management institut bochum // mib

Audit-Checkliste ISO/IEC 42001:2023 KI-Managementsystem

Verwendungshinweis:
Diese Checkliste ist als Leitfaden zu verstehen. Auditor:innen sollten flexibel bleiben und je nach Kontext, Größe und Komplexität der Organisation sowie der eingesetzten KI-Systeme Schwerpunkte setzen und zusätzliche Fragen formulieren.

Die Spalte "Nachweis / Beobachtungen / Methoden" soll dokumentieren, wie die Konformität geprüft wurde (z.B. Dokumentenprüfung, Interview, Beobachtung, Systemtest).

Die Spalte "Konformität" dient der Bewertung.

Struktur der Checkliste:
(Wie im Original beibehalten, relevant für das Verständnis der Gesamtstruktur, auch wenn nur Teile extrahiert werden)

- Allgemeine Informationen zum Audit
- Kapitel 4: Kontext der Organisation
- Kapitel 5: Führung
- Kapitel 6: Planung
- Kapitel 7: Unterstützung
- Kapitel 8: Betrieb
- Kapitel 9: Leistungsbewertung
- Kapitel 10: Verbesserung
- Anhang A (normativ): Referenzziele und Kontrollen für das Management (Dies ist ein sehr detaillierter Abschnitt)

Allgemeine Informationen zum Audit

(Dieser Abschnitt wird zur Vollständigkeit eines Auditberichts beibehalten, auch wenn er nicht direkt zu den Kapiteln 4-10 gehört)

Kriterium	**Feststellung/Information**
Auditierte Organisation	
Auditierter Bereich/Standort	
Auditdatum(e)	
Lead-Auditor	
Auditteam	
Ansprechpartner Organisation	
Audit-Nr.	
Ziel des Audits	(z.B. Erstzertifizierung, Überwachung, Rezertifizierung)
Scope des AIMS	(Gemäß Dokumentation der Organisation)
Referenzdokumente	ISO/IEC 42001:2023, AIMS-Dokumentation der Organisation
SoA (Statement of Applicablity)	SoA Datum / Version

Kapitel 4: Kontext der Organisation

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
4.1	Hat die Organisation externe und interne Themen bestimmt, die für ihren Zweck relevant sind und ihre Fähigkeit beeinflussen, die beabsichtigten Ergebnisse ihres AIMS zu erreichen?	4.1	Dokumentenprüfung, Interviews	
4.2	Wurde bestimmt, ob der Klimawandel ein relevantes Thema ist?	4.1	Dokumentenprüfung, Interviews	
4.3	Hat die Organisation den beabsichtigten Zweck der KI-Systeme berücksichtigt, die sie entwickelt, bereitstellt oder nutzt?	4.1	Dokumentenprüfung, Interviews	
4.4	Hat die Organisation ihre Rollen in Bezug auf diese KI-Systeme bestimmt (gemäß NOTE 1 zu 4.1)?	4.1	Dokumentenprüfung, Interviews	
4.5	Hat die Organisation die interessierten Parteien bestimmt, die für das AIMS relevant sind?	4.2	Dokumentenprüfung, Interviews	
4.6	Wurden die relevanten Anforderungen dieser interessierten Parteien bestimmt?	4.2	Dokumentenprüfung, Interviews	
4.7	Wurde festgelegt, welche dieser Anforderungen durch das AIMS adressiert werden?	4.2	Dokumentenprüfung, Interviews	
4.8	Hat die Organisation die Grenzen und Anwendbarkeit des AIMS festgelegt, um dessen Anwendungsbereich zu definieren?	4.3	Dokumentenprüfung (Scope-Dokument)	
4.9	Wurden bei der Festlegung des Anwendungsbereichs die externen und internen Themen (4.1) und die Anforderungen interessierter Parteien (4.2) berücksichtigt?	4.3	Dokumentenprüfung	
4.10	Ist der Anwendungsbereich als dokumentierte Information verfügbar?	4.3	Dokumentenprüfung	
4.11	Bestimmt der Anwendungsbereich die Aktivitäten der Organisation in Bezug auf die Anforderungen der Norm (Führung, Planung, Unterstützung etc.)?	4.3	Dokumentenprüfung, Interviews	
4.12	Hat die Organisation ein AIMS eingerichtet,	4.4	Dokumentenprüfung (AIMS-Handbuch,	

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
	implementiert, aufrechterhalten, fortlaufend verbessert und dokumentiert, einschließlich der benötigten Prozesse und deren Wechselwirkungen?		Prozessbeschreibungen), Interviews	

Kapitel 5: Führung

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
5.1	Zeigt die oberste Leitung Führung und Engagement in Bezug auf das AIMS (durch Sicherstellung von KI-Politik, Zielen, Integration, Ressourcen etc.)?	5.1	Interviews mit oberster Leitung, Dokumentenprüfung	
5.2	Stellt die oberste Leitung sicher, dass die KI-Politik und KI-Ziele festgelegt sind und mit der strategischen Ausrichtung der Organisation vereinbar sind?	5.1 a)	Interviews, Prüfung KI-Politik & Ziele, Strategiedokumente	
5.3	Stellt die oberste Leitung die Integration der AIMS-Anforderungen in die Geschäftsprozesse der Organisation sicher?	5.1 b)	Interviews, Prüfung Prozesslandschaft	
5.4	Stellt die oberste Leitung sicher, dass die für das AIMS benötigten Ressourcen verfügbar sind?	5.1 c)	Interviews, Budgetprüfung, Personalplanung	
5.5	Kommuniziert die oberste Leitung die Bedeutung eines effektiven KI-Managements und der Einhaltung der AIMS-Anforderungen?	5.1 d)	Interviews, interne Kommunikationsnachweise	
5.6	Stellt die oberste Leitung sicher, dass das AIMS seine beabsichtigten Ergebnisse erzielt?	5.1 e)	Interviews, KPI-Auswertungen, Management Review Protokolle	
5.7	Leitet und unterstützt die oberste Leitung Personen, um zur Wirksamkeit des AIMS beizutragen?	5.1 f)	Interviews mit Mitarbeitern, Schulungsnachweise	
5.8	Fördert die oberste Leitung die fortlaufende Verbesserung?	5.1 g)	Interviews, Nachweis von Verbesserungsprojekten	
5.9	Unterstützt die oberste Leitung andere relevante Rollen, um deren Führung in ihren	5.1 h)	Interviews	

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
	Verantwortungsbereichen zu demonstrieren?			
5.10	Hat die oberste Leitung eine KI-Politik festgelegt, die a) dem Zweck der Organisation angemessen ist, b) einen Rahmen für KI-Ziele bietet, c) eine Verpflichtung zur Erfüllung geltender Anforderungen enthält und d) eine Verpflichtung zur fortlaufenden Verbesserung des AIMS enthält?	5.2	Prüfung der KI-Politik	
5.11	Ist die KI-Politik als dokumentierte Information verfügbar?	5.2	Dokumentenprüfung	
5.12	Verweist die KI-Politik, soweit relevant, auf andere organisationale Politiken?	5.2	Prüfung der KI-Politik	
5.13	Wird die KI-Politik innerhalb der Organisation kommuniziert?	5.2	Kommunikationsnachweise, Mitarbeiterinterviews	
5.14	Ist die KI-Politik für interessierte Parteien, soweit angemessen, verfügbar?	5.2	Webseite, Informationsbroschüren	
5.15	Sind die Verantwortlichkeiten und Befugnisse für relevante Rollen zugewiesen und innerhalb der Organisation kommuniziert?	5.3	Organigramm, Stellenbeschreibungen, Interviews	
5.16	Hat die oberste Leitung die Verantwortung und Befugnis zugewiesen für: a) die Sicherstellung, dass das AIMS den Anforderungen dieser Norm entspricht, und b) die Berichterstattung über die Leistung des AIMS an die oberste Leitung?	5.3	Stellenbeschreibungen, Interviews	

Kapitel 6: Planung

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
6.1	Berücksichtigt die Organisation bei der Planung des AIMS die Themen aus 4.1 und die Anforderungen aus 4.2 und bestimmt die Risiken und Chancen, die adressiert werden müssen?	6.1.1	Risikomanagement-dokumentation, SWOT-Analysen, Protokolle	

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
6.2	Werden Risiken und Chancen bestimmt, um a) sicherzustellen, dass das AIMS seine beabsichtigten Ergebnisse erreichen kann, b) unerwünschte Auswirkungen zu verhindern oder zu reduzieren, c) fortlaufende Verbesserung zu erreichen?	6.1.1	Risikobewertungsberichte, Maßnahmenpläne	
6.3	Hat die Organisation KI-Risikokriterien festgelegt und aufrechterhalten, die Folgendes unterstützen: Unterscheidung akzeptabler von nicht akzeptablen Risiken, Durchführung von KI-Risikobewertungen, Durchführung der KI-Risikobehandlung, Bewertung von KI-Risikoauswirkungen?	6.1.1	Dokumentierte KI-Risikokriterien	
6.4	Bestimmt die Organisation Risiken und Chancen gemäß: dem Domänen- und Anwendungskontext eines KI-Systems, dem beabsichtigten Einsatz, dem externen und internen Kontext (4.1)?	6.1.1	Risikobewertungs-dokumentation für spezifische KI-Systeme	
6.5	Plant die Organisation: a) Maßnahmen zur Adressierung dieser Risiken und Chancen, b) wie diese Maßnahmen in ihre AIMS-Prozesse integriert und implementiert und deren Wirksamkeit bewertet werden?	6.1.1	Maßnahmenpläne, Prozessbeschreibungen, Wirksamkeitsprüfungen	
6.6	Wird dokumentierte Information über ergriffene Maßnahmen zur Identifizierung und Adressierung von KI-Risiken und KI-Chancen aufbewahrt?	6.1.1	Risikoregister, Maßnahmenverfolgung	
6.7	Hat die Organisation einen KI-Risikobewertungsprozess definiert und etabliert, der: a) von KI-Politik und -Zielen informiert und darauf abgestimmt ist, b) so gestaltet ist, dass wiederholte Bewertungen konsistente, valide und vergleichbare Ergebnisse liefern?	6.1.2 a), b)	Prozessbeschreibung KI-Risikobewertung, Vergleich von Ergebnissen	

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
6.8	Identifiziert der KI-Risikobewertungsprozess Risiken, die das Erreichen der KI-Ziele fördern oder verhindern?	6.1.2 c)	Risikobewertungsberichte	
6.9	Analysiert der KI-Risikobewertungsprozess KI-Risiken, um: 1) potenzielle Konsequenzen für Organisation, Individuen und Gesellschaften zu bewerten, 2) ggf. die realistische Wahrscheinlichkeit zu bewerten, 3) Risikoniveaus zu bestimmen?	6.1.2 d)	Risikobewertungsberichte, Impact Assessments	
6.10	Bewertet der KI-Risikobewertungsprozess KI-Risiken, um: 1) Ergebnisse der Risikoanalyse mit Risikokriterien zu vergleichen, 2) bewertete Risiken für die Risikobehandlung zu priorisieren?	6.1.2 e)	Risikobewertungsberichte, Priorisierungsmatrix	
6.11	Wird dokumentierte Information über den KI-Risikobewertungsprozess aufbewahrt?	6.1.2	Prozessdokumentation, Berichte	
6.12	Hat die Organisation unter Berücksichtigung der Risikobewertungsergebnisse einen KI-Risikobehandlungsprozess definiert, um: a) geeignete Optionen zur KI-Risikobehandlung auszuwählen?	6.1.3 a)	Prozessbeschreibung KI-Risikobehandlung, Auswahl von Behandlungsoptionen	
6.13	Bestimmt der KI-Risikobehandlungsprozess alle Kontrollen, die zur Implementierung der gewählten Optionen notwendig sind, und vergleicht diese mit Anhang A, um sicherzustellen, dass keine notwendigen Kontrollen ausgelassen wurden?	6.1.3 b)	Kontrolllisten, Abgleich mit Anhang A, Statement of Applicability (SoA)	
6.14	Berücksichtigt der KI-Risikobehandlungsprozess die für die Implementierung relevanten Kontrollen aus Anhang A?	6.1.3 c)	SoA, Risikobehandlungsplan	
6.15	Identifiziert der KI-Risikobehandlungsprozess, ob zusätzliche Kontrollen	6.1.3 d)	SoA, Risikobehandlungsplan	

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
	über Anhang A hinaus notwendig sind, um alle Behandlungsoptionen zu implementieren?			
6.16	Berücksichtigt der KI-Risikobehandlungsprozess die Anleitung in Anhang B für die Implementierung der bestimmten Kontrollen?	6.1.3 e)	Interviews, Überprüfung der Kontrollimplementierung	
6.17	Erstellt der KI-Risikobehandlungsprozess ein Statement of Applicability (SoA), das die notwendigen Kontrollen enthält und Begründungen für Ein- und Ausschluss von Kontrollen liefert?	6.1.3 f)	SoA-Dokument	
6.18	Formuliert der KI-Risikobehandlungsprozess einen KI-Risikobehandlungsplan?	6.1.3 g)	KI-Risikobehandlungsplan	
6.19	Holt die Organisation die Genehmigung des designierten Managements für den KI-Risikobehandlungsplan und die Akzeptanz der Restrisiken ein?	6.1.3	Genehmigungsnachweise, Managemententscheidungen	
6.20	Sind die notwendigen Kontrollen auf die Ziele in 6.2 ausgerichtet, als dokumentierte Information verfügbar, innerhalb der Organisation kommuniziert und für interessierte Parteien, soweit angemessen, verfügbar?	6.1.3	SoA, Kontrolldokumentation, Kommunikationsnachweise	
6.21	Wird dokumentierte Information über den KI-Risikobehandlungsprozess aufbewahrt?	6.1.3	Prozessdokumentation, Risikobehandlungsplan, SoA	
6.22	Hat die Organisation einen Prozess zur Bewertung der potenziellen Konsequenzen für Individuen, Gruppen von Individuen oder beide und Gesellschaften definiert, die aus Entwicklung, Bereitstellung oder Nutzung von KI-Systemen resultieren können (KI-System-Folgenabschätzung)?	6.1.4	Prozessbeschreibung KI-System-Folgenabschätzung	
6.23	Bestimmt die KI-System-Folgenabschätzung die potenziellen Konsequenzen des Einsatzes, der beabsichtigten Nutzung und des vorhersehbaren	6.1.4	Berichte der KI-System-Folgenabschätzung	

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
	Missbrauchs eines KI-Systems für Individuen, Gruppen oder beide und Gesellschaften?			
6.24	Berücksichtigt die KI-System-Folgenabschätzung den spezifischen technischen und gesellschaftlichen Kontext, in dem das KI-System eingesetzt wird, und anwendbare Rechtsordnungen?	6.1.4	Berichte der KI-System-Folgenabschätzung	
6.25	Wird das Ergebnis der KI-System-Folgenabschätzung dokumentiert und ggf. relevanten interessierten Parteien zur Verfügung gestellt?	6.1.4	Dokumentierte Ergebnisse, Nachweis der Bereitstellung	
6.26	Berücksichtigt die Organisation die Ergebnisse der KI-System-Folgenabschätzung bei der Risikobewertung (6.1.2)?	6.1.4	Risikobewertungsberichte	
6.27	Hat die Organisation KI-Ziele auf relevanten Funktionen und Ebenen festgelegt?	6.2	Dokumentierte KI-Ziele	
6.28	Sind die KI-Ziele: a) konsistent mit der KI-Politik, b) messbar (falls praktikabel), c) berücksichtigen sie anwendbare Anforderungen, d) werden sie überwacht, e) kommuniziert, f) bei Bedarf aktualisiert, g) als dokumentierte Information verfügbar?	6.2	Überprüfung der KI-Ziele anhand der Kriterien, Monitoring-Aufzeichnungen, Kommunikationsnachweise	
6.29	Bestimmt die Organisation bei der Planung, wie ihre KI-Ziele erreicht werden sollen: was getan wird, welche Ressourcen benötigt werden, wer verantwortlich ist, wann es abgeschlossen sein wird, wie die Ergebnisse bewertet werden?	6.2	Maßnahmenpläne zur Zielerreichung	
6.30	Werden Änderungen am AIMS, wenn die Organisation den Bedarf dafür feststellt, in geplanter Weise durchgeführt?	6.3	Änderungsmanagementprozess, Änderungsanträge und -protokolle	

Kapitel 7: Unterstützung

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
7.1	Bestimmt und stellt die Organisation die Ressourcen bereit, die für Einrichtung, Implementierung, Aufrechterhaltung und fortlaufende Verbesserung des AIMS benötigt werden?	7.1	Budgetplanung, Personalplanung, Infrastrukturplanung	
7.2	Bestimmt die Organisation die notwendige Kompetenz von Personen, die unter ihrer Kontrolle arbeiten und ihre KI-Leistung beeinflussen?	7.2 a)	Kompetenzmatrizen, Stellenbeschreibungen	
7.3	Stellt die Organisation sicher, dass diese Personen auf Basis angemessener Ausbildung, Schulung oder Erfahrung kompetent sind?	7.2 b)	Schulungsnachweise, Zertifikate, Erfahrungsnachweise	
7.4	Ergreift die Organisation gegebenenfalls Maßnahmen, um die notwendige Kompetenz zu erwerben, und bewertet die Wirksamkeit der ergriffenen Maßnahmen?	7.2 c)	Schulungspläne, Wirksamkeitsbewertungen von Schulungen	
7.5	Ist angemessene dokumentierte Information als Nachweis der Kompetenz verfügbar?	7.2	Personalakten, Schulungszertifikate	
7.6	Sind sich Personen, die unter der Kontrolle der Organisation arbeiten, bewusst über: die KI-Politik, ihren Beitrag zur Wirksamkeit des AIMS (einschließlich der Vorteile verbesserter KI-Leistung), die Auswirkungen der Nichteinhaltung der AIMS-Anforderungen?	7.3	Mitarbeiterinterviews, Schulungsunterlagen zu Awareness	
7.7	Bestimmt die Organisation die internen und externen Kommunikationen, die für das AIMS relevant sind, einschließlich: was, wann, mit wem und wie kommuniziert wird?	7.4	Kommunikationsplan, Kommunikationsmatrix, Protokolle	
7.8	Umfasst das AIMS der Organisation: a) dokumentierte Information, die von dieser Norm gefordert wird, b) dokumentierte Information, die von der Organisation als notwendig für die Wirksamkeit des AIMS bestimmt wurde?	7.5.1	Überprüfung der AIMS-Dokumentation auf Vollständigkeit	
7.9	Stellt die Organisation bei der Erstellung und Aktualisierung dokumentierter Information	7.5.2	Verfahren zur Dokumentenerstellung und -	

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
	eine angemessene Identifizierung und Beschreibung, Format und Medien sowie Überprüfung und Genehmigung auf Eignung und Angemessenheit sicher?		aktualisierung, Beispiele für geprüfte Dokumente	
7.10	Wird dokumentierte Information, die vom AIMS und dieser Norm gefordert wird, kontrolliert, um sicherzustellen, dass sie: a) verfügbar und für den Gebrauch geeignet ist, wo und wann sie benötigt wird, b) angemessen geschützt ist (z.B. vor Verlust der Vertraulichkeit, unsachgemäßer Verwendung oder Integritätsverlust)?	7.5.3 a), b)	Dokumentenlenkungsverfahren, Zugriffskontrollen, Backup-Verfahren	
7.11	Adressiert die Organisation für die Kontrolle dokumentierter Information folgende Aktivitäten, soweit anwendbar: Verteilung, Zugriff, Abruf und Nutzung; Lagerung und Erhaltung (einschließlich Lesbarkeit); Kontrolle von Änderungen (z.B. Versionskontrolle); Aufbewahrung und Verfügung?	7.5.3	Verfahren zur Dokumentenlenkung, Stichprobenprüfung der Umsetzung	
7.12	Wird extern stammende dokumentierte Information, die von der Organisation als notwendig für Planung und Betrieb des AIMS bestimmt wurde, angemessen identifiziert und kontrolliert?	7.5.3	Verzeichnis externer Dokumente, Nachweis der Kontrolle	

Kapitel 8: Betrieb

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
8.1	Plant, implementiert und kontrolliert die Organisation die Prozesse, die zur Erfüllung der Anforderungen und zur Umsetzung der in Kapitel 6 bestimmten Maßnahmen benötigt werden, durch: Festlegung von Kriterien für die Prozesse, Implementierung der Kontrolle der Prozesse gemäß den Kriterien?	8.1	Prozessbeschreibungen, Arbeitsanweisungen, Prozess-KPIs	
8.2	Implementiert die Organisation die gemäß 6.1.3 bestimmten Kontrollen, die sich auf den Betrieb des AIMS beziehen (z.B. KI-Systementwicklungs- und Nutzungslebenszyklus-bezogene Kontrollen)?	8.1	SoA, Nachweis der Implementierung von Kontrollen (siehe auch Audit von Anhang A)	
8.3	Wird die Wirksamkeit dieser Kontrollen überwacht und werden Korrekturmaßnahmen in Betracht gezogen, wenn die beabsichtigten Ergebnisse nicht erreicht werden?	8.1	Monitoring-Aufzeichnungen, Berichte über Wirksamkeitsprüfungen, Korrekturmaßnahmenpläne	
8.4	Ist dokumentierte Information in dem Umfang verfügbar, der notwendig ist, um Vertrauen zu haben, dass die Prozesse wie geplant durchgeführt wurden?	8.1	Prozessaufzeichnungen, Protokolle	
8.5	Kontrolliert die Organisation geplante Änderungen und überprüft die Konsequenzen unbeabsichtigter Änderungen, wobei bei Bedarf Maßnahmen zur Minderung nachteiliger Auswirkungen ergriffen werden?	8.1	Änderungsmanagementprozess, Aufzeichnungen von Änderungsbewertungen	
8.6	Stellt die Organisation sicher, dass extern bereitgestellte Prozesse, Produkte oder Dienstleistungen, die für das AIMS relevant sind, kontrolliert werden?	8.1	Lieferantenmanagementprozess, Verträge, Lieferantenbewertungen	
8.7	Führt die Organisation KI-Risikobewertungen gemäß 6.1.2 in geplanten Intervallen oder bei wesentlichen Änderungen durch?	8.2	Zeitplan für Risikobewertungen, Protokolle von Risikobewertungen nach Änderungen	
8.8	Bewahrt die Organisation dokumentierte Information über die Ergebnisse aller KI-Risikobewertungen auf?	8.2	Risikobewertungsberichte	
8.9	Implementiert die Organisation den KI-Risikobehandlungsplan gemäß 6.1.3 und überprüft dessen Wirksamkeit?	8.3	Nachweis der Implementierung des Behandlungsplans, Wirksamkeitsprüfungen	

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
8.10	Wird bei neuen Risiken, die eine Behandlung erfordern, ein Risikobehandlungsprozess gemäß 6.1.3 durchgeführt?	8.3	Nachweis der Behandlung neu identifizierter Risiken	
8.11	Werden Risikobehandlungsoptionen, die nicht wirksam sind, überprüft, neu validiert und der Risikobehandlungsplan aktualisiert?	8.3	Überprüfungsprotokolle, aktualisierte Pläne	
8.12	Bewahrt die Organisation dokumentierte Information über die Ergebnisse aller KI-Risikobehandlungen auf?	8.3	Risikobehandlungsberichte	
8.13	Führt die Organisation KI-System-Folgenabschätzungen gemäß 6.1.4 in geplanten Intervallen oder bei wesentlichen Änderungen durch?	8.4	Zeitplan für Folgenabschätzungen, Protokolle von Folgenabschätzungen nach Änderungen	
8.14	Bewahrt die Organisation dokumentierte Information über die Ergebnisse aller KI-System-Folgenabschätzungen auf?	8.4	Berichte der KI-System-Folgenabschätzung	

Kapitel 9: Leistungsbewertung

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
9.1	Bestimmt die Organisation: was überwacht und gemessen werden muss; die Methoden für Überwachung, Messung, Analyse und Bewertung, um valide Ergebnisse sicherzustellen; wann die Überwachung und Messung durchgeführt wird; wann die Ergebnisse analysiert und bewertet werden?	9.1	Überwachungs- und Messplan, definierte Metriken und Methoden, Zeitpläne	
9.2	Ist dokumentierte Information als Nachweis der Ergebnisse verfügbar?	9.1	Messprotokolle, Analyseberichte	
9.3	Bewertet die Organisation die Leistung und Wirksamkeit des AIMS?	9.1	Management Review Protokolle, Leistungsberichte	
9.4	Führt die Organisation interne Audits in geplanten Intervallen durch, um Informationen darüber zu liefern, ob das AIMS: a) den eigenen Anforderungen der Organisation und den Anforderungen dieser Norm entspricht, b) wirksam	9.2.1	Auditplan, Auditberichte	

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
	implementiert und aufrechterhalten wird?			
9.5	Plant, etabliert, implementiert und pflegt die Organisation (ein) Auditprogramm(e), einschließlich Häufigkeit, Methoden, Verantwortlichkeiten, Planungsanforderungen und Berichterstattung?	9.2.2	Dokumentiertes Auditprogramm	
9.6	Berücksichtigt die Organisation bei der Erstellung des Auditprogramms die Bedeutung der betroffenen Prozesse und die Ergebnisse früherer Audits?	9.2.2	Auditprogramm, Begründung für Audithäufigkeit	
9.7	Definiert die Organisation für jedes Audit die Auditziele, -kriterien und den -umfang?	9.2.2 a)	Auditpläne für einzelne Audits	
9.8	Wählt die Organisation Auditoren aus und führt Audits so durch, dass Objektivität und Unparteilichkeit des Auditprozesses sichergestellt sind?	9.2.2 b)	Qualifikationsnachweise der Auditoren, Unabhängigkeitserklärungen	
9.9	Stellt die Organisation sicher, dass die Ergebnisse der Audits an relevante Manager berichtet werden?	9.2.2 c)	Auditberichte, Verteilerlisten	
9.10	Ist dokumentierte Information als Nachweis der Implementierung des Auditprogramms und der Auditergebnisse verfügbar?	9.2.2	Auditprogramm, Auditpläne, Auditberichte	
9.11	Überprüft die oberste Leitung das AIMS der Organisation in geplanten Intervallen, um dessen fortlaufende Eignung, Angemessenheit und Wirksamkeit sicherzustellen?	9.3.1	Management Review Plan, Einladungen, Protokolle	
9.12	Umfasst die Managementbewertung Eingaben wie: Status von Maßnahmen aus früheren Reviews; Änderungen externer/interner Themen; Änderungen von Bedürfnissen/Erwartungen interessierter Parteien; Informationen zur AIMS-Leistung (Nichtkonformitäten, Korrekturmaßnahmen, Überwachungs-/Messergebnisse, Auditergebnisse, Chancen zur fortlaufenden Verbesserung)?	9.3.2	Management Review Protokolle, zugrundeliegende Berichte und Analysen	
9.13	Umfassen die Ergebnisse der Managementbewertung Entscheidungen über Chancen	9.3.3	Management Review Protokolle, Aktionspläne	

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
	zur fortlaufenden Verbesserung und jeglichen Bedarf an Änderungen des AIMS?			
9.14	Ist dokumentierte Information als Nachweis der Ergebnisse von Managementbewertungen verfügbar?	9.3.3	Management Review Protokolle	

Kapitel 10: Verbesserung

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
10.1	Verbessert die Organisation fortlaufend die Eignung, Angemessenheit und Wirksamkeit des AIMS?	10.1	Nachweis von Verbesserungsprojekten, Aktualisierungen von Prozessen/Dokumenten aufgrund von Reviews/Audits etc.	
10.2	Wenn eine Nichtkonformität auftritt, reagiert die Organisation darauf und ergreift ggf. Maßnahmen zur Kontrolle und Korrektur und behandelt die Konsequenzen?	10.2 a)	Prozess für Nichtkonformitäten und Korrekturmaßnahmen, Beispiele bearbeiteter Nichtkonformitäten	
10.3	Bewertet die Organisation die Notwendigkeit von Maßnahmen zur Beseitigung der Ursache(n) der Nichtkonformität, damit sie nicht erneut oder an anderer Stelle auftritt, durch: Überprüfung der Nichtkonformität; Bestimmung der Ursachen; Bestimmung, ob ähnliche Nichtkonformitäten existieren oder potenziell auftreten können?	10.2 b)	Ursachenanalysen, Aufzeichnungen	
10.4	Implementiert die Organisation jegliche benötigte Maßnahme?	10.2 c)	Nachweis implementierter Korrekturmaßnahmen	
10.5	Überprüft die Organisation die Wirksamkeit jeglicher ergriffener Korrekturmaßnahme?	10.2 d)	Wirksamkeitsprüfungen	
10.6	Nimmt die Organisation bei Bedarf Änderungen am AIMS vor?	10.2 e)	Aktualisierte AIMS-Dokumentation	
10.7	Sind Korrekturmaßnahmen den Auswirkungen der aufgetretenen Nichtkonformitäten angemessen?	10.2	Bewertung der Angemessenheit von Korrekturmaßnahmen	
10.8	Ist dokumentierte Information als Nachweis verfügbar über: die Art der Nichtkonformitäten und jegliche nachfolgend ergriffene Maßnahmen; die	10.2	Aufzeichnungen zu Nichtkonformitäten und Korrekturmaßnahmen	

Nr.	Auditfrage (basierend auf ISO/IEC 42001 Anforderungen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
	Ergebnisse jeglicher Korrekturmaßnahme?			

Anhang A (normativ): Referenzziele und Kontrollen für das Management

Hinweis: Die Organisation muss nicht alle Kontrollen aus Anhang A anwenden, sondern diejenigen, die für die Behandlung ihrer KI-Risiken und zur Erreichung ihrer KI-Ziele notwendig sind (siehe 6.1.3). Die Auswahl muss im Statement of Applicability (SoA) begründet sein. Dieses Audit prüft die Implementierung der im SoA als anwendbar deklarierten Kontrollen.

A.2 Politiken im Zusammenhang mit KI

(Ziel: Managementrichtung und Unterstützung für KI-Systeme gemäß Geschäftsanforderungen bereitstellen.)

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
A2.1	Hat die Organisation eine Politik für die Entwicklung oder Nutzung von KI-Systemen dokumentiert? (Wird bereits unter 5.2 geprüft, hier Fokus auf Implementierung der Kontrolle)	A.2.2	KI-Politik Dokument, Interviews	
A2.2	Hat die Organisation bestimmt, wo andere Politiken von den Zielen der Organisation in Bezug auf KI-Systeme betroffen sein könnten oder darauf anwendbar sind, und diese entsprechend abgestimmt/aktualisiert?	A.2.3	Analyse der Wechselwirkungen von Politiken, aktualisierte Politiken, KI-Politik	
A2.3	Wird die KI-Politik in geplanten Intervallen oder bei Bedarf überprüft, um ihre fortlaufende Eignung, Angemessenheit und Wirksamkeit sicherzustellen? (Wird bereits unter 5.2 geprüft, hier Fokus auf Implementierung)	A.2.4	Überprüfungsprotokolle der KI-Politik, Nachweis von Aktualisierungen	

A.3 Interne Organisation

(Ziel: Rechenschaftspflicht innerhalb der Organisation etablieren, um ihren verantwortungsvollen Ansatz für Implementierung, Betrieb und Management von KI-Systemen aufrechtzuerhalten.)

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
A3.1	Sind Rollen und Verantwortlichkeiten für KI gemäß den Bedürfnissen der Organisation definiert und zugewiesen? (Wird bereits unter 5.3 geprüft, hier Fokus auf Implementierung)	A.3.2	Organigramm, Stellenbeschreibungen, Verantwortlichkeitsmatrix für KI-Aspekte	
A3.2	Hat die Organisation einen Prozess definiert und eingeführt, um Bedenken hinsichtlich der Rolle der Organisation in Bezug auf ein KI-System während dessen gesamten Lebenszyklus zu melden?	A.3.3	Prozessbeschreibung für Meldung von Bedenken, anonyme Meldekanäle, Untersuchungsprotokolle	

A.4 Ressourcen für KI-Systeme

(Ziel: Sicherstellen, dass die Organisation die Ressourcen (einschließlich KI-Systemkomponenten und -Assets) des KI-Systems berücksichtigt, um Risiken und Auswirkungen vollständig zu verstehen und zu adressieren.)

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
A4.1	Hat die Organisation relevante Ressourcen identifiziert und dokumentiert, die für die Aktivitäten in bestimmten KI-System-Lebenszyklusphasen und andere KI-bezogene Aktivitäten erforderlich sind?	A.4.2	Ressourcendokumentation (z.B. Inventarlisten, Systemarchitekturen)	
A4.2	Dokumentiert die Organisation im Rahmen der Ressourcenidentifikation Informationen über die für das KI-System genutzten Datenressourcen (Herkunft, Aktualität, Kategorien, Kennzeichnungsprozess, Verwendungszweck, Qualität, Aufbewahrung, Bias-Probleme etc. gemäß B.4.3)?	A.4.3	Dokumentation der Datenressourcen, Datenmanagementpläne, Metadaten	
A4.3	Dokumentiert die Organisation im Rahmen der Ressourcenidentifikation Informationen über die für das KI-System genutzten Tooling-Ressourcen (Algorithmen, Modelle, Datenaufbereitungstools, Evaluierungsmethoden etc. gemäß B.4.4)?	A.4.4	Dokumentation der Tooling-Ressourcen, Software- und Hardwareinventare für Entwicklung/Deployment	
A4.4	Dokumentiert die Organisation im Rahmen der Ressourcenidentifikation Informationen über die für das KI-System genutzten System- und Computing-Ressourcen (Anforderungen, Standort, Verarbeitung, Auswirkungen Hardware etc. gemäß B.4.5)?	A.4.5	Dokumentation der System- und Computing-Ressourcen, Kapazitätsplanung	
A4.5	Dokumentiert die Organisation im Rahmen der Ressourcenidentifikation Informationen über die menschlichen Ressourcen und deren Kompetenzen, die für Entwicklung, Einsatz, Betrieb, Wartung etc. des KI-Systems genutzt werden (gemäß B.4.6)?	A.4.6	Kompetenzprofile, Schulungsnachweise, Rollenbeschreibungen für KI-Personal	

A.5 Bewertung der Auswirkungen von KI-Systemen

(Ziel: Auswirkungen von KI-Systemen auf Einzelpersonen oder Gruppen von Einzelpersonen oder beide sowie auf Gesellschaften, die vom KI-System während seines Lebenszyklus betroffen sind, zu bewerten.)

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
A5.1	Hat die Organisation einen Prozess etabliert, um die potenziellen Konsequenzen für Einzelpersonen, Gruppen oder beide und Gesellschaften zu bewerten, die aus dem KI-System während seines Lebenszyklus resultieren können? (Wird bereits unter 6.1.4 geprüft, hier Fokus auf Implementierung)	A.5.2	Prozessbeschreibung für KI-System-Folgenabschätzung, Kriterien für Durchführung	
A5.2	Dokumentiert die Organisation die Ergebnisse von KI-System-Folgenabschätzungen und bewahrt die Ergebnisse für einen definierten Zeitraum auf?	A.5.3	Berichte der Folgenabschätzungen, Aufbewahrungsrichtlinien	
A5.3	Bewertet und dokumentiert die Organisation die potenziellen Auswirkungen von KI-Systemen auf Einzelpersonen oder Gruppen von Einzelpersonen während des gesamten Lebenszyklus des Systems (unter Berücksichtigung von Fairness, Rechenschaftspflicht, Transparenz, Sicherheit, Datenschutz, Gesundheit, finanzielle Folgen, Zugänglichkeit, Menschenrechte gemäß B.5.4)?	A.5.4	Spezifische Folgenabschätzungsberichte für Individuen/Gruppen, Konsultation von Experten/Betroffenen	
A5.4	Bewertet und dokumentiert die Organisation die potenziellen gesellschaftlichen Auswirkungen ihrer KI-Systeme während deren gesamten Lebenszyklus (unter Berücksichtigung von Umwelt, Wirtschaft, Regierung, Gesundheit & Sicherheit, Normen & Kultur gemäß B.5.5)?	A.5.5	Spezifische Folgenabschätzungsberichte für gesellschaftliche Auswirkungen, Analyse von Missbrauchspotenzial	

A.6 KI-System-Lebenszyklus

A.6.1 Managementleitlinien für die Entwicklung von KI-Systemen

(Ziel: Sicherstellen, dass die Organisation Ziele identifiziert und dokumentiert sowie Prozesse für das verantwortungsvolle Design und die Entwicklung von KI-Systemen implementiert.)

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
A6.1	Hat die Organisation Ziele identifiziert und dokumentiert, um die verantwortungsvolle Entwicklung von KI-Systemen zu leiten, und diese Ziele berücksichtigt sowie Maßnahmen zu deren Erreichung in den Entwicklungslebenszyklus integriert? (Teilweise in 6.2 geprüft)	A.6.1.2	Dokumentierte Entwicklungsziele (z.B. Fairness, Sicherheit), Nachweis der Integration in Entwicklungsprozesse (z.B. Tests)	
A6.2	Hat die Organisation spezifische Prozesse für das verantwortungsvolle Design und die Entwicklung des KI-Systems definiert und dokumentiert (unter Berücksichtigung von Lebenszyklusphasen, Testanforderungen, menschlicher Aufsicht, Folgenabschätzungen, Trainingsdatenregeln, Expertise, Freigabekriterien, Genehmigungen, Änderungskontrolle, Usability, Einbindung Interessierter etc. gemäß B.6.1.3)?	A.6.1.3	Dokumentierte Entwicklungsprozesse, Checklisten, Vorlagen für Entwicklungsphasen	

A.6.2 KI-System-Lebenszyklus

(Ziel: Kriterien und Anforderungen für jede Phase des KI-System-Lebenszyklus definieren.)

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
A6.3	Spezifiziert und dokumentiert die Organisation Anforderungen für neue KI-Systeme oder wesentliche Erweiterungen bestehender Systeme (unter Berücksichtigung des "Warum" und "Wie" gemäß B.6.2.2)?	A.6.2.2	Anforderungsdokumente, Spezifikationen, Business Cases für KI-Systeme	
A6.4	Dokumentiert die Organisation das Design und die Entwicklung des KI-Systems basierend auf organisationalen Zielen, dokumentierten Anforderungen und Spezifikationskriterien (unter Berücksichtigung von ML-Ansatz, Algorithmus, Trainingsdatenqualität, Evaluierung, Hardware/Software, Sicherheitsaspekte, Schnittstellen, Interoperabilität etc. gemäß B.6.2.3)?	A.6.2.3	Design-Dokumente, Systemarchitekturen, Entwicklungsjournale	

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
A6.5	Definiert und dokumentiert die Organisation Verifikations- und Validierungsmaßnahmen für das KI-System und spezifiziert Kriterien für deren Anwendung (einschließlich Testmethoden, Testdatenauswahl, Freigabekriterien, Evaluierungsplan für Risiken und Ziele, Umgang mit Leistungsschwächen etc. gemäß B.6.2.4)?	A.6.2.4	Verifikations- und Validierungspläne, Testprotokolle, Evaluierungskriterien, Nachweis der Prüfung gegen Kriterien	
A6.6	Dokumentiert die Organisation einen Deployment-Plan und stellt sicher, dass angemessene Anforderungen vor dem Deployment erfüllt sind (unter Berücksichtigung unterschiedlicher Umgebungen, separater Komponenten, Freigabekriterien, Managementgenehmigungen etc. gemäß B.6.2.5)?	A.6.2.5	Deployment-Pläne, Freigabeprotokolle, Checklisten vor Deployment	
A6.7	Definiert und dokumentiert die Organisation die notwendigen Elemente für den laufenden Betrieb des KI-Systems, mindestens System- und Leistungsüberwachung, Reparaturen, Updates und Support (unter Berücksichtigung von kontinuierlichem Lernen, Konzept-/Daten-Drift, Fehlerbehandlung, Update-Prozesse, Support-SLAs, Umgang mit nicht intendierter Nutzung, KI-spezifische Sicherheitsbedrohungen etc. gemäß B.6.2.6)?	A.6.2.6	Betriebshandbücher, Monitoring-Konzepte und -Tools, Update-Verfahren, Support-Prozesse, Incident Management für KI, Leistungsmetriken und deren Überwachung	
A6.8	Bestimmt die Organisation, welche technische Dokumentation des KI-Systems für jede relevante Kategorie interessierter Parteien (Nutzer, Partner, Aufsichtsbehörden etc.) benötigt wird und stellt diese in angemessener Form bereit (einschließlich Verwendungszweck, Nutzungshinweise, technische Annahmen/Grenzen, Monitoring-Fähigkeiten, Designentscheidungen, Dateninformationen, Risikomanagement, Verifikations-/Validierungsaufzeichnungen, Änderungen, Folgenabschätzungsdoku, Fehler-Rollback-Pläne, SOPs,	A.6.2.7	Technische Dokumentation (Benutzerhandbücher, Systembeschreibungen etc.), Nachweis der Bereitstellung an definierte Parteien, Aktualität und Genehmigung der Dokumentation	

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
	Verantwortlichkeiten etc. gemäß B.6.2.7)?			
A6.9	Bestimmt die Organisation, in welchen Phasen des KI-System-Lebenszyklus die Aufzeichnung von Ereignisprotokollen aktiviert sein sollte, mindestens jedoch, wenn das KI-System in Gebrauch ist (zur Nachverfolgbarkeit, Erkennung von Leistungsabweichungen etc. gemäß B.6.2.8)?	A.6.2.8	Logging-Konzept, Beispiele für Ereignisprotokolle, Aufbewahrungsrichtlinien für Logs	

A.7 Daten für KI-Systeme

(Ziel: Sicherstellen, dass die Organisation die Rolle und Auswirkungen von Daten in KI-Systemen bei Anwendung, Entwicklung, Bereitstellung oder Nutzung von KI-Systemen während deren Lebenszyklen versteht.)

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
A7.1	Definiert, dokumentiert und implementiert die Organisation Datenmanagementprozesse im Zusammenhang mit der Entwicklung von KI-Systemen (unter Berücksichtigung von Datenschutz, Sicherheit, Transparenz, Repräsentativität, Genauigkeit etc. gemäß B.7.2)?	A.7.2	Datenmanagementplan, Datenschutz-Folgenabschätzung für Daten, Sicherheitskonzepte für Daten	
A7.2	Bestimmt und dokumentiert die Organisation Details über die Erfassung und Auswahl der in KI-Systemen verwendeten Daten (Datenkategorien, -menge, -quellen, -eigenschaften, Demografie, Vorbehandlung, Rechte, Metadaten, Herkunft etc. gemäß B.7.3)?	A.7.3	Dokumentation zur Datenerfassung und -auswahl, Verträge mit Datenlieferanten	
A7.3	Definiert und dokumentiert die Organisation Anforderungen an die Datenqualität und stellt sicher, dass die zur Entwicklung und zum Betrieb des KI-Systems verwendeten Daten diese Anforderungen erfüllen (unter Berücksichtigung von Bias, Eignung für den Zweck etc. gemäß B.7.4)?	A.7.4	Datenqualitätsrichtlinien, Messprotokolle zur Datenqualität, Verfahren zur Bias-Reduktion	
A7.4	Definiert und dokumentiert die Organisation einen Prozess zur Aufzeichnung der Herkunft (Provenance) von Daten, die in ihren KI-Systemen über die Lebenszyklen der Daten und des KI-Systems verwendet werden (einschließlich Erstellung,	A.7.5	Prozessbeschreibung Datenherkunft, Aufzeichnungen zur Datenherkunft, Verifizierungsmaßnahmen	

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
	Aktualisierung, Übertragung etc. gemäß B.7.5)?			
A7.5	Definiert und dokumentiert die Organisation ihre Kriterien für die Auswahl von Datenaufbereitungen und die zu verwendenden Datenaufbereitungsmethoden (statistische Exploration, Bereinigung, Imputation, Normalisierung, Skalierung, Kennzeichnung, Kodierung etc. gemäß B.7.6)?	A.7.6	Richtlinien zur Datenaufbereitung, Dokumentation der angewandten Methoden und deren Auswahlkriterien	

A.8 Informationen für interessierte Parteien von KI-Systemen

(Ziel: Sicherstellen, dass relevante interessierte Parteien die notwendigen Informationen haben, um die Risiken und ihre Auswirkungen (sowohl positiv als auch negativ) zu verstehen und zu bewerten.)

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
A8.1	Bestimmt und stellt die Organisation die notwendigen Informationen für Nutzer des KI-Systems bereit (einschließlich technischer Details, Anweisungen, Benachrichtigung über Interaktion mit KI, Funktionsweise, Verwendungszweck, potenzielle Schäden/Nutzen, Zugänglichkeit, Systemzweck, Interaktionshinweise, Override-Möglichkeiten, technische Anforderungen, menschliche Aufsicht, Genauigkeit/Leistung, Ergebnisse Folgenabschätzung, Revisionen von Nutzenbehauptungen, Updates, Kontaktinformationen, Schulungsmaterial etc. gemäß B.8.2)?	A.8.2	Benutzerdokumentation, Online-Hilfen, Systembenachrichtigungen, Kriterien für Informationsbereitstellung, Validierung der Zugänglichkeit und Vollständigkeit der Informationen	
A8.2	Stellt die Organisation Fähigkeiten für interessierte Parteien bereit, um nachteilige Auswirkungen des KI-Systems zu melden (z.B. Unfairness gemäß B.8.3)?	A.8.3	Meldekanäle für externe Parteien, Prozess zur Bearbeitung von Meldungen	
A8.3	Bestimmt und dokumentiert die Organisation einen Plan zur Kommunikation von Vorfällen an Nutzer des KI-Systems (unter Berücksichtigung von KI-spezifischen, Sicherheits- oder Datenschutzvorfällen, gesetzlichen/vertraglichen Anforderungen an	A.8.4	Incident-Kommunikationsplan, Integration in allgemeines Incident Management, Beispiele für Kommunikationen	

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
	Meldungstypen, Zeitrahmen, zu benachrichtigende Behörden, Detailgrad etc. gemäß B.8.4)?			
A8.4	Bestimmt und dokumentiert die Organisation ihre Verpflichtungen zur Meldung von Informationen über das KI-System an interessierte Parteien (z.B. Behörden, Kunden), einschließlich Art der Information und Zeitrahmen (technische Doku, Risiken, Ergebnisse Folgenabschätzung, Logs etc. gemäß B.8.5)?	A.8.5	Verzeichnis der Meldepflichten, Nachweis erfolgter Meldungen, Prozess zur Informationsweitergabe an Behörden	

A.9 Nutzung von KI-Systemen

(Ziel: Sicherstellen, dass die Organisation KI-Systeme verantwortungsvoll und gemäß organisationalen Politiken nutzt.)

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
A9.1	Definiert und dokumentiert die Organisation Prozesse für die verantwortungsvolle Nutzung von KI-Systemen (unter Berücksichtigung von Genehmigungen, Kosten, Beschaffungsanforderungen, gesetzlichen Anforderungen etc. gemäß B.9.2)?	A.9.2	Richtlinien zur Nutzung von KI-Systemen, Genehmigungsprozesse für KI-Einsatz	
A9.2	Identifiziert und dokumentiert die Organisation Ziele, um die verantwortungsvolle Nutzung von KI-Systemen zu leiten (Fairness, Rechenschaftspflicht, Transparenz, Erklärbarkeit, Zuverlässigkeit, Sicherheit, Robustheit, Datenschutz, Zugänglichkeit etc.) und implementiert Mechanismen zur Zielerreichung (einschließlich menschlicher Aufsicht, Überprüfung von Drittanbieterlösungen etc. gemäß B.9.3)?	A.9.3	Dokumentierte Nutzungsziele, Implementierungsnachweise (z.B. menschliche Review-Prozesse, Kriterien für automatisierte Entscheidungen, Schulung des Aufsichtspersonals, Meldung von Leistungsproblemen)	
A9.3	Stellt die Organisation sicher, dass das KI-System gemäß den beabsichtigten Nutzungen des KI-Systems und seiner Begleitdokumentation verwendet wird (einschließlich spezifischer Ressourcen, menschlicher Aufsicht, Datenausrichtung, Monitoring, Kommunikation von Bedenken, Protokollierung etc. gemäß B.9.4)?	A.9.4	Nutzungsrichtlinien, Schulungsnachweise für Anwender, Monitoring-Aufzeichnungen des KI-Einsatzes, Ereignisprotokolle zur Nutzung, Nachweis der Kommunikation bei Abweichungen	

A.10 Beziehungen zu Dritten und Kunden

(Ziel: Sicherstellen, dass die Organisation ihre Verantwortlichkeiten versteht, rechenschaftspflichtig bleibt und Risiken angemessen verteilt werden, wenn Dritte in irgendeiner Phase des KI-System-Lebenszyklus beteiligt sind.)

Nr.	Auditfrage (basierend auf Anhang A Kontrollen)	Referenz (Kapitel / Kontrolle)	Nachweis / Beobachtungen / Methoden	Konformität ((Ja/Nein / N/A / Abweichung / Anmerkung))
A10.1	Stellt die Organisation sicher, dass Verantwortlichkeiten innerhalb ihres KI-System-Lebenszyklus zwischen der Organisation, ihren Partnern, Lieferanten, Kunden und Dritten zugewiesen sind (Dokumentation aller Parteien und ihrer Rollen, ggf. Unterscheidung PII-Controller/Processor etc. gemäß B.10.2)?	A.10.2	Verantwortlichkeitsmatrix für KI-Lebenszyklus, Verträge mit Dritten, Dokumentation der Rollenverteilung (z.B. bei PII-Verarbeitung)	
A10.2	Etabliert die Organisation einen Prozess, um sicherzustellen, dass ihre Nutzung von Dienstleistungen, Produkten oder Materialien, die von Lieferanten bereitgestellt werden, mit dem Ansatz der Organisation zur verantwortungsvollen Entwicklung und Nutzung von KI-Systemen übereinstimmt (Berücksichtigung verschiedener Lieferantentypen, Risikobewertung, Anforderungen an Lieferanten, Überwachung, Integration von Komponenten, Forderung nach Korrekturmaßnahmen etc. gemäß B.10.3)?	A.10.3	Lieferantenmanagementprozess für KI, Lieferantenbewertungen, vertragliche Vereinbarungen mit KI-spezifischen Kapiteln, Prozess zur Eskalation bei Lieferantenproblemen, Anforderung und Prüfung von Lieferantendokumentation	
A10.3	Stellt die Organisation sicher, dass ihr verantwortungsvoller Ansatz zur Entwicklung und Nutzung von KI-Systemen die Erwartungen und Bedürfnisse ihrer Kunden berücksichtigt (Verständnis von Anforderungen, vertraglichen Verpflichtungen, Informationsbereitstellung über Risiken und Nutzungsgrenzen etc. gemäß B.10.4)?	A.10.4	Kundenfeedback-Analysen, Vertragsvorlagen mit KI-Kapiteln, Prozess zur Kommunikation von Nutzungseinschränkungen und Risiken an Kunden, Dokumentation bereitgestellter Informationen	