAS-Verfahren als „Publicly Available Specification“, d. h. durch Konsens der beteiligten Akteure (aus Wirtschaft, Verbänden und Wissenschaft), erstellt.

DIN SPEC 92001-3

Titel	DIN SPEC 92001-3 Artificial Intelligence - Life Cycle Processes and Quality Requirements - Part 3: Explainability
Aktuelle Version	Ausgabe 2023-08
Organisation	DIN Deutsches Institut für Normung e. V.
Status	Veröffentlicht
Umfang	24 Seiten
Inhalt	Diese Norm befasst sich mit der Erklärbarkeit von Künstlicher Intelligenz und definiert Ansätze zur Förderung von Transparenz während des gesamten Lebenszyklus von KI-Systemen. Aus Sicht der KI-Governance ist vor allem das Stakeholder-Modell relevant. Dieses wird ebenso wie das Modell zum Lebenszyklus von KI-Systemen von der ISO/IEC 22989 übernommen und aufeinander bezogen. Die Rollen der verschiedenen Stakeholder in den einzelnen Phasen des Lebenszyklus eines KI-System werden detailliert behandelt.[64] Auch die Ausführungen zur Erklärbarkeit werden auf die Informationsbedürfnisse der Stakeholder und ihre Interaktionen mit KI-Systemen bezogen.
Grundsätze	6
Link	DIN-Webseite: https://www.dinmedia.de/de/technische-regel/din-spec-92001-3/369799101

[63] Vgl. Abschnitt 1.2.
[64] Vgl. DIN SPEC 92001-3, S. 9ff.

Der Prüfungsstandard IDW PS 861 dient als Vorgabe für die durch Wirtschaftsprüfer vorgenommene Prüfung von KI-Systemen. Damit sind Unternehmen, die KI einsetzen, in keiner Weise an den Standard gebunden. Das Veranlassen von (freiwilligen) Prüfungen nach IDW PS 861 ist aber eine Möglichkeit, wie die Leitungsorgane eines Unternehmens ihrer Überwachungsverantwortung nachkommen können.

IDW PS 861

Titel	IDW PS 861 zur Prüfung von künstlicher Intelligenz
Aktuelle Version	1. Auflage
Organisation	IDW Institut der Wirtschaftsprüfer in Deutschland e. V.
Status	Veröffentlicht, Stand: 10.03.2023
Umfang	55 Seiten
Inhalt	Der IDW PS 861 befasst sich mit der Prüfung von KI-Systemen und legt die Anforderungen an die freiwillige Prüfung dieser Systeme, die von Wirtschaftsprüfern durchgeführt werden, fest. Der Standard dient als Leitfaden für die Durchführung von Prüfungen, die sicherstellen sollen, dass KI-Systeme zuverlässig, sicher und den regulatorischen Anforderungen entsprechend betrieben werden. Das Veranlassen von Prüfungen nach IDW PS 861 ist Teil der Überwachungsverantwortung der Leitungsorgane. Dementsprechend wird der Umfang dieser Verantwortung dargestellt.[65] Für die Ausgestaltung der KI-Governance geben sowohl die Anwendungshinweise (insb. durch die auf die Elemente des KI-Systems bezogenen Maßnahmen) als auch die Prüfungshandlungen im Rahmen der Angemessenheits- und Wirksamkeitsprüfungen eine Hilfestellung. Hier werden z. B. die KI-Strategie, der Schutz des KI-Systems oder der Umgang mit den für das KI-System erforderlichen Daten thematisiert.[66]
Grundsätze	3, 4, 5, 6, 8, 9, 11
Link	IDW-Webseite: https://shop.idw-verlag.de/IDW-PS-Pruefung-von-KI-Systemen-IDW-PS-861-03.2023/20685

Der Standard IEEE Std 7010™-2020 richtet sich auf die sozial-gesellschaftliche Dimension des KI-Einsatzes. Autonome und intelligente Systeme sollen auch das menschliche Wohlbefinden fördern oder zumindest nicht beeinträchtigen.

[65] IDW PS 861, Tz. 44f.
[66] Vgl. IDW PS 861, Abschnitt 6.2.1.2.

IEEE Std 7010™-2020

Titel	IEEE 7010-2020 IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being
Aktuelle Version	Ausgabe 2020
Organisation	IEEE Institute of Electrical and Electronic Engineers
Status	Veröffentlicht
Umfang	95 Seiten
Inhalt	Die IEEE 7010-2020 enthält eine Vorgehensweise zur Bewertung der Auswirkungen autonomer und intelligenter Systeme (A/IS) auf das menschliche Wohlbefinden. Die Norm zielt darauf ab, ein Rahmenwerk bereitzustellen, das die Messung und Verbesserung der positiven und negativen Auswirkungen von A/IS auf das menschliche Wohlbefinden über den gesamten Lebenszyklus eines Systems hinweg unterstützt. Es wird besonderer Wert gelegt auf die Einbindung von Stakeholdern, die Datenerhebung, die Analyse von Risiken für das Wohlbefinden und Indikatoren, die das Wohlbefinden in Bereichen wie psychologisches Wohlbefinden, Umwelt, Arbeit, Bildung und Gemeinschaft messen.
Grundsätze	6, 7, 8, 9, 10, 11
Link	IEEE-Webseite: https://standards.ieee.org/ieee/7010/7718/

Das AI Risk Management Framework der NIST gehört mittlerweile zu den meist verbreiteten Standards im Bereich der KI. Für die KI-Governance ist es insb. durch seine expliziten Ausführungen zur KI-Governance relevant.

NIST AI 100-1

Titel	NIST AI 100-1 Artificial Intelligence Risk Management Framework (AI RMF 1.0)
Aktuelle Version	Ausgabe 2023-01
Organisation	NIST National Institute of Standards and Technology U.S. Department of commerce
Status	Veröffentlicht
Umfang	43 Seiten
Inhalt	Das NIST AI RMF bietet einen umfassenden Rahmen für das Management von KI-Risiken. Die Norm beschreibt Methoden zur Identifizierung, Bewertung und Steuerung von Risiken, die durch KI-Systeme entstehen können. Zu den Hauptthemen gehören Risiken im Zusammenhang mit Datenschutz, Sicherheit, Fairness, Transparenz und gesellschaftlichen Auswir-

	kungen. Das Rahmenwerk ist in vier Hauptfunktionen unterteilt: (1) Govern, (2) Map, (3) Measure und (4) Manage.[67] Das Framework enthält ein eignes KI-Lebenszyklusmodell. Den einzelnen Lebenszyklusphasen werden detailliert Akteure als Stakeholder zugeordnet.[68] In einem der Anhänge werden spezifische KI-Risiken und die Bedeutung von Cyber- und Datenschutzrisiken für KI-Systeme behandelt.[69]
Grundsätze	6, 9, 10, 11
Link	Download von NIST-Webseite: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

[67] Siehe *NIST AI 100-1*, S. 20-33.
[68] Siehe *ebd.*, S. 11.
[69] Siehe *ebd.*, S. 38f.

4 Governance-Bezug der KI-Normen und -Standards

Die Tabellen 2 und 3 zeigen zusammenfassend, welche der Governance-Grundsätze nach der ISO 37000 von den in den Kapiteln 2 und 3 geschilderten KI-Normen und -Standards abgedeckt werden.

Nr.		Gültig	Entwurf	Grundsätze der Corporate Governance											Summe
				1. Zweck	2. Wertschöpfung	3. Strategie	4. Aufsicht	5. Rechenschaftspflicht	6. Einbindung von Anspruchsgruppen	7. Führung	8. Daten und Entscheidungen	9. Risikobeherrschung	10. Gesellschaft. Verantwortung	11. Langfristige Existenzfähigkeit und Leistung	
K I - N o r m e n															
1	E DIN EN ISO/IEC 23894		X				X		X			X	X	X	5
2	ISO/IEC 5259-1	X									X				1
3	ISO/IEC 5259-3	X									X	X			2
4	ISO/IEC 5259-4	X									X				1
5	ISO/IEC DIS 5259-5		X				X	X		X	X	X			5
6	ISO/IEC 22989	X							X		X	X			3
7	ISO/IEC 23894	X					X		X			X	X	X	5
8	ISO/IEC TR 24368	X								X			X	X	3
9	ISO/IEC 24668	X							X	X	X	X			4
10	ISO/IEC 38507	X			X		X	X		X	X	X			6
11	ISO/IEC 42001	X					X	X	X	X	X	X	X	X	8
12	ISO/IEC DIS 42005		X						X	X		X	X	X	5

Tabelle 2 Von KI-Normen abgedeckte Governance-Grundsätze nach ISO 37000

Nr.		Gültig	Entwurf	Grundsätze der Corporate Governance											Summe
				1. Zweck	2. Wertschöpfung	3. Strategie	4. Aufsicht	5. Rechenschaftspflicht	6. Einbindung von Anspruchsgruppen	7. Führung	8. Daten und Entscheidungen	9. Risikobeherrschung	10. Gesellschaft. Verantwortung	11. Langfristige Existenzfähigkeit und Leistung	
KI-Standards															
13	DIN SPEC 92001-3	X							X						1
14	IDW PS 861	X				X	X	X	X		X	X		X	7
15	IEEE Std 7010TM-2020	X							X	X	X	X	X	X	6
16	NIST AI 100-1	X							X			X	X	X	4
Allgemeine Governance-Normen															
17	DIN ISO 31000	X					X	X		X		X			4
18	DIN ISO 37000	X		X	X	X	X	X	X	X	X	X	X	X	11
19	ISO 31000	X					X	X		X		X			4
20	ISO 37000	X		X	X	X	X	X	X	X	X	X	X	X	11
21	ISO/IEC 38500	X		X	X	X	X	X	X	X	X	X	X	X	11
	Summe[70]			3	4	4	8	7	11	10	12	14	8	9	

Tabelle 3 Von KI-Standards und allgemeinen Governance-Normen abgedeckte Governance-Grundsätze nach ISO 37000

Inhaltliche Schwerpunkte

Die inhaltlichen Schwerpunkte in Bezug auf die Governance-Grundsätze der ISO 3700 bzw. der ISO/IEC 38500 liegen somit auf der Risikobeherrschung, den für KI-Systeme zu nutzenden Daten und den von den KI-Syste-

[70] Um Verzerrungen zu vermeiden, werden bei der Summierung Normen, die sowohl als ISO- bzw. ISO/IEC-Normen als auch als DIN-Normen vorliegen, nur einmal gezählt,

men vorbereiteten oder gefällten Entscheidungen sowie der Einbindung von Stakeholdern. Dieses Ergebnis ist vor dem Hintergrund der aus dem EU AI Act resultierenden aktuellen Fachdiskussion nicht überraschend. Vor allen die im EU AI Act vorgesehen hohen Bußgelder[71] lassen den Einsatz von KI-Systemen in den Fokus des Risikomanagements geraten. Viele der Risiken von KI-Systemen resultieren einerseits aus den Daten, mit denen die KI-Systeme trainiert werden, und andererseits aus den Daten, die das KI-System generiert und die damit zur Grundlage von Entscheidungen werden. Als weitere fokussierte Themen folgen die Aufsicht und Rechenschaftspflicht sowie die Führung. Diese Grundsätze umreißen die Verantwortung der Leitungsorgane und des Top-Managements beim Einsatz von KI-Systemen.

„Lücken“

Eher selten wird die Einflussnahme von KI auf den Unternehmenszweck sowie Fragen der Wertschöpfung und Strategie thematisiert. Am ehesten finden sich diesbezügliche Aussagen in den allgemeinen Governance-Normen. Dies ist insofern nicht überraschend, da sich der KI-Einsatz in seinem Nutzen und seinen Wertschöpfungspotenzialen nicht grundlegend vom IT-Einsatz allgemein unterscheidet.

Gegenüberstellung

Dieses Ergebnis wird in Tabelle 3 den Ergebnissen einer Literaturstudie gegenübergestellt. Diese hatte explizit das Ziel, „die Handlungsbereiche einer KI-Governance als Teil einer IT- bzw. Corporate Governance, diesbezügliche Schwerpunkte, aber auch Lücken“ aufzuzeigen.[72] In dieser Tabelle sind die Häufigkeiten der Adressierung der Governance-Grundsätze nach der ISO 37000 bzw. der ISO/IEC 38500 im Vergleich dargestellt. Rang 1 nimmt derjenige Grundsatz ein, der am häufigsten von den in der Literaturstudie analysierten wissenschaftlichen Aufsätzen und Fachartikeln bzw. den in diesem Arbeitspapier beschriebenen Normen und Standards adressiert wurde. Dementsprechend nimmt der von den verschiedenen Texten am wenigsten adressierte Governance-Grundsatz den letzten Rang 11 ein.

Übereinstimmungen

An Gemeinsamkeiten fällt auf, dass der letzte Rang vom Governance-Grundsatz „Zweck“ eingenommen wird. Trotz des „Hype“ um das Thema „Künstliche Intelligence“ scheint die disruptive Wirkung von KI auf den Unternehmenszweck weder in der Praxis noch in der Forschung angekommen zu sein. Dies dürfte sich in naher Zukunft ändern. Ebenso stimmen die

[71] Nach Art. 99 EU AI Act können Verstöße mit Geldbußen in Höhe von bis zu 35 Mio. EUR bzw. 7 % des Jahresumsatzes eines Unternehmens geahndet werden.
[72] *Klotz et al. 2024*, S. 1595.

Häufigkeiten hinsichtlich der Risikobeherrschung (fast) überein. Dieses Thema wird somit einhellig von den Aufsätzen einerseits und den Normen bzw. Standards andererseits in den Vordergrund gestellt. Ähnliche Übereinstimmungen, was eine relativ höhere Häufigkeit anbelangt, liegen bei der Einbindung von KI-Stakeholdern und der Führung in Bezug auf den KI-Einsatz vor. Ähnlich häufig, allerdings „im Mittelfeld" liegend, ist die gesellschaftliche Verantwortung Gegenstand der Aufsätze, Fachartikel, Normen und Standards. Dagegen wird der Grundsatz der Strategie übereinstimmend ähnlich selten thematisiert.

Tabelle 4
Gegenüberstellung Arbeitspapier und Literaturstudie

	1. Zweck	2. Wertschöpfung	3. Strategie	4. Aufsicht	5. Rechenschaftspflicht	6. Einbindung von Anspruchsgruppen	7. Führung	8. Daten und Entscheidungen	9. Risikobeherrschung	10. Gesellschaft. Verantwortung	11. Langfristige Existenzfähigkeit und Leistung
Arbeitspapier	11	9	9	6	8	3	4	2	1	6	5
Literaturstudie	11	1	8	2	2	6	2	6	2	8	10
Differenz	0	8	1	4	6	3	2	4	1	2	5

Differenzen

Mit Blick auf die Differenzen in Bezug auf die Rangpositionen bestehen größere Unterschiede bei den Grundsätzen der Wertschöpfung, der Rechenschaftspflicht sowie der langfristige Existenzfähigkeit und Leistung. Insofern stellt die gleichzeitige Berücksichtigung der Erkenntnisse aus wissenschaftlichen Aufsätzen und Fachartikel einerseits, Normen und Standards andererseits einen recht ausgewogenen Fundus an Konzepten, Modellen, Leitlinien und Empfehlungen für die Ausgestaltung der KI-Governance im Unternehmen dar.

Governance-Schwerpunkte

Die Tabellen 2 und 3 ermöglichen es zudem, ausgehend von einem definierten Governance-Grundsatz die hierfür relevanten KI-Normen und -Standards zu

ermitteln und somit für eine diesbezügliche Ausgestaltung der KI-Governance gezielt auf diese Normen und Standards zuzugreifen. Stehen z. B. Fragen der Rechenschaft in Bezug auf den KI-Einsatz im Mittelpunkt, sollten hierfür zuerst die Normen ISO/IEC DIS 5259-5, ISO/IEC 38507, ISO/IEC 42001 und der IDW PS 861 herangezogen werden.

5 Verzeichnis der KI-Normen und Standards

Tabelle 5
Verzeichnis der KI-Normen

Nr.	Normen	Jahr
	DIN-Normen	
1	E DIN EN ISO/IEC 23894 Informationstechnik – Künstliche Intelligenz – Leitlinien für Risikomanagement (ISO/IEC 23894:2023)	2023
2	DIN ISO 31000 Risikomanagement – Leitlinien (ISO 31000:2018)	2018
3	DIN ISO 37000 Anleitung für Governance von Organisationen (ISO 37000:2021)	2024
	ISO-Normen	
4	ISO 31000 Risk management – Guidelines	2018
5	ISO 37000 Governance of organizations – Guidance	2021
	ISO/IEC-Normen	
6	ISO/IEC 5259-1 Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 1: Overview, terminology, and examples	2024
7	ISO/IEC 5259-3 Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 3: Data quality management requirements and guidelines	2024
8	ISO/IEC 5259-4 Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 4: Data quality process framework	2024
9	ISO/IEC DIS 5259-5 Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 5: Data quality governance framework	2024
10	ISO/IEC 22989 Information technology – Artificial intelligence – Artificial intelligence concepts and terminology	2022
11	ISO/IEC 23894 Information technology – Artificial intelligence – Guidance on risk management	2023
12	ISO/IEC TR 24368 Information technology – Artificial Intelligence – Overview of ethical and societal concerns	2022
13	ISO/IEC 24668 Information technology – Artificial intelligence – Process management framework for big data analytics	2022
14	ISO/IEC 38500 Information technology – Governance of IT for the organization	2024
15	ISO/IEC 38507 Information technology – Governance of IT – Governance implications of the use of artificial intelligence by organizations	2022
16	ISO/IEC 42001 Information technology – Artificial intelligence – Management system	2023

17	ISO/IEC DIS 42005 Information technology – Artificial intelligence – AI system impact assessment	2024

Tabelle 6
Verzeichnis der KI-Standards

Nr.	Standards	Jahr
1	DIN SPEC 92001-3 Artificial Intelligence – Life Cycle Processes and Quality Requirements – Part 3: Explainability	2022
2	IDW PS 861 zur Prüfung von künstlicher Intelligenz	2023
3	IEEE 7010-2020 IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being	2020
4	NIST AI 100-1 Artificial Intelligence Risk Management Framework (AI RMF 1.0)	2023

Zeitliche Verteilung

Die Verteilung in Bezug auf die Veröffentlichung der Normen und Standards zeigt die Aktualität und Dynamik der Thematik, s. Abb. 3.

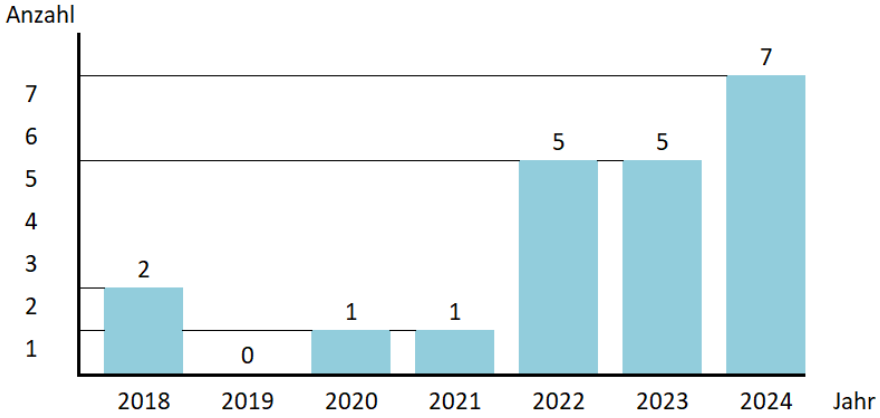

Abbildung 3
Zeitliche Verteilung der Normen und Standards

17 der 21 Normen und Standards stammen aus den Jahren 2023 und 2024. Dies ist mit den Programmen der KI-Normungs- und Standardisierungorganisationen zu erklären. So realisiert z. B. das DIN derzeit ein Projektprogramm zur Umsetzung der „Deutschen Normungsroadmap für Künstliche Intelligenz“. Gemeinsam mit Partnern aus Industrie, Wissenschaft und Verwaltung führt das DIN verschiedene Umsetzungsprojekte durch. Aus diesen Projekten wird konkreter Normungs- und Standardisierungsbedarf abgeleitet und in Normen und Standards umgesetzt.[73] Auch dies ist ein Grund dafür, dass kurzfristig mit weiteren, auch für die KI-Governance relevanten Normen zu rechnen ist.

[73] Siehe S. *DIN 2024b*.

Quellenangaben

DIN EN 45020
DIN EN 45020:2007-03 – Normung und damit zusammenhängende Tätigkeiten – Allgemeine Begriffe (ISO/IEC Guide 2:2004), DIN Deutsches Institut für Normung e. V. 2007

DIN 2024a
DIN DIN Deutsches Institut für Normung e. V. (Hg.): DIN SPEC; https://www.din.de/de/forschung-und-innovation/din-spec (letzter Zugriff am 06.11.2024)

DIN 2024b
DIN DIN Deutsches Institut für Normung e. V. (Hg.): Projekte zu KI und Normung, https://www.din.de/de/forschung-und-innovation/themen/kuenstliche-intelligenz/projekte-zu-ki-und-normung (letzter Zugriff am 06.11.2024)

IEC 2024a
International Electrotechnical Commission (IEC) (Hg.): Technical report (TR); https://www.iec.ch/publications/technical-reports (letzter Zugriff am 06.11.2024)

IEC 2024b
International Electrotechnical Commission (IEC) (Hg.): Technical specification (TS) and publicly available specification (PAS); https://www.iec.ch/publications/specifications (letzter Zugriff am 06.11.2024)

ISO 2024
International Organization for Standardization (ISO) (Hg.): Management System Standards list; https://www.iso.org/management-system-standards-list.html (letzter Zugriff am 06.11.2024)

Klotz 2013
Klotz, Michael: Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 2: Normen. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, 2013 (SIMAT AP, 5 (2013), 24), online verfügbar unter: https://www.econstor.eu/dspace/bitstream/10419/88419/1/773961380.pdf (letzter Zugriff am 06.11.2024)

Klotz 2020
Klotz, Michael: IT-Compliance. In: Ernst Tiemeyer (Hg.): Handbuch IT-Management – Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 7. Auflage, München: Hanser 2020, S. 841-884

Klotz 2024
Klotz, Michael: IT-Governance genormt – die neue ISO/IEC 38500 (revolutions). In: IT-Governance, Jg. 18 (2024), Nr. 39, S. 19-24

Klotz et al. 2024
Klotz, Michael; Adam, Waldemar; Noack-Sandring, Lukas; Schueschke, Niklas: Literaturstudie zu den Handlungsbereichen einer Governance für den Einsatz von KI-Systemen im Unternehmen. INFORMATIK 2024, IT-Governance und Strategisches Informationsmanagement (ITG-SIM), Wiesbaden. 24.-26. September 2024, Gesellschaft für Informatik e.V., Bonn, S. 1597-1609, https://doi.org/10.18420/inf2024_139

Mäntymäki et al. 2022
Mäntymäki, Matti; Minkkinen, Matti; Birkstedt, Teemu; Viljanen, Mika: Defining organizational AI governance. AI and Ethics, Jg. 2 (2022), Nr. 4, S. 603–609

Rowan et al. 2024
Rowan, Jim; Ammanath, Beena; Perricos, Costi; Sniderman, Brenna; Jarvis, David: Now decides next: Moving from potential to performance. Deloitte´s State of Generative AI in the Enterprise, Quarter three report, Deloitte Development LLC, August 2024,), online verfügbar unter: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-state-of-gen-ai-q3.pdf (letzter Zugriff am 06.11.2024)

VOI 2008
VOI Verband Organisations- und Informationssysteme e. V. (Hg.): Standards und Normen im Umfeld ECM – Leitfaden für organisatorische und technische Anforderungen, Berlin: VOI 2008

Verzeichnis der SIMAT-Arbeitspapiere

AP	Datum	Autor	Titel
01-09-001	01.2009	M. Klotz	Datenschutz in KMU – Lehren für die IT-Compliance
01-09-002	02.2009	M. Klotz	Von der Informationsgesellschaft zum Informationsarbeiter
01-09-003	09.2009	L. Ramin / M. Klotz	Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT
01-09-004	10.2009	S. Kubisch	Corporate Governance gemäß BilMoG und SOX
02-10-005	06.2010	M. Klotz	PMBOK-Compliance der Projektmanagement- Software Projektron BCS
02-10-006	07.2010	A. Woltering	Kontinuierliche Verbesserung von Desktop- Services mittels Benchmarking
02-10-007	09.2010	M. Klotz	Grundlagen der Projekt-Compliance
02-10-008	11.2010	I. Karminski	Grundlagen und aktuelle Entwicklungen der digitalen Betriebsprüfung
02-10-009	12.2010	D. Engel/ N. Zdrowomyslaw	Benchmarking-Studie Stralsund 2010
03-11-010	02.2011	E. Tiemeyer	Kennzahlengestütztes IT-Projektcontrolling – Projekt-Score-cards einführen und erfolgreich nutzen
03-11-011	05.2011	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Über-sicht, Teil 1: Rechtliche Regelwerke
03-11-012	06.2011	M. Klotz	Konzeption des persönlichen Informationsmanagements
03-11-013	08.2011	H. Auerbach/ N. Zdrowomyslaw	9. STeP-Kongress „Region gestalten! Gesundheitswirtschaft und Zukunftsmanagement“
03-11-014	08.2011	M. Klotz	Rollen der Information im Unternehmen
03-11-015	08.2011	Ahlfeldt	eGuides in kulturellen Einrichtungen – deutsch-sprachige Museums-Apps
03-11-016	11.2011	S. J. Saatmann / I. Sulk / M. Klotz	Studie zu gewerblichen Strompreisen in Mecklenburg-Vor-pommern – Strom als Wettbewerbsfaktor und Gegenstand der Standortvermarktung
04-12-017	02.2012	M. Klotz / I. Sulk / E. Wieck	GDPdU-Konformität von Projektmanagementsoftware – Exemplarische Konzeption und Umsetzung
04-12-018	07.2012	M. Horn-Vahlefeld	Projektdesign als organisatorischer Rahmen des Projekt-managements
04-12-019	08.2012	M. Klotz / J. Kriegel	ITIL und Datenschutz – Überlegungen für eine Integration des Datenschutzes in die IT-Prozesse nach ITIL
04-12-020	09.2012	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Über-sicht, Teil 1: Rechtliche Regelwerke, 2. Aufl.
04-12-021	10.2012	I. Sulk / M. Klotz	Einsatz von eGuides auf der Marienburg in Malbork (Polen) – Erhebung und Analyse einer Best Practice
04-12-022	12.2012	Witty, M. / C. Kliebisch	Die Versicherungsbranche unter FATCA
05-13-023	01.2013	S. J. Saatmann	The price-link in the natural gas market – The development of the oil price-link and alternative price mechanisms
05-13-024	02.2013	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 2: Normen

06-14-025	01.2014	M. Klotz	IT-Compliance nach COBIT® – Gegenüberstellung von COBIT® 4.0 und COBIT® 5
06-14-026	04.2014	L. von Blumröder	Projektpriorisierung im Rahmen eines ganzheitlichen Projektportfoliomanagements
06-14-027	06.2014	S. Press	Automatisierte Kontrollen in der Beschaffung – Exemplarische Konzeption und Umsetzung
06-14-028	07.2014	M. Klotz	IT-Compliance – Begrifflichkeit und Grundlagen
07-15-029	09.2015	M. Klotz	Projektmanagement-Normen und -Standards
08-16-030	08.2016	M. Klotz	ISO/IEC 3850x – Die Normenreihe zur IT-Governance
09-17-031	09.2017	S. Marx	Project Management Practice in Interreg Projects – Reflective Analysis and Recommendations
09-17-032	11.2017	S. Marx	Knowledge Management in Interreg Cross-Border Cooperation – a Project Perspective
10-18-033	11.2018	M. Klotz / S. Marx	Projektmanagement-Normen und -Standards, 2. Auflage
11-19-034	08.2019	M. Klotz	IT-Compliance nach COBIT® 2019
11-19-035	09.2019	I. Sulk / P. Hagen / M. Klotz	Kontrollanforderungen an ein ERP/Cloud-System und Umsetzung in automatisierte Kontrollen
12-20-036	03.2020	S. Marx / M. Klotz	Earned-Value-Analyse – Einführung und Beispiele
12-20-037	04.2020	M. Kenter / C. Bülow / M. Weber / L. Kennes	Lebensqualität in Vorpommern-Rügen – Ein Vergleich mit ausgewählten Metropolen und Vergleichsstädten Deutschlands
12-20-038	05.2020	S. Marx / M. Klotz	Hackathons in Museums – Recommendations from an International Event Series
13-21-039	03.2021	M. Naybzadeh	Standards und Zertifizierungen für Cloud-Services
13-21-040	11.2021	M. Kenter / C. Bülow / L. Kennes	Die Unternehmenslandschaft in Mecklenburg-Vorpommern im Vergleich zu anderen Regionen Deutschlands – Eine empirische Studie repräsentativer Landkreise aus allen 16 Bundesländern Deutschlands in Bezug auf ausgewählte Kennzahlen in Verbindung mit Unternehmen
14-22-041	07.2022	M. Klotz / S. Marx	Projektmanagement-Normen und -Standards, 3. Auflage
16-24-042	08.2024	M. Klotz	Persönliches Informationsmanagement – Grundlagen einer effektiven Informationsnutzung
16-24-043	11.2024	M. Klotz / L.-E. Pissors	KI-Normen und -Standards – Unterstützung für die Gestaltung der KI-Governance