KI im Unternehmen einsetzen: Einfach, effizient und gesetzeskonform dank ISO 42001

IHK Webinar, 21.1.2025

Quelle: Erzeugt mit Dall-E

Referent Klaus Kilvinger

- Gründer & Geschäftsführender Gesellschafter der Opexa Advisory GmbH
- Besondere Expertise im Bereich der Informationssicherheit und in zertifizierten Managementsystemen (ISO 27001, TISAX®, B3S)
- Sprecher zur Informationssicherheitsmanagement auf den Veranstaltungen der DGQ, IHK München/Oberbayern, BVMW, KnowBe4 Con London, PITS Berlin, Management Circle Frankfurt (u.a.)
- Langjährige Expertise im Bereich IT- Serviceindustrie und Software-Qualitätssicherung mit umfangreicher Führungserfahrung
- www.opexaadvisory.de
- Klaus.kilvinger@opexa.de

Opexa Leistungen

- Fokus zu 100 % auf **Informationssicherheitsmanagement**
- **Umfassende Begleitung** bei der Implementierung eines ISMS (**ISO 27001, TISAX®, B3S), DORA** & **NIS2**
  - Erläuterung der Anforderungen und „Übersetzung“ des Inhaltes, GAP-Analysen
  - Vorbereitung auf Audits und Auditbegleitung und Support bei Beseitigung der Abweichungen
- Consulting zum **Business Continuity Management** (**ISO 22301, BSI 200-4**)
- Seminare zu **ISO 27001:2022, TISAX® V6, DORA, NIS2**
- Informationssicherheitsbeauftragter als Service: **ISB / CISO as a Service „CISO a la carte“**
- Support der Einführung von **ISMS Lösungen**
- **Eigene Lösung „EnterpriseOS“ für IMS (ISMS, QMS etc.)** mit Integration verschiedener bereits etablierter Managementsysteme (z. B. ISO 900l, 27001, 14001) oder neuer Inhalte (ISO 42001) in bestehende Systeme

Fachpublikationen zu KI

QZ Magazin 07/24

Digital Business Cloud 9/24

Buch in 2024 erschienen

Praktische Anwendung KI

DORA im Finanzbereich

Verträge von Drittdienstleistern sind umzustellen auf DORA – Anforderungen

Umsetzung:

- Analyse von **mehreren 100** Dokumenten
- Erkennen von Abweichungen
- Vorschlag für Vertragsergänzungen
- Check durch Experten
- Dokumentation für BaFin
- Aufbau Informationsregister

DORA-Vertragsprüfung | Opexa Advisory

Quelle: DALL-E

Ausbildungsinitiative

Unsere Experten entwickeln Seminare und führen diese mit *namhaften und ausgewählten Partnern* durch.

Aktuelle Formate und Themen:

- ISO 27001:2022 Update
- ISO 27001:2022 Implementer mit Personenzertifizierung
- TISAX® VDA ISA Version 6 - Update
- TISAX® Training - Foundation Level (Seit 2018! First Mover: Weltweit erstes TISAX Training)
- Informationssicherheitsbeauftragter Automotive (ISB-A) mit Personenzertifizierung
- KI – Implementer: Seminar mit Personenzertifizierung (Basis ISO 42001, AI –Act) ab 04/2025

Agenda

- KI-Verordnung und die Anforderungen: Kurzer Überblick
- Managementsysteme: Kurze Beschreibung und konkreter Nutzen im Unternehmen
- KI-Managementsystem-Norm ISO 42001: Inhalte und Struktur
- Umsetzung der KI-Verordnung mit Hilfe der ISO 42001: Wo hilft die Norm weiter?
  - > Die Rolle des Qualitätsmanagements
  - > Die Rolle des Datenschutzes und der Informationssicherheit
  - > Umsetzungsoptionen mit Hilfe von Dokumenten und/oder Softwarelösungen
- Integrative Vorteile bei Kombination von Normen
- Warum die Norm nutzen?
- Q&A

Agenda

- **KI-Verordnung und die Anforderungen: Kurzer Überblick**
- Managementsysteme: Kurze Beschreibung und konkreter Nutzen im Unternehmen
- KI-Managementsystem-Norm ISO 42001: Inhalte und Struktur
- Umsetzung der KI-Verordnung mit Hilfe der ISO 42001: Wo hilft die Norm weiter?
  - > Die Rolle des Qualitätsmanagements
  - > Die Rolle des Datenschutzes und der Informationssicherheit
  - > Umsetzungsoptionen mit Hilfe von Dokumenten und/oder Softwarelösungen
- Integrative Vorteile bei Kombination von Normen
- Warum die Norm nutzen?
- Q&A

Fragen

- Setzen Sie heute schon KI ein und was machen Sie damit?
- Haben Sie für Ihr Unternehmen und das Umfeld angemessene Richtlinien für die Nutzung der KI entwickelt, abgestimmt und dokumentiert?
- Haben Sie die Richtlinie mit dem ISB/CISO und Datenschutz abgestimmt?
- Ist sie in den relevanten Abteilungen in die Prozesse und Methoden implementiert?
- Haben Sie diese den Mitarbeitern nachweislich vermittelt und ist der generelle Wissensaufbau zu KI im Unternehmen angeschoben?
- Haben Sie dies auch für Ihre Kunden und dem Markt kenntlich gemacht und den Vorteil von KI kommuniziert?

Ki-Verordnung

- Am 12. Juli 2024 wurde die KI-**Verordnung** im Amtsblatt der EU veröffentlicht.
- Es erfolgt keine Übertragung in das nationale Recht, sie ist sofort in der ganzen EU gültig.
- Sie tritt 20 Tage nach ihrer Veröffentlichung am **1. August 2024** in Kraft.
- Es gelten verschiedene Regelungen zu Übergangszeiten für Teile der Verordnung.
- Risikobasierter Ansatz

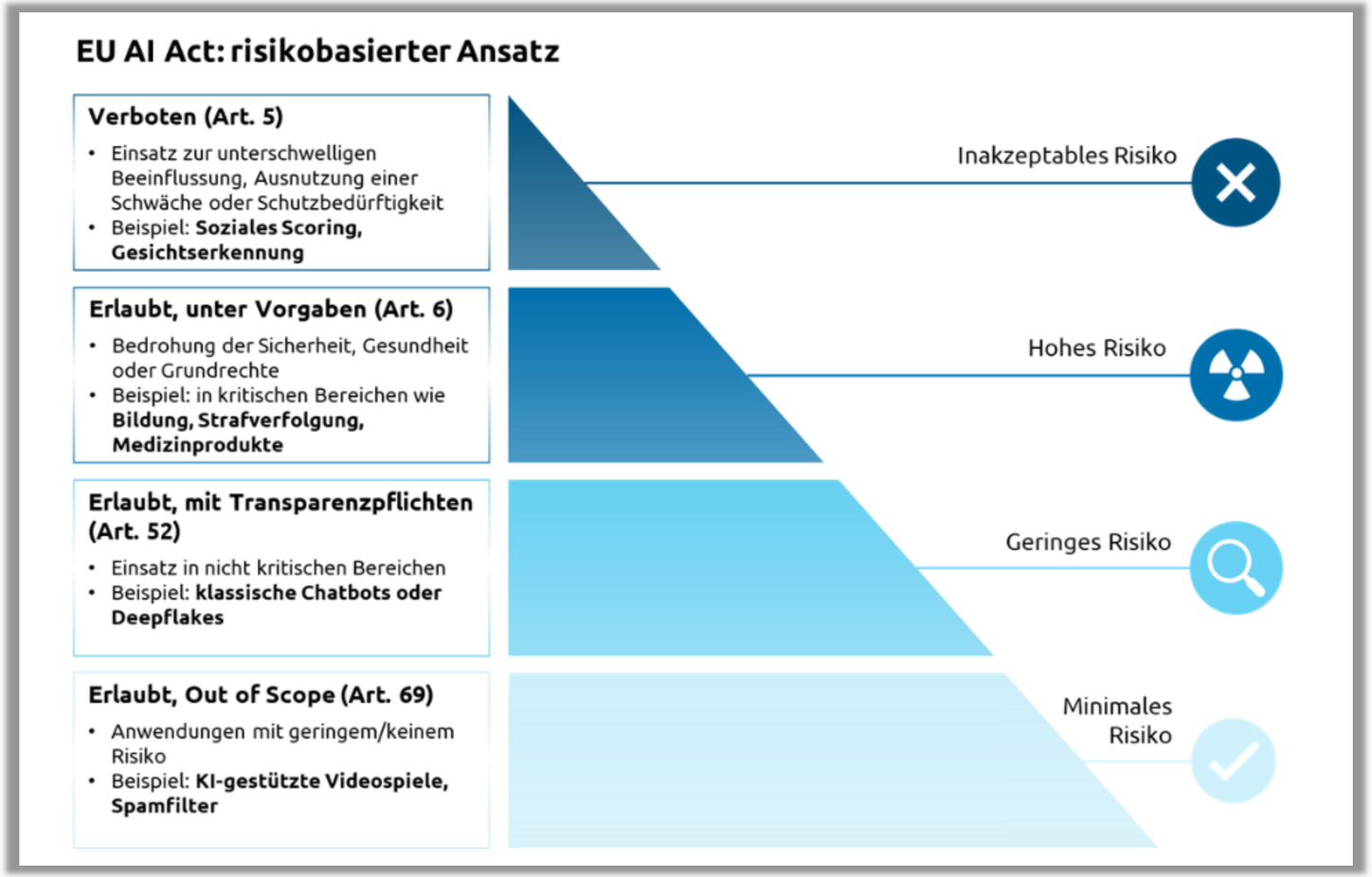
Risikostufen

Unakzeptable Systeme sind ab 2. Februar 2025 verboten

Hochrisikoanwendungen
- Ab 2. August 2026 reguliert
- Sind einer Konformitätsbewertung zu unterziehen
- Anbieter müssen Qualitäts- und Risikomanagementsysteme einführen

Wissen Sie schon, was sie einsetzen?

Ist das Risiko schon bekannt und die richtige Risikogruppe gefunden?



Quelle: Capgemini

Hochrisiko-KI

- Systeme, die biometrische Daten verarbeiten
- Systeme, die in der kritischen Infrastruktur zum Einsatz kommen
- Bewertung von Schülern
- Zugangsprüfungen zur Universität
- Bewerberauswahl, Beförderungen und Kündigungen im Arbeitsleben
- Anspruch auf Sozialhilfe
- Prüfung der Kreditwürdigkeit
- Risikobewertung und Preisbildung bei Lebens- und Krankenversicherungen
- Prognose von Rückfälligkeit bei Straftaten
- Einflussmöglichkeit auf Wahlen
- Einschätzung von Sicherheitsrisikos oder eines ausgehenden Gesundheitsrisikos von Einzelnen bei Migration, Asyl sowie Grenzkontrolle.

Pflichtenkatalog für Hochrisiko-KI

Artikel 9
Risikomanagementsystem

(1) Für Hochrisiko-KI-Systeme wird ein Risikomanagementsystem eingerichtet, angewandt, dokumentiert und aufrechterhalten.

(2) Das Risikomanagementsystem versteht sich als ein kontinuierlicher iterativer Prozess während des gesamten Lebenszyklus eines KI-Systems, der eine regelmäßige systematische Aktualisierung erfordert. Es umfasst folgende Schritte:

a) Ermittlung und Analyse der bekannten und vorhersehbaren Risiken, die von jedem Hochrisiko-KI-System ausgehen;

b) Abschätzung und Bewertung der Risiken, die entstehen können, wenn das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird;

c) Bewertung anderer möglicherweise auftretender Risiken auf der Grundlage der Auswertung der Daten aus dem in Artikel 61 genannten System zur Beobachtung nach dem Inverkehrbringen;

d) Ergreifung geeigneter Risikomanagementmaßnahmen gemäß den Bestimmungen der folgenden Absätze.

(3) Bei den in Absatz 2 Buchstabe d genannten Risikomanagementmaßnahmen werden die Auswirkungen und möglichen Wechselwirkungen, die sich aus der kombinierten Anwendung der Anforderungen dieses Kapitels 2 ergeben, gebührend berücksichtigt. Diese Maßnahmen tragen dem allgemein anerkannten Stand der Technik Rechnung, wie er auch in einschlägigen harmonisierten Normen oder gemeinsamen Spezifikationen zum Ausdruck kommt.

(4) Die in Absatz 2 Buchstabe d genannten Risikomanagementmaßnahmen werden so gestaltet, dass jedes mit einer bestimmten Gefahr verbundene Restrisiko sowie das Gesamtrestrisiko der Hochrisiko-KI-Systeme als vertretbar beurteilt werden kann, sofern das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird. Diese Restrisiken müssen den Nutzern mitgeteilt werden.

Bei der Festlegung der am besten geeigneten Risikomanagementmaßnahmen ist Folgendes sicherzustellen:

a) weitestmögliche Beseitigung oder Verringerung der Risiken durch eine geeignete Konzeption und Entwicklung,

b) gegebenenfalls Anwendung angemessener Minderungs- und Kontrollmaßnahmen im Hinblick auf nicht auszuschließende Risiken;

c) Bereitstellung angemessener Informationen gemäß Artikel 13, insbesondere bezüglich der in Absatz 2 Buchstabe b des vorliegenden Artikels genannten Risiken, und gegebenenfalls entsprechende Schulung der Nutzer.

Bei der Beseitigung oder Verringerung der Risiken im Zusammenhang mit der Verwendung des Hochrisiko-KI-Systems werden die technischen Kenntnisse, die Erfahrungen und der Bildungsstand, die vom Nutzer erwarten werden können, sowie das Umfeld, in dem das System eingesetzt werden soll, gebührend berücksichtigt.

(5) Hochrisiko-KI-Systeme müssen getestet werden, um die am besten geeigneten Risikomanagementmaßnahmen zu ermitteln. Durch das Testen wird sichergestellt, dass Hochrisiko-KI-Systeme stets bestimmungsgemäß funktionieren und die Anforderungen dieses Kapitels erfüllen.

(6) Die Testverfahren müssen geeignet sein, die Zweckbestimmung des KI-Systems zu erfüllen, und brauchen nicht über das hierfür erforderliche Maß hinauszugehen.

Agenda

- KI-Verordnung und die Anforderungen: Kurzer Überblick
- **Managementsysteme: Kurze Beschreibung und konkreter Nutzen im Unternehmen**
- KI-Managementsystem-Norm ISO 42001: Inhalte und Struktur
- Umsetzung der KI-Verordnung mit Hilfe der ISO 42001: Wo hilft die Norm weiter?
  - > Die Rolle des Qualitätsmanagements
  - > Die Rolle des Datenschutzes und der Informationssicherheit
  - > Umsetzungsoptionen mit Hilfe von Dokumenten und/oder Softwarelösungen
- Integrative Vorteile bei Kombination von Normen
- Warum die Norm nutzen?
- Q&A

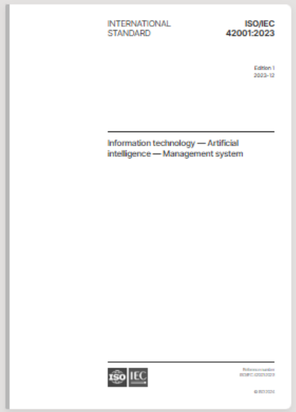
Managementsysteme

- Managementsysteme bündeln Tätigkeiten, Instrumente und Methoden der Unternehmensführung.
- Managementsysteme sind wirksame Instrumente, auf die Unternehmen im Rahmen ihrer betrieblichen Organisation zurückgreifen können.
- Sie ermöglichen es Unternehmen, komplexe bereichsübergreifende Führungsaufgaben zu bewältigen.
- Durch klare Rollen, Regeln und Abläufe werden Themen wie Qualität, Nachhaltigkeit, Innovation, Wissen und Arbeitssicherheit strukturiert gemanagt.
- Managementsysteme können als ein systematisches, gezieltes und geplantes Herangehen an die Umsetzung der Unternehmenspolitik und von Unternehmenszielen bezeichnet werden.
- Beispiele: ISO 9001, ISO 45001, ISO 14001, ISO 27001

Agenda

- KI-Verordnung und die Anforderungen: Kurzer Überblick
- Managementsysteme: Kurze Beschreibung und konkreter Nutzen im Unternehmen
- **KI-Managementsystem-Norm ISO 42001: Inhalte und Struktur**
- Umsetzung der KI-Verordnung mit Hilfe der ISO 42001: Wo hilft die Norm weiter?
  - > Die Rolle des Qualitätsmanagements
  - > Die Rolle des Datenschutzes und der Informationssicherheit
  - > Umsetzungsoptionen mit Hilfe von Dokumenten und/oder Softwarelösungen
- Integrative Vorteile bei Kombination von Normen
- Warum die Norm nutzen?
- Q&A

ISO/IEC 42001:2023



Read sample

ISO/IEC 42001:2023

Information technology — Artificial intelligence — Management system

Published (Edition 1, 2023)

ISO/IEC 42001 ist eine internationale Norm, die Anforderungen an die Einrichtung, Implementierung, Wartung und kontinuierliche Verbesserung eines Managementsystems für künstliche Intelligenz (AIMS) in Organisationen festlegt. Sie richtet sich an Unternehmen, die KI-basierte Produkte oder Dienstleistungen **bereitstellen** oder **nutzen,** um eine verantwortungsvolle Entwicklung und Nutzung von KI-Systemen zu gewährleisten.

Warum ist die ISO/IEC 42001 wichtig?
Sie bietet eine wertvolle **Orientierungshilfe** für dieses sich schnell verändernde Technologiefeld.
Sie befasst sich mit den einzigartigen Herausforderungen, die KI mit sich bringt, wie z. B. ethische Überlegungen, Transparenz und kontinuierliches Lernen.
Für Unternehmen wird **ein strukturierter Weg** zum Management von Risiken und Chancen im Zusammenhang mit KI dargelegt, der Innovation und Governance in Einklang bringt.

Struktur

- Harmonized Structure (Integrierbar mit ISO 9001, 27001 etc.)
- Normativer Teil (Kap. 1-10)
- 4 Anhänge, 51 Seiten
- Anhang A Controls (38 zu verschiedenen Themen)
- Anhang B Implementation Guidance for AI Controls
- Anhang C Potential AI-related organizational objectives and risk sources
- Anhang D Use of AI Management System across domains or sectors

→ Die ISO 42006 regelt das Zertifizierungsverfahren der ISO 42001

Inhalt

Quelle: ISO 42001

Inhalt Anhang A - Auszug

A.3.2
AI roles and responsibilities
Roles and responsibilities for AI shall be defined and allocated according to the needs of the organization.

A.3.3
Reporting of concerns
The organization shall define and put in place a process to report concerns about the organization's role with respect to an AI system throughout its life cycle.

A.4.2
Resource documentation
The organization shall identify and document relevant resources required for the activities at given AI system life cycle stages and other AI-related activities relevant for the organization.

A.6.2.2
AI system requirements and specification
The organization shall specify and document requirements for new AI systems or material enhancements to existing systems.

A.6.2.3
Documentation of AI system design and development
The organization shall document the AI system design and development based on organizational objectives, documented requirements and specification criteria.

Quelle: ISO 42001

Themen

1. Organisationshilfe (Zusammenspiel von Governance, Management, Prozessen, Schulungen, Maßnahmen, Entwicklungsphase (»by design«), Daily Business)
2. Richtlinien und Qualitätsstandards
3. Risikomanagement (Bewertung und Folgeaktivitäten)-Dokumentation
4. Transparenzhilfe (Datenqualität, Test, Fortentwicklung mit neuen Daten)
5. Wertschöpfungskette
6. AI Act Konformitätsprüfung auf Basis Dokumentation & Antragswesen
7. Dokumentation und Berichtswesen
8. Pflege- und Weiterentwicklungsbasis
9. Compliance (Monitoring, KPI, Auditfähigkeit für interne/externe Prüfer, Regulatorik)

Agenda

- KI-Verordnung und die Anforderungen: Kurzer Überblick
- Managementsysteme: Kurze Beschreibung und konkreter Nutzen im Unternehmen
- KI-Managementsystem-Norm ISO 42001: Inhalte und Struktur
- **Umsetzung der KI-Verordnung mit Hilfe der ISO 42001: Wo hilft die Norm weiter?**
  - **> Die Rolle des Qualitätsmanagements**
  - **> Die Rolle des Datenschutzes und der Informationssicherheit**
  - **> Umsetzungsoptionen mit Hilfe von Dokumenten und/oder Softwarelösungen**
- Integrative Vorteile bei Kombination von Normen
- Warum die Norm nutzen?
- Q&A

Rolle des Qualitätsmanagements

Artikel 17 KI-VO:

Anbieter von AI-Systemen mit hohem Risiko müssen ein Qualitätsmanagementsystem einrichten, das die Einhaltung dieser Verordnung gewährleistet. Dieses System ist systematisch und ordnungsgemäß in Form von schriftlichen Strategien, Verfahren und Anweisungen zu dokumentieren.

- Es besteht eine starke Überschneidung zwischen den Anforderungen der EU-KI-Gesetzgebung und den Methoden des klassischen Qualitätsmanagements zur systematischen Planung und Steuerung von Abläufen mit Blick auf deren Qualität.

- QM zielt mit Tätigkeiten und Maßnahmen darauf ab, eine geforderte Produkt- oder Dienstleistungsqualität zu erreichen und beinhaltet alle organisatorischen Maßnahmen, die der Überwachung und Verbesserung der Prozessqualität, der Arbeitsqualität und damit der Produkt- und Dienstleistungsqualität dienen. (Regelkreis nach „Deming“, Lebenszyklus)

- Verfahren zur Daten-Governance müssen implementiert werden, um die Sicherheit und Qualität der verwendeten Daten zu gewährleisten.

Rolle des DS und IS

Artikel 15 KI-VO:

KI-Systeme mit hohem Risiko sind so zu konzipieren und zu entwickeln, dass sie ein angemessenes Niveau an Genauigkeit, Robustheit und Cybersicherheit erreichen und während ihres gesamten Lebenszyklus in dieser Hinsicht konsistent funktionieren.

- Anbieter müssen eine detaillierte technische Dokumentation führen, die auch Aspekte der Informationssicherheit umfasst
- Implementierung von Schutzmaßnahmen gegen Angriffe und Manipulationsversuche
- Ziele der Informationssicherheit: CIA (Confidentiality, Integrity, Availability) für **alle** Daten (Personenbezogene Daten und Firmendaten)
- Datenschutz & Informationssicherheit arbeiten Hand hin Hand

Umsetzungsoptionen

- Gelebte Praxis (Mund zu Mund, Erfahrungswissen, bilaterale Abstimmungen)
- Papier (Speicherung, Änderung, Drucken, Versionierung, Transport usw.)
- Elektronische Dokumente (Zugriff, Änderungsmanagement, Integration, Prozesse usw.) als „elektronische Loseblattsammlung“ oder mit Prozessen, Abhängigkeiten, Links, Freigaben usw.
- On Premise bzw. eigene Infrastruktur, Arbeitsplatzsystem, Netz
- Cloud-Lösung (Eigen, Nationaler Provider, Hyperscaler)
- Aspekte (Agiles Arbeiten, Wasserfall, Sprachen und Standorte, Änderungsform und -häufigkeit)
- Softwarelösungen mit verschiedenen Schwerpunkten und Philosophien (Prozessmanagement, Fachliche Inhalte, Dokumentenmanagement, Silos, Integrationen etc.) sowie Zielgruppen (Branchen, Startup) und Leistungsfähigkeit hinsichtlich der abbildbaren Größe einer Organisation (10 MA oder Konzern mit 100.000 MA) oder auch Arbeitsweise (Agile Projekte, Kollaborativ, Scrum, Kanban, Workflow)

Integrierte Managementsysteme

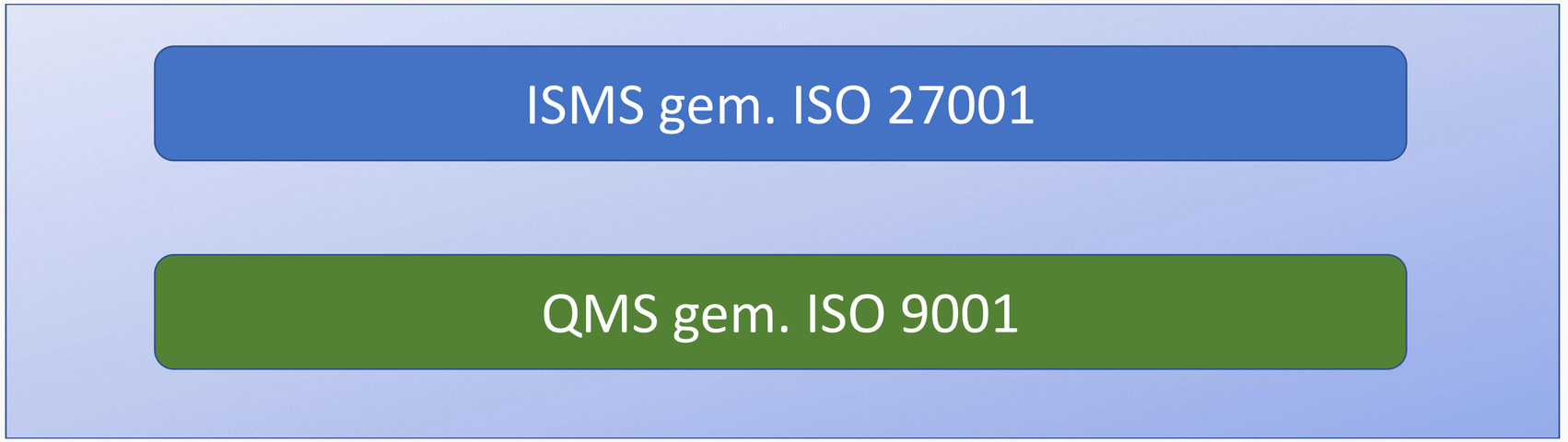
Um der Vielfalt an Anforderungen gerecht zu werden, können **mehrere Managementsysteme gleichzeitig** erforderlich sein. Dadurch steigt allerdings die Gefahr, dass durch parallele Regelungen, unklare Verantwortlichkeiten, umfangreiche Dokumentationen, Doppelarbeiten, widersprüchliche Lösungsansätze, Informationsverluste und **unnötige Kosten** anfallen. Alle Aspekte zusammen gefährden die Wirksamkeit des Gesamtsystems.

Vorteile eines integrierten Managementsystems:

- Nutzung von Synergieeffekten (z. B. einheitliche Verfahren und Instrumente)
- Reduzierung von Verwaltungsaufwand durch gemeinsame Dokumentation der Einzelsysteme
- Identifizierung und Optimierung von Schnittstellen
- Steigerung der Effizienz durch Vermeidung von Doppelarbeiten
- Vereinfachung komplexer Prozess- und Organisationsstrukturen
- Aufdeckung widersprüchlicher Anforderungen und möglicher Zielkonflikte
- Einsparung von Kosten und Zeit
- Erhöhung der Akzeptanz bei den Mitarbeitern

Managementsysteme

Beispiel: **Qualität und Informationssicherheit.**

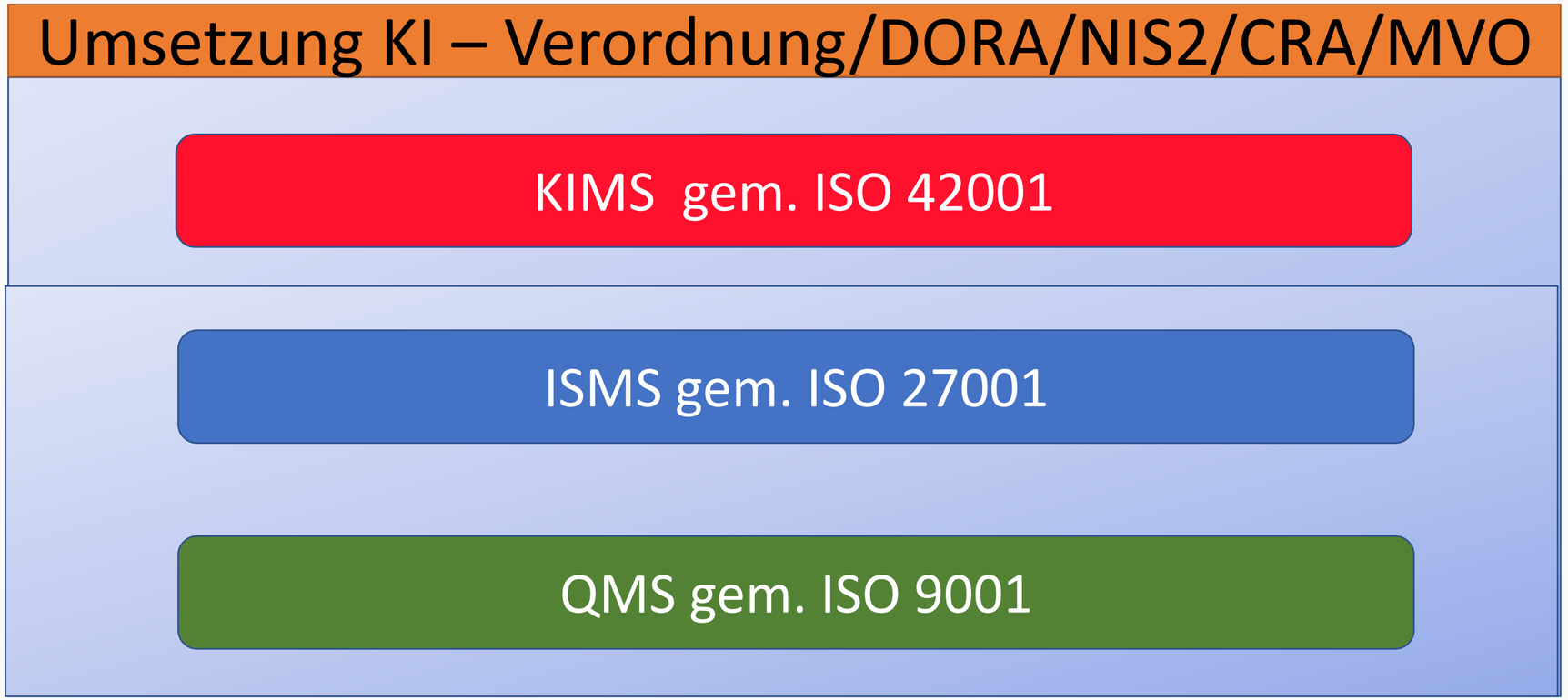


EnterpriseOS®

IMS lieferbar

ISO/IEC 42001 Integration

Integrierte Managementsysteme mit ISO 42001 helfen bei der Nutzung von KI und bilden das Fundament für die Anwendung und Einhaltung der KI-Verordnung



EnterpriseOS

IMS mit KIMS Q3/2025

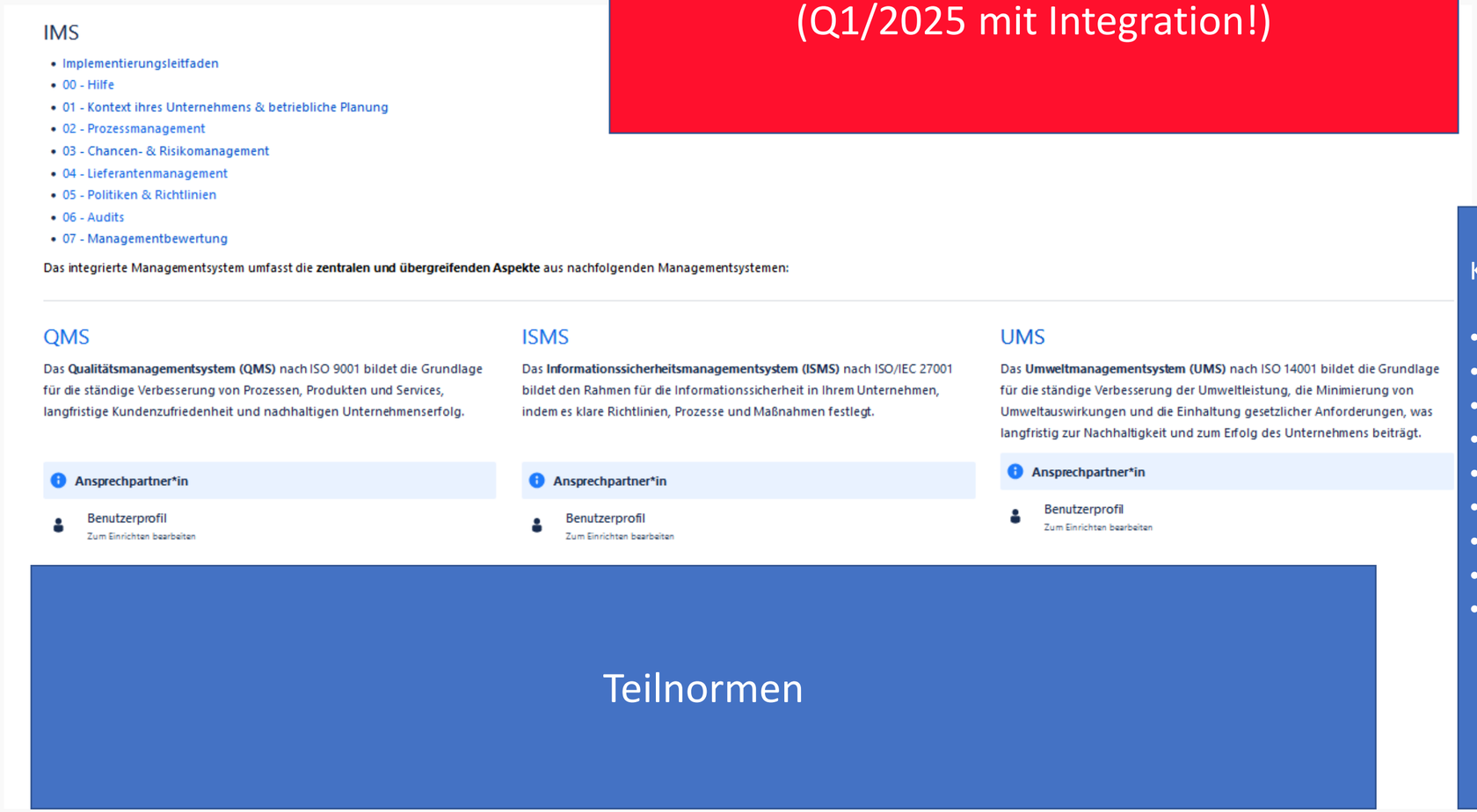
EnterpriseOS

IMS lieferbar

EnterpriseOS®

KI-Managementsystem

(Q1/2025 mit Integration!)



Teilnormen

KIMS (gem. ISO 42001)

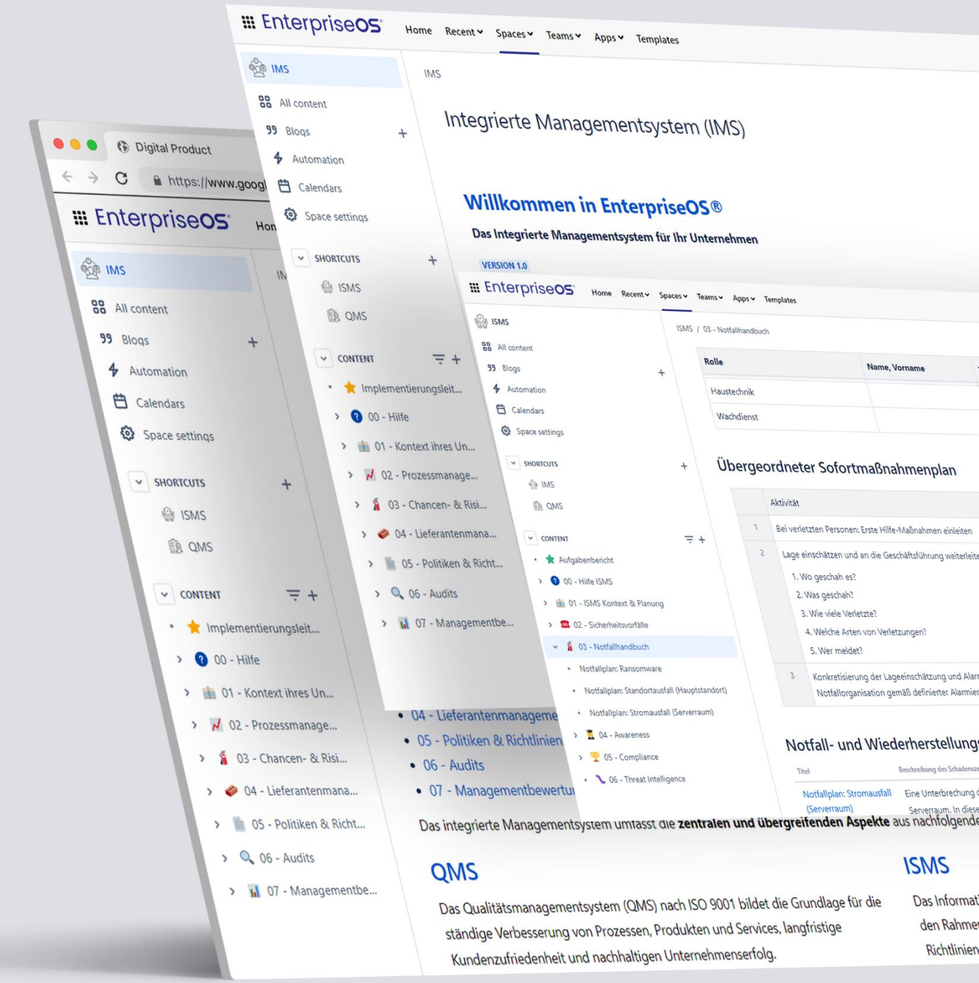
- Implementierungsleitfaden
- 00 Hilfe KIMS
- 01 Kontext und Planung
- 02 Risikomanagement
- 03 nn
- 04 nn
- 05 nn
- 06 nn
- 07 nn

Richtlinien, Auditplanung, Rollen- und Rechte,
Lieferantenmanagement siehe IMS

EnterpriseOS®

Management Systems made simple.

www.enterpriseos.de



Agenda

- KI-Verordnung und die Anforderungen: Kurzer Überblick
- Managementsysteme: Kurze Beschreibung und konkreter Nutzen im Unternehmen
- KI-Managementsystem-Norm ISO 42001: Inhalte und Struktur
- Umsetzung der KI-Verordnung mit Hilfe der ISO 42001: Wo hilft die Norm weiter?
  - > Die Rolle des Qualitätsmanagements
  - > Die Rolle des Datenschutzes und der Informationssicherheit
  - > Umsetzungsoptionen mit Hilfe von Dokumenten und/oder Softwarelösungen
- **Integrative Vorteile bei Kombination von Normen**
- Warum die Norm nutzen?
- Q&A

Weitere wichtige Normen

Grundsätzlich helfen Normen bei Reduktion von Komplexität, Austausch unter Marktteilnehmern, konservieren Wissen auf Basis von Wissenschaft, Technik und Erfahrung, und helfen bei der Verteilung und Nutzung von Wissen

ISO/IEC FDIS 42005

Information technology — Artificial intelligence — AI system impact assessment

Norm für die Risikoeinschätzung bei KI-Systemen

ISO/IEC FDIS 42006

Information technology — Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems

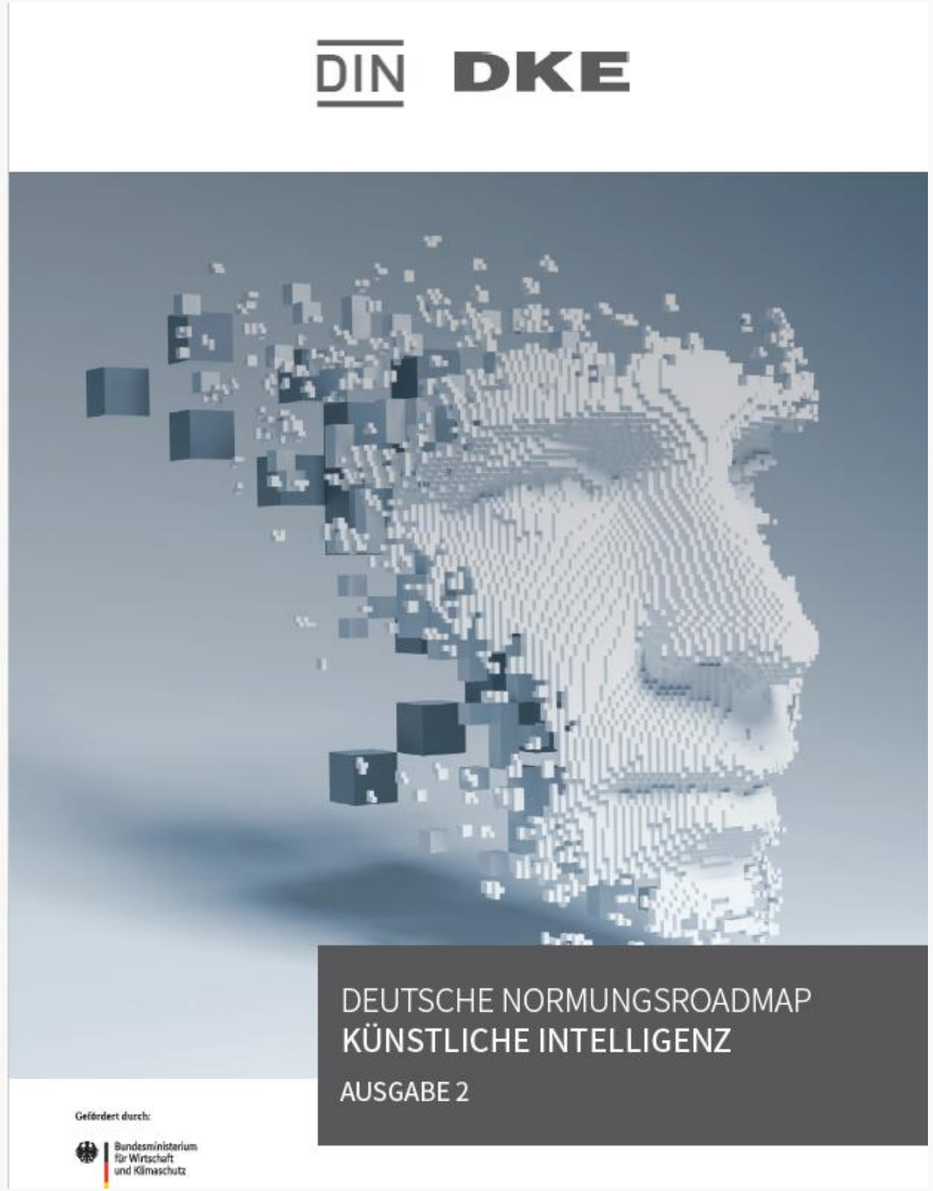
Norm für die Zertifizierung der ISO 42001 mit Anforderungen, Inhalte, Regeln der Prüfung

Wichtige Normen/Standards

ISO 27001 Informationssicherheits-management	**DSGVO**	**ISO 42001** KI-Managementsystem
DIN/TS 92004 Leitlinien zur Identifikation und Analyse von Risiken in KI-Systemen im gesamten Lebenszyklus (Entwickler, Anwender, Betreiber) als Ergänzung zur 23894	**ISO 23894** Informationstechnik - Künstliche Intelligenz - Leitlinien für Risikomanagement	**ISO 42005** Impact Assessment (Draft)
ISO 25059 System- und Software-Engineering - Qualitätskriterien und Bewertung von Systemen und Softwareprodukten (SQuaRE) - Qualitätsmodell für KI-Systeme	**ISO 22989** Informationstechnik - Künstliche Intelligenz - Konzepte und Terminologie der künstlichen Intelligenz	**ISO 42006** Regelungen zu Zertifizierung der 42001 (Draft)

Normungsroadmap

- Vielfältige Hilfen (kostenlos)
- Überblick behalten
- Branchen- und Industrieverbände bieten ggf. weitere Unterstützung



Agenda

- KI-Verordnung und die Anforderungen: Kurzer Überblick
- Managementsysteme: Kurze Beschreibung und konkreter Nutzen im Unternehmen
- KI-Managementsystem-Norm ISO 42001: Inhalte und Struktur
- Umsetzung der KI-Verordnung mit Hilfe der ISO 42001: Wo hilft die Norm weiter?
  - > Die Rolle des Qualitätsmanagements
  - > Die Rolle des Datenschutzes und der Informationssicherheit
  - > Umsetzungsoptionen mit Hilfe von Dokumenten und/oder Softwarelösungen
- Integrative Vorteile bei Kombination von Normen
- **Warum die Norm nutzen?**
- Q&A

Opportunitätsbetrachtung

Wenn Sie KI nutzen, aber Kosten und Aufwand minimal halten wollen, sowie Normen scheuen und auch kein IMS oder KIMS einführen wollen:

- Wenn Sie KI nutzen, sollten Sie einschätzen, welche Art der Anwendung vorliegt, um Risiken abzuwenden.
- Wenn Sie die regulatorischen Anforderungen der KI-VO erfüllen müssen, ist alles erforderliche zu organisieren, Dokumentieren, über den Lebenszyklus erhalten usw., was ggf. rechtliche Konsequenzen hat, wenn es nicht angemessen erfolgt
- EHDA-Kosten nicht ignorieren (reinvent the wheel)
- Ohne ISO 42001 ist eine Zertifizierung eines KI-Managementsystems **nicht möglich**!
- Markterwartungen?

Disruption

Die Nutzung der KI ist anspruchsvoll, es gibt viel zu tun, ja!

Manche werden sagen, die Norm braucht man doch nicht, das ist alles viel zu viel Aufwand!

Aber:

Die KI ist eine epochale Disruption, die mit grundlegenden technologischen Umwälzungen wie der Dampfmaschine oder dem Internet vergleichbar ist und die KI - Technologie ist es, die:

- Ein neues technologisches und kulturelles Zeitalter begründet
- Neue Geschäftsmodelle hervorbringt
- Ganze Industrien transformiert
- Einen enormen Produktivitätsschub auslöst

Frage: **Wollen Sie die großen Herausforderungen von morgen mit Antworten von gestern in homöopathischer Dosis angehen?**

Warum die Norm nutzen

- **Aufwandsreduktion:** Sie müssen sich das alles nicht selbst ausdenken
- **Geschwindigkeit:** Sie können heute schon auf einen Standard zurückgreifen
- **KI-Governance:** Hilft bei der Einhaltung gesetzlicher und regulatorischer Standards
- **Praktische Anleitung:** KI-spezifische Risiken effektiv managen
- **Kosteneffizienz:** Standards reduzieren internen Aufwand
- **Unterstützung weiterer Anforderungen:** CRA, MVO, Produkthaftpflicht, NIS2, DORA
- **Zertifizierung:** Von 3rd-Party-Auditoren prüf- und zertifizierbar (2025 geplant)

AWS und ISO42001

- ANAB, eine amerikanische Akkreditierungsstelle, hat auf Basis des ISO 42006-Drafts bereits eine Akkreditierung der Zertifizierungsstelle „Schellman Compliance, LLC" zugelassen!

- Schellman hat für Teile von AWS im November 2024 eine Zertifizierung des KIMS nach ISO 42001 durchgeführt (siehe Link unten)!

AWS achieves ISO/IEC 42001:2023 Artificial Intelligence Management System accredited certification

by Sara Duffer, Ashish Singh, and Peter Hallinan | on 25 NOV 2024 | in Announcements, Artificial Intelligence, Compliance, Responsible AI, Security, Identity, & Compliance | Permalink | Comments | Share

Amazon Web Services (AWS) is excited to be the first major cloud service provider to announce ISO/IEC 42001 accredited certification for AI services, covering: Amazon Bedrock, Amazon Q Business, Amazon Textract, and Amazon Transcribe. ISO/IEC 42001 is an international management system standard that outlines requirements and controls for organizations to promote the responsible development and use of AI systems.

Agenda

- KI-Verordnung und die Anforderungen: Kurzer Überblick
- Managementsysteme: Kurze Beschreibung und konkreter Nutzen im Unternehmen
- KI-Managementsystem-Norm ISO 42001: Inhalte und Struktur
- Umsetzung der KI-Verordnung mit Hilfe der ISO 42001: Wo hilft die Norm weiter?
  - > Die Rolle des Qualitätsmanagements
  - > Die Rolle des Datenschutzes und der Informationssicherheit
  - > Umsetzungsoptionen mit Hilfe von Dokumenten und/oder Softwarelösungen
- Integrative Vorteile bei Kombination von Normen
- Warum die Norm nutzen?
- **Q&A**

Q&A

Quelle: Spektrum der Wissenschaft, Spezial, Ausgabe 1.22

Ende

www.opexaadvisory.de

Kontaktdaten

Opexa Advisory GmbH

Franz-Joseph-Straße 11

D-80801 München

+49 89 9018 0448

Office@opexa.de

www.opexaadvisory.de

Klaus Kilvinger

Geschäftsführer

Disclaimer

- Die in diesem Vortrag genannten Produkte und Marken sowie Fotos dritter gehören den Eigentümern der jeweiligen Markenrechte. Alle anderen Rechte an dem Vortrag liegen bei der Opexa Advisory GmbH.
- Die Rechte an TISAX® gehören der ENX Association.
- Die Informationen wurde nach bestem Wissen und Gewissen zusammengestellt und deren Anwendung erfolgt ohne Gewähr.
- Die in diesem Dokument vermittelten Informationen stellen keine Rechtsberatung dar.
- Der Nachdruck oder eine Vervielfältigung dieses Dokumentes ist verboten, Verstöße werden verfolgt.

7 Schritte zum Erfolg

1. KI – Stellen/Fachleute/Beauftragten einrichten (Daueraufgabe!) mit Ausbildung
2. KI-Lösungen vorab sichten, bewerten, dokumentieren, ggf. vom Markt nehmen (inakzeptabel) mit Blick auf Januar 2025
3. Integriertes Managementsystem (IMS) einführen incl. ISMS (asap zertifizieren)
4. ISO 42001 im IMS integrieren (asap zertifizieren) und im Unternehmen einführen
5. Ergänzung des KI-MS mit Bezug auf die Anforderungen der KI-VO
6. Umfassende Kontrollen auf Betriebs-/Systemebene und Reviews etablieren
7. Pflege und Weiterentwicklung des IMS (Transparenzpflichten mit lernenden Systemen über die Laufzeit, CRA, MVO usw.)