ISO/IEC 42001: Ein Management-System für KI

KI verändert Wirtschaft und Gesellschaft grundlegend. Automatisierte Entscheidungsprozesse, selbstlernende Algorithmen und datengetriebene Innovationen eröffnen enorme Potenziale, bringen aber auch Herausforderungen mit sich. Unternehmen, die KI einsetzen, stehen vor zentralen Fragen: Wie lassen sich Risiken kontrollieren? Wie kann Transparenz und Nachvollziehbarkeit gewährleistet werden? Und wie bleibt Innovation dennoch agil?

Hier kommt die ISO/IEC 42001 ins Spiel – die weltweit erste Norm für ein Managementsystem für Künstliche Intelligenz (AIMS – Artificial Intelligence Management System). Sie wurde im Dezember 2023 veröffentlicht und bietet Unternehmen eine strukturierte, risiko- und governanceorientierte Herangehensweise, um KI verantwortungsvoll, effizient und sicher zu implementieren.

Was ist die ISO/IEC 42001?

Die ISO/IEC 42001:2023 ist eine international anerkannte Norm, die sich gezielt mit den Anforderungen an ein Managementsystem für KI auseinandersetzt. Sie orientiert sich an etablierten Standards wie der ISO 9001 (Qualitätsmanagement) oder der ISO/IEC 27001 (Informationssicherheit) und schafft damit eine einheitliche Grundlage für Governance, Risikomanagement, Transparenz und kontinuierliche Verbesserung von KI-Systemen. Die Norm ist analog anderer Normen aufgebaut und gliedert sich in die folgenden Hauptkapitel:

- **Kapitel 3:** Begriffe und Definitionen – Insgesamt werden 26 Begriffe definiert, unter anderem «AI system impact assessment» und «data quality»
- **Kapitel 4:** Kontext der Organisation – Welche internen und externen Faktoren beeinflussen den KI-Einsatz? Die verschiedenen Fussnoten geben zusätzliche Informationen.
- **Kapitel 5:** Führung – Welche Verantwortlichkeiten tragen das Management und die Stakeholder? Zusätzlich muss eine KI-Politik erstellt und die Rollen inkl. Verantwortlichkeiten definiert werden.
- **Kapitel 6:** Planung – Welche Risiken und Chancen sind zu berücksichtigen? Wie werden diese anschliessend behandelt? Welche KI-Ziele verfolgt das Unternehmen. Auch eine KI-Folgenabschätzung muss erstellt werden (analog einer Datenschutz-Folgenabschätzung).
- **Kapitel 7:** Unterstützung – Welche Ressourcen, Kompetenzen und Kommunikationswege sind essenziell? Auch die Awareness der involvierten Personen ist sicherzustellen. Weiter gehören Vorgaben an die Art der Dokumentation dazu.
- **Kapitel 8:** Betrieb – Wie lassen sich KI-Systeme sicher und effizient steuern? Die in Kapitel 6 erstellten Definitionen gilt es an dieser Stelle umzusetzen.
- **Kapitel 9:** Bewertung der Leistung – Welche Methoden garantieren ein wirksames Monitoring und Reporting? Dazu gehört die Definition von KPIs, die Durchführung des internen Audits und die Erstellung des Management-Berichts.
- **Kapitel 10:** Verbesserung – Wie werden KI-Systeme kontinuierlich optimiert? Und wie wird mit allfälligen Nicht-Konformitäten umgegangen, damit diese schnell behoben werden und sich nicht wiederholen können.
- **Anhang A:** Referenzkontrollziele – analog der ISO 27001 werden hier 38 umzusetzende Massnahmen definiert. Sie teilen sich auf die folgenden Themen auf: Richtlinien im Zusammenhang mit KI (3), Interne Organisation (2), Ressourcen für KI-Systeme (5), Bewertung der Auswirkungen von KI-Systemen (4), Lebenszyklus eines KI-Systems (9), Daten für KI-Systeme (5), Informationen für Interessenten an KI-Systemen (3), Einsatz von KI-Systemen (3), Beziehungen zu Drittanbietern und Kunden (3).
- **Anhang B:** Leitfaden zur Umsetzung von KI-Kontrollen – die in Anhang A definierten Anforderungen werden mit Implementierungshinweisen

Bild: Pixabay

Wie lassen sich Risiken kontrollieren? Wie kann Transparenz und Nachvollziehbarkeit gewährleistet werden? Und wie bleibt Innovation dennoch agil? Hier kommt die ISO/IEC 42001 ins Spiel.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

ergänzt. Der Aufbau ist analog der ISO 27002 aufgebaut.
- **Anhang C:** Mögliche KI-bezogene Organisationsziele und Risikoquellen – der Anhang enthält elf mögliche Ziele und sieben Risiko-Quellen, die berücksichtigt werden können, aber nicht müssen.

Die ISO/IEC 42001 ist branchenübergreifend anwendbar und hilft Unternehmen, KI-Prozesse strukturiert zu etablieren, zu kontrollieren und kontinuierlich anzupassen.

Warum ist die ISO/IEC 42001 wichtig?

KI-Technologien sind oft komplex, intransparent und hochgradig datengetrieben. Dies kann zu unvorhersehbaren Risiken führen: Bias in Algorithmen (Bias bedeutet dabei eine systematische Verzerrung der Wahrnehmung oder von Urteilen), mangelnde Erklärbarkeit, ethische Bedenken oder sogar rechtliche Konflikte.

Daher beantwortet die ISO/IEC 42001 entscheidende Fragen:
- Wie definiert ein Unternehmen klare Richtlinien für den KI-Einsatz?
- Welche Massnahmen verhindern Diskriminierung und Fehlentscheidungen?
- Wie können KI-Systeme sicher und regelkonform betrieben werden?
- Welche Anforderungen stellt das Risikomanagement an KI-Projekte?

Durch die Einführung standardisierter Prozesse hilft die Norm, Verantwortlichkeiten zu klären, Compliance sicherzustellen und Risiken zu minimieren.

Die Kernprinzipien der ISO/IEC 42001

Die Norm basiert auf einem strukturierten Managementansatz mit den folgenden Schwerpunkten:

1. KI-Governance und Verantwortlichkeit
   - Festlegung klarer Rollen und Zuständigkeiten im Unternehmen
   - Definition einer unternehmensweiten KI-Strategie

2. Risikomanagement und Transparenz
   - Identifikation, Analyse und Behandlung von KI-spezifischen Risiken
   - Berücksichtigung ethischer, technischer und rechtlicher Anforderungen

3. Kontinuierliche Verbesserung und Audits
   - Etablierung eines dynamischen Überwachungs- und Anpassungssystems
   - Regelmässige interne und externe Audits zur Optimierung

4. Dokumentation und Erklärbarkeit
   - Sicherstellung nachvollziehbarer Entscheidungsprozesse
   - Erstellung technischer und organisatorischer Dokumentationen

Diese Prinzipien gewährleisten, dass KI nicht nur leistungsfähig, sondern auch sicher, fair und regelkonform eingesetzt wird.

Für wen ist die Norm relevant?

Die ISO/IEC 42001 richtet sich an alle Organisationen, die KI-gestützte Produkte oder Dienstleistungen entwickeln, bereitstellen oder nutzen. Dazu gehören:
- Technologieunternehmen (Softwareentwicklung, Cloud-Dienste, Plattformen)
- Finanzsektor (Banken, Versicherungen, FinTechs)
- Gesundheitswesen (Medizinische KI, Diagnostik, Pharmaindustrie)
- Öffentliche Verwaltung (Smart Cities, KI in Behörden und Justiz)
- Industrie & Logistik (Automatisierung, Predictive Maintenance, Robotik)

Welche Vorteile bringt die Implementierung?

Ein nach ISO/IEC 42001 zertifiziertes KI-Managementsystem bietet Unternehmen zahlreiche Vorteile:
- Wettbewerbsvorteil – Nachweis einer verantwortungsvollen und regelkonformen KI-Nutzung schafft Vertrauen.
- Regulatorische Sicherheit – Vorbereitung auf zukünftige gesetzliche Vorgaben wie den AI-Act der EU.
- Reduziertes Haftungsrisiko – Systematisches Risikomanagement minimiert rechtliche und finanzielle Fallstricke.
- Effizienzsteigerung – Standardisierte Prozesse verbessern die Entwicklung, Implementierung und Wartung von KI-Systemen.
- Bessere Akzeptanz bei Stakeholdern – Klare Regeln und Transparenz fördern das Vertrauen bei Kunden und Partnern.

Zukunftssichere KI mit ISO/IEC 42001

Die ISO/IEC 42001 ist mehr als eine Norm – sie ist ein strategischer Leitfaden für verantwortungsbewusste KI-Entwicklung und -Nutzung. Unternehmen, die sich jetzt mit dieser Norm auseinandersetzen, können Chancen nutzen, Risiken minimieren und Innovationspotenzial sicher ausschöpfen. Die Norm kann für CHF 199 auf der offizielle ISO-Seite mittels nebenstehendem QR-Code gekauft werden.