

ISO 42001

Checkliste

45 Prüfpunkte — KI-Governance, Daten, KI-Sicherheit und autonome Agenten

Eine Arbeitsliste für Organisationen, die KI einsetzen — nicht nur für die, die sich zertifizieren lassen wollen. Jeder Punkt sagt, worauf er sich stützt: auf die Norm, auf Anhang A, auf eigenständiges Recht oder auf anerkannte Praxis.

ISO/IEC 42001:2023 · Anhang A · Verordnung (EU) 2024/1689 (KI-VO) nur dort, wo sie sachlich zutrifft

45

Prüfpunkte

7

Abschnitte

4

Ebenen

SEHEN SIE SICH UNSERE SOFTWARE AN

AI Governance Suite

ein Werkzeug von **CyberWerkSuite**

cyberwerksuite.com

CyberWerkSuite

cyberwerksuite.com

Dr. Sait Yalazay

CISO · DPO · Author | CISM · CIPP · AAISM · LA 27001, 27701, 22301, 42001

Architect of Automated Compliance Systems for NIS2, GDPR, ISMS, BCM, DORA, Cloud Security (C5), Tisax & AI Act

Eine Norm ohne Frist — und Fragen, die trotzdem gestellt werden.

ISO/IEC 42001 ist freiwillig. Es gibt keine Frist, keine Aufsichtsbehörde und keine Sanktion. Gestellt werden die Fragen trotzdem: vom Kunden in der Beschaffung, vom Auditor Ihres ISMS, und von der eigenen Leitung an dem Tag, an dem ein Agent etwas getan hat, das sich nicht zurücknehmen lässt.

Die vier Ebenen

WAS HINTER JEDEM PUNKT STEHT

N — Normkapitel der ISO/IEC 42001. Verbindlich für die, die zertifiziert werden wollen.

A — Kontrolle aus Anhang A. Die Anwendbarkeit wird in der Anwendbarkeitserklärung begründet, nicht vorausgesetzt.

R — eigenständige Rechtspflicht (DSGVO, KI-VO). Gilt unabhängig von dieser Norm; 42001 begründet sie nicht und hebt sie nicht auf.

H — anerkannte Praxis und Stand der Technik. **Steht nicht in der Norm.** Aufgenommen, weil ein Auditor danach fragt und ein Angreifer sie ausnutzt.

Was diese Liste nicht ist

ABGRENZUNG

Kein Zertifizierungsaudit und keine Anwendbarkeitserklärung. Sie prüft, ob die Fragen **beantwortbar** sind — nicht, ob eine Zertifizierungsstelle die Antwort akzeptiert. Wo ein Punkt **H** trägt, ist er kein Normerfordernis; wer ihn streicht, verstößt gegen nichts.

Ein Durchgang je **KI-System**, nicht je Organisation. Ein Haus mit vier Modellen in Produktion hat vier Antworten auf dieselbe Frage — und genau dort fällt die Prüfung auseinander.

Das KI-Managementsystem

Zuerst der Rahmen: Geltungsbereich, Politik, Rollen, Inventar.

☐	1 Der Geltungsbereich des KI-Managementsystems ist schriftlich festgelegt und von der Leitung genehmigt.	N · 42001 · 4.3
☐	2 Eine von der Leitung unterzeichnete KI-Leitlinie liegt vor; sie benennt Zweck, Reichweite und Grenzen des KI-Einsatzes und ist für die Beschäftigten auffindbar.	N · 42001 · 5.2
☐	3 Rollen und Befugnisse sind zugewiesen und bekannt gemacht — einschließlich benannter Verantwortlicher für KI-Betrieb, KI-Risiko und ethische Fragen .	N · 42001 · 5.3
☐	4 Ein vollständiges KI-Inventar wird gepflegt und regelmäßig aktualisiert; für jedes System sind Zweck, Verantwortliche und Einstufung hinterlegt.	A · Anhang A.4.4
☐	5 Für die Einführung neuer KI-Systeme besteht ein definierter Genehmigungsprozess im Lebenszyklusmanagement.	A · Anhang A.6.2.2
☐	6 Es gibt einen Prozess, der nicht inventarisierte KI („Schatten-KI“) über Beschaffungs-, SaaS-, Netzwerk- und Discovery-Kontrollen erkennt und in den Geltungsbereich überführt.	H · Praxis
☐	7 Ein internes Auditprogramm für das KI-Managementsystem ist etabliert; Feststellungen werden dokumentiert und bis zur Umsetzung nachverfolgt.	N · 42001 · 9.2

Risiko und Folgenabschätzung

Was bewertet wird, womit verglichen wird, und wann neu bewertet wird.

☐	8 KI-Risikokriterien — Akzeptanzschwellen und Risikotoleranz — sind festgelegt, von der Leitung genehmigt und gepflegt.	N · 42001 · 6.1.2
☐	9 Das Risikobewertungsverfahren ist wiederholbar und bezieht Verzerrung, Erklärbarkeit, Robustheit und Sicherheit ausdrücklich ein.	N · 42001 · 6.1.4
☐	10 Der Risikobehandlungsprozess gleicht die bestimmten Maßnahmen gegen Anhang A ab, damit keine erforderliche Kontrolle ausgelassen wird.	N · 42001 · 6.1.3
☐	11 Zu jeder Anhang-A-Kontrolle ist festgehalten, ob sie angewendet wird, warum die Entscheidung so ausfiel, wie weit die Umsetzung ist und wer sie verantwortet — in einem Dokument, nicht verstreut.	N · 42001 · 6.1.3 d
☐	12 Vor dem Einsatz wird geprüft und schriftlich festgehalten, wen das System treffen kann — die einzelne betroffene Person, ganze Personengruppen, und das Umfeld außerhalb der Organisation.	N · 42001 · 8.3
☐	13 Risikobewertungen werden in geplanten Intervallen und bei wesentlichen Änderungen — Modell, Daten, Zweck, Kontext, Regulierung — erneut durchgeführt; die Auslöser sind dokumentiert.	N · 42001 · 8.2

AI Governance Suite

ein Werkzeug von **CyberWerkSuite**

AUS 45 WIRD 111

Die Liste, die Sie gerade lesen, ist der öffentliche Ausschnitt.

Im Werkzeug stehen 111 Kontrollen — jede mit Prüffrage, Anwendbarkeitsentscheidung, Begründung, Umsetzungsstatus und Verantwortlichem. Am Ende steht keine Tabelle, sondern eine Anwendbarkeitserklärung, die man vorlegen kann.

111 Kontrollen

Governance, Risiko, Daten, KI-Sicherheit, Agenten, Lieferkette — in einem Katalog statt in sechs Dateien.

SoA auf Knopfdruck

Anwendbarkeit, Begründung, Status und Verantwortlicher je Kontrolle — als Dokument, nicht als Screenshot.

Anhang-A-Abgleich

Die Risikobehandlung wird gegen Anhang A geprüft, damit keine erforderliche Kontrolle stillschweigend fehlt.

Mehrere KI-Systeme

Ein Durchgang je System, ein Gesamtbild für die Leitung.

111

Kontrollen

38

Anhang-A-Bezüge

1

SoA-Ausgabe

DE/EN

Sprachen

[AI Governance Suite ansehen](#)cyberwerksuite.com

HINWEIS

Das Werkzeug ersetzt keine Zertifizierungsstelle. Es erzeugt die Nachweise, die eine Zertifizierungsstelle sehen will.

Where Compliance Meets Automation

Daten und Datenherkunft

Woher die Daten kommen, was mit ihnen gemacht wurde, und was das Modell behalten hat.

- | | | |
|--------------------------|---|-------------------------|
| ☐ | 14 Für Entwicklungs- und Verbesserungsdaten ist geregelt, wer sie freigibt, wie ihre Qualität geprüft wird und woran auffallen würde, dass sie die Zielgruppe einseitig abbilden . | A · Anhang A.7.4 |
| ☐ | 15 Erhebung und Auswahl sind je Datensatz dokumentiert: Kategorien, Quellen, Demografie, Rechte an personenbezogenen Daten und Urheberrechten sowie die Rechtmäßigkeit von Web-Scraping . | A · Anhang A.7.3 |
| ☐ | 16 Die Datenprovenienz ist über den gesamten Lebenszyklus — Erzeugung, Aktualisierung, Übertragung — nachvollziehbar aufgezeichnet. | A · Anhang A.7.3 |
| ☐ | 17 Für die Datenaufbereitung — Bereinigung, Imputation, Normalisierung, Kodierung, Labeling — sind Kriterien festgelegt und dokumentiert. | A · Anhang A.7.6 |

Was das Modell behalten hat.

Der Teil, der erst weh tut, wenn jemand ein Auskunftersuchen stellt.

- | | | |
|--------------------------|--|----------------------|
| ☐ | 18 Produktions-Feedback- und Ground-Truth-Labeling-Pipelines sind qualitätsgesichert und gegen Poisoning geschützt, bevor sie in das Nachtraining einfließen. | H · Praxis |
| ☐ | 19 Das Modell ist auf Memorierung und Wiedergabe personenbezogener Daten getestet — Membership-Inference, Extraktion, Prompt-Recall. | H · Praxis |
| ☐ | 20 Betroffenenrechte werden — soweit technisch machbar — auch gegen Trainingsdaten und das trainierte Modell umgesetzt: Unlearning , Ausgabeunterdrückung, Nachtrainings-Auslöser. | R · DSGVO Art. 15–21 |
| ☐ | 21 Aufbewahrungsfristen für Trainingsdaten, Prompts, Ausgaben und KI-Logs sind definiert und mit automatischen Lösch- oder Überprüfungsauslösern technisch durchgesetzt . | H · Praxis |

KI-Sicherheit: Modell, Kette, Guardrails

Der Teil, den Managementsystem-Checklisten überspringen.

- | | | |
|--------------------------|---|---------------------------|
| ☐ | 22 Bevor ein KI-System gebaut oder gekauft wird, steht schriftlich, wofür es da ist , welche Daten es braucht und woran gemessen wird, ob es tut was es soll. | A · Anhang A.6.2.2 |
| ☐ | 23 Änderungen an Modell, Daten, Prompts oder Konfiguration lösen vor dem Release eine erneute Risiko- und Auswirkungsbewertung, eine Re-Validierung und eine Freigabe mit Rollback-Plan aus. | A · Anhang A.6.2.3 |
| ☐ | 24 Jede Produktions-Modellversion ist in einem Register erfasst und mit Trainingsdatenversion, Code-Commit, Hyperparametern, Metriken und Freigabe verknüpft, sodass sie reproduzierbar nachgebaut werden kann. | H · Praxis |
| ☐ | 25 Je KI-System wird eine maschinenlesbare KI-/ML-Stückliste (ML-BOM) erzeugt — Basismodelle, Datensätze, Gewichte, Adapter, Plugins, Bibliotheken samt Herkunft, Lizenz und Schwachstellenverfolgung. | H · Praxis |

Eingang, Ausgang, und was dazwischen passiert.

Vier Punkte, die in keiner Managementsystem-Checkliste stehen — und in jedem Vorfallbericht.

☐	26 Modellgewichte und -artefakte sind kryptografisch signiert mit nachprüfbarer Build-Provenienz; unsigned Artefakte werden am Deployment-Gate abgewiesen.	H · Praxis
☐	27 Es bestehen getestete Schutzmaßnahmen gegen Prompt-Injection und Jailbreaks — Eingabefilterung, System-Prompt-Härtung, Bypass-Tests.	H · Praxis
☐	28 Nicht vertrauenswürdige Inhalte aus RAG, Tools, Web, Dateien und E-Mails sind isoliert und gekennzeichnet, sodass sie nicht als Anweisungen interpretiert werden können.	H · Praxis
☐	29 Eine modellunabhängige Guardrail-Schicht moderiert Eingaben und Ausgaben, schließt im Fehlerfall sicher (fail-closed) und protokolliert Blockierungen.	H · Praxis

Zwei Regelwerke, **eine** Beratung.

KI-VO (EU) 2024/1689 und ISO/IEC 42001 — getrennt geprüft, gemeinsam umgesetzt.

CWS AI COMPLIANCE

Erst die Einstufung, dann die Pflichten, dann das Managementsystem.

- ✓ **Einstufung** Welche KI-Systeme Sie betreiben, welche Rolle Sie einnehmen — Anbieter, Betreiber, Einführer — und welche davon die KI-VO erfasst.
- ✓ **Rechtspflichten** Was unabhängig von jeder Norm gilt: Transparenz, menschliche Aufsicht, KI-Kompetenz, DSGVO-Schnittstelle.
- ✓ **Managementsystem** ISO/IEC 42001 als Trägerstruktur — Politik, Risiko, Folgenabschätzung, Anhang-A-Abgleich, SoA.
- ✓ **KI-Sicherheit** Prompt-Injection, Guardrails, Modellprovenienz, autonome Agenten.

Für Organisationen, die KI bereits einsetzen und den Nachweis nachziehen müssen.

Erstgespräch vereinbaren

cyberwerksuite.com

EBENFALLS IM PORTFOLIO

AI Governance**Suite**

KI-MANAGEMENTSYSTEM

111 Kontrollen, SoA-Ausgabe, Mehrsystembetrieb.

cyberwerksuite.com

Where Compliance Meets Automation

Autonome Agenten

Wenn das System nicht mehr antwortet, sondern handelt.

☐	30 Autonome Agenten arbeiten nach dem Least-Privilege-Prinzip mit eng begrenzten, explizit freigegebenen Tools (Allow-Lists, Deny-by-Default); jede Fähigkeit ist einzeln autorisiert.	H · Praxis
☐	31 Irreversible oder folgenschwere Agentenaktionen — Zahlungen, Löschungen, externe Kommunikation, Code-Merge oder Deploy — erfordern eine menschliche Freigabe mit vollständigem Audit-Trail.	H · Praxis
☐	32 Token-, Rechen-, Parallelitäts-, Tiefen- und Kostenkontingente sind je Mandant mit Circuit-Breakern , Agenten-Schleifenlimits und Budgetalarmen durchgesetzt.	H · Praxis
☐	33 Modellgenerierter oder agentenausgeführter Code läuft in isolierten, netzwerkbeschränkten, kurzlebigen Sandboxes mit Ressourcenlimits und ohne Zugriff auf Produktionsgeheimnisse.	H · Praxis
☐	34 Alle LLM-Ausgaben werden als nicht vertrauenswürdig behandelt und vor jeder nachgelagerten Senke — Browser, Shell, Datenbank, Code-Ausführung, Drittsysteme — kontextgerecht bereinigt bzw. kodiert.	H · Praxis
☐	35 Für KI-gestützte Entscheidungen ist eine menschliche Aufsicht eingerichtet, die tatsächlich eingreifen kann.	A · Anhang A.6.2 · AI Act Art. 14

Lieferkette und Dritte

Das fremde Modell bleibt Ihre Verantwortung.

☐	36 Ein strukturierter KI-Beschaffungsprozess mit festen Prüffragen ist implementiert und wird konsequent angewendet.	A · Anhang A.10.2
☐	37 Drittanbieter- und Basismodelle werden vor der Einführung risikobewertet — Rechtmäßigkeit der Trainingsdaten, Fähigkeiten, Einschränkungen — und auf Lizenz- und Nutzungsbedingungskonformität geprüft.	A · Anhang A.9.2
☐	38 Die Subunternehmer der KI-Anbieter entlang der KI-Lieferkette sind bekannt und werden hinsichtlich relevanter Anforderungen geprüft.	A · Anhang A.10.4
☐	39 Die Allgemeinen Geschäftsbedingungen aller eingesetzten KI-Dienste werden vor der Nutzung systematisch analysiert und bewertet.	H · Praxis
☐	40 Die Verantwortlichkeiten über den KI-Lebenszyklus sind zwischen Organisation, Partnern, Lieferanten, Kunden und Dritten zugewiesen und dokumentiert — einschließlich der Rollen Verantwortlicher/Auftragsverarbeiter .	R · DSGVO Art. 26, 28

Transparenz, Menschen und Betrieb

Wer erfährt was — und wer merkt, wenn das Modell nachlässt.

☐	41 Wer das System bedient, weiß dass es KI ist — und findet ohne Nachfragen heraus, was es kann und was es nicht kann.	A · Anhang A.8.2 · AI Act Art. 50
☐	42 Der Einsatz von KI wird gegenüber externen Stakeholdern transparent und verständlich kommuniziert.	A · Anhang A.10.4
☐	43 Betroffene Personen können Beschwerden zu KI-gestützten Entscheidungen einreichen, und dafür ist ein zugänglicher Weg vorgesehen.	A · Anhang A.8.2
☐	44 Es existiert ein vertraulicher, repressionsfreier Meldekanal für Bedenken zu KI-Systemen, der operativ funktioniert und dessen Ergebnisse in die Management-Review einfließen.	H · Praxis
☐	45 KI-Systeme werden im Betrieb laufend überwacht — insbesondere auf Abweichungen im Modellverhalten und auf nachlassende Leistung.	A · Anhang A.10.2

Woran Sie erkennen, dass diese Liste redlich ist.

Dieselben drei Regeln, nach denen wir jeden CWS-Katalog bauen.

1

Herkunft steht an jedem Punkt

Norm, Anhang A, eigenständiges Recht oder Praxis — sichtbar am Punkt selbst, nicht in einer Fußnote. Wer **H** streicht, verstößt gegen nichts. Das soll man sehen können.

2

Normtext wird nicht abgedruckt

Keine Formulierung der ISO/IEC 42001 wird wörtlich wiedergegeben. Jeder Punkt ist eine CWS-Formulierung der Prüffrage. Die Norm selbst kauft man bei Beuth/DIN Media.

3

Der Stand ist datiert

Fassung ISO/IEC 42001:2023. Bezüge zur KI-VO stehen auf dem Stand vom **20. September 2026** und nur dort, wo sie sachlich zutreffen — die Norm begründet keine Rechtspflicht.

Die 45 Punkte sind ein Ausschnitt aus 111. Der Ausschnitt ist die Auswahl, die wir in Projekten zuerst prüfen — nicht die leichteste Hälfte.

Von der Liste zum **System**.

Die Lücken haben Sie. Es fehlt die Reihenfolge.

CWS CONSULTANCY · AI GOVERNANCE

Kein Papierprojekt — gearbeitet wird an echten Systemen.

- ✓ **Standortbestimmung** Ihre KI-Systeme gegen den vollständigen Kontrollkatalog gehalten — je Kontrolle Anwendbarkeit, Begründung, Status.
- ✓ **Reihenfolge** Was zuerst, was kann warten, was ohnehin Rechtspflicht ist — mit Terminen und Aufwand, nicht mit Ampeln.
- ✓ **Umsetzung** Politik, Rollen, Inventar, Folgenabschätzung, Anhang-A-Abgleich, Guardrails — gebaut, nicht beschrieben.
- ✓ **Nachweis** Anwendbarkeitserklärung, internes Audit, Managementbewertung — vorlegbar.

Für Organisationen, die KI bereits einsetzen und den Nachweis nachziehen müssen.

Erstgespräch vereinbaren

cyberwerksuite.com

DAS WERKZEUG DAZU

AI Governance**Suite**

KI-MANAGEMENTSYSTEM

Vollständiger Kontrollkatalog, Anwendbarkeitserklärung als Dokument.

cyberwerksuite.com

Where Compliance Meets Automation