MANAGEMENTSYSTEME FÜR KÜNSTLICHE INTELLIGENZ

ISO 42001
Übersichtsleitfaden

Inhalt

Navigieren in der KI-Landschaft

Verstehen der Trends, die Technologie, Risiko und Verantwortung neu gestalten

Künstliche Intelligenz (KI) wird zunehmend in allen Branchen eingesetzt, die Informationstechnologie nutzen, und wird voraussichtlich eine der wichtigsten wirtschaftlichen Triebkräfte sein. Eine Folge dieses Trends ist, dass bestimmte Anwendungen in den kommenden Jahren zu gesellschaftlichen Herausforderungen führen können. Vom Finanzwesen über die Fertigung bis hin zum Gesundheitswesen und zur Logistik treibt die KI Fortschritte bei der Automatisierung, Effizienz und Entscheidungsfindung voran. Die weit verbreitete Einführung von generativer KI und maschinellem Lernen hat neue Möglichkeiten eröffnet, aber auch die Notwendigkeit einer stärkeren **Governance**, größerer **Transparenz** und klarerer **Verantwortlichkeit beschleunigt**.

Die globale KI-Landschaft wird von drei konvergierenden Trends geprägt:

Beschleunigte Umsetzung

Die Unternehmen arbeiten schnell daran, KI in ihre Kernprozesse einzubinden. Nach Angaben von IBM erkunden 42 % der Unternehmen bereits generative KI oder setzen sie aktiv ein. Dieses Tempo übersteigt jedoch häufig die Entwicklung formaler Governance-Strukturen, was zu Lücken in der Aufsicht, Qualitätssicherung und im Risikomanagement führt.

Die Entwicklung der Verordnung

Regierungen und Regulierungsbehörden reagieren auf die zunehmenden gesellschaftlichen Bedenken mit neuen Rahmenregelungen, die gewährleisten sollen, dass KI-Systeme sicher, fair und erklärbar sind. Das 2024 verabschiedete EU AI Act ist ein Präzedenzfall für eine risikobasierte Regulierung, und ähnliche Initiativen sind weltweit im Gange. Die Botschaft ist klar: Vertrauen in KI muss verdient werden, nicht vorausgesetzt.

Zunehmende Kontrolle und ethische Erwartungen

Von Datenschutz und geistigem Eigentum bis hin zu Voreingenommenheit und Rechenschaftspflicht: Unternehmen stehen unter dem Druck zu zeigen, dass ihr Einsatz von KI ethisch, verantwortungsvoll und sicher ist. Das öffentliche Vertrauen ist zerbrechlich – und Fehltritte können schnell zu Reputationsschäden, regulatorischen Konsequenzen und verlorenen Chancen führen.

Diese Trends signalisieren einen Wendepunkt. KI hat sich von Pilotprogrammen zu einer strategischen Infrastruktur entwickelt. Und mit diesem Wandel geht ein Bedarf an strukturierter, systemweiter Governance einher, die mit dem Ehrgeiz skalieren kann – und einer Überprüfung standhält.

Was ist ISO 42001?

Der erste internationale Managementsystemstandard für KI

ISO 42001 ist die weltweit erste KI-spezifische Managementsystemnorm, die einen strukturierten Rahmen für den verantwortungsvollen Umgang von Organisationen mit künstlicher Intelligenz bietet.

Der Standard richtet sich an Organisationen, die KI entwickeln, einsetzen oder sich auf sie verlassen. Er legt die Anforderungen für die Einrichtung, Umsetzung, Pflege und kontinuierliche Verbesserung eines Managementsystems für künstliche Intelligenz (AIMS) fest.

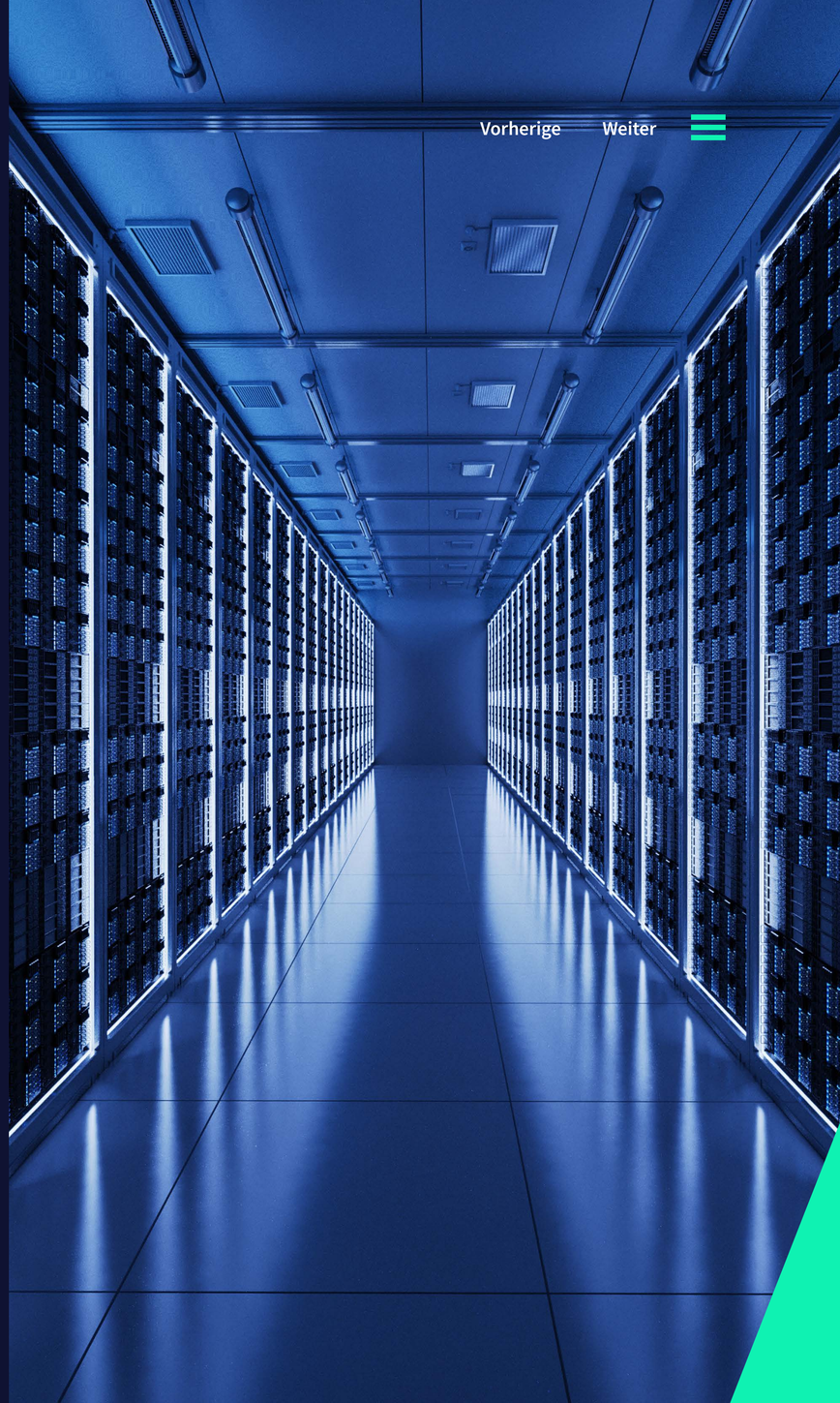
Unabhängig davon, ob Sie KI in Ihre Geschäftsabläufe integrieren oder KI-fähige Produkte und Dienstleistungen anbieten, hilft Ihnen ISO 42001 dabei, ethische Grundsätze zu verankern, Risiken zu managen und die globalen Erwartungen an vertrauenswürdige KI zu erfüllen.

Zu den wichtigsten Elementen der Norm gehören:

- **Governance und Rechenschaftspflicht** – Festlegung von Rollen, Zuständigkeiten und Aufsicht für KI-bezogene Aktivitäten
- **Risikobasierte Kontrollen** – Identifizierung und Behandlung von Risiken während des gesamten Lebenszyklus des KI-Systems
- **Transparenz und Erklärbarkeit** – Unterstützung einer klaren Kommunikation darüber, wie KI-Systeme funktionieren und Entscheidungen treffen
- **Kontinuierliche Verbesserung** – Nutzung von Feedback, Überwachung und Leistungsdaten, um Ihre AIMS im Laufe der Zeit zu verbessern

Die ISO 42001 folgt der Struktur des Anhangs SL, so dass sie leicht in andere Normen wie ISO 9001, ISO 27001 oder ISO 45001 integriert werden kann, was einen konsistenten und harmonisierten Ansatz für das Risikomanagement in Ihrer Organisation ermöglicht.

Durch die Übernahme von ISO 42001 können Organisationen ein klares Bekenntnis zu verantwortungsvoller Innovation demonstrieren und so in einer zunehmend von KI geprägten Welt Vertrauen bei Kunden, Partnern und Regulierungsbehörden schaffen.



Warum sich zertifizieren lassen?

Die Zertifizierung nach ISO 42001 ist mehr als eine Formalität. Sie ist ein unabhängiges, weltweit anerkanntes Prüfzeichen, das sicherstellt, dass Ihre Organisation verantwortungsvoll und effektiv mit künstlicher Intelligenz umgeht.

Zeigt Engagement für bewährte Verfahren
Die Zertifizierung signalisiert, dass Sie es mit dem Aufbau ethischer, transparenter und gut geführter KI-Systeme ernst meinen – im Einklang mit den internationalen Erwartungen.

Aufbau von Vertrauen und Glaubwürdigkeit bei den Kunden
Für viele Branchen wird die Zertifizierung zu einer Lizenz zum Handeln. Sie gibt Kunden, Partnern und Interessengruppen die Gewissheit, dass Ihre KI-Praktiken sicher, verantwortungsbewusst und gut verwaltet sind.

Unterstützung der Ziele in den Bereichen Datenschutz, Ethik und Informationssicherheit
Der Zertifizierungsprozess hilft Ihnen dabei, die KI-Governance in Ihre umfassenderen Risikomanagementsysteme einzubetten und so den Datenschutz, die verantwortungsvolle Innovation und die ethische Aufsicht zu stärken.

Zukunftssicherheit für Ihre Compliance
Zunehmende Prüfung und ethische Erwartungen Von Datenschutz und geistigem Eigentum bis hin zu Vorurteilen und Verantwortlichkeit stehen Unternehmen unter Druck, nachzuweisen, dass ihre Nutzung von KI ethisch, verantwortungsbewusst und sicher ist. Öffentliches Vertrauen ist fragil – und Fehltritte können schnell zu Reputationsschäden, regulatorischen Konsequenzen und verpassten Chancen führen. Diese Trends markieren einen Wendepunkt. KI ist von Pilotprogrammen zu strategischer Infrastruktur aufgestiegen. Und mit diesem Wandel wächst der Bedarf an strukturierter, systemweiter Governance, die mit den Ambitionen skaliert – und der Prüfung standhält.

Die wichtigsten Anforderungen der ISO 42001:

Anhang SL Kapitelstruktur

Die Struktur des ISO-Anhangs SL besteht aus zehn Abschnitten. Der gesamte Inhalt einer Managementsystemnorm, einschließlich ISO 42001, muss die Kriterien aller zehn Abschnitte erfüllen, um dem Rahmen des Anhangs SL zu entsprechen. Die Kapitel sind in folgende Kategorien eingeteilt:

Kapitel 1
Umfang

Definiert die beabsichtigten Ergebnisse des AI-Management systems und seine Anwendbarkeit innerhalb der Organisation.

Kapitel 2
Normative Referenzen

Listet referenzierte Normen auf, die für die Anwendung von ISO 42001 wesentlich sind.

Kapitel 3
Begriffe und Definitionen

Enthält Definitionen der wichtigsten Begriffe, die in der Norm verwendet werden, um ein gemeinsames Verständnis zu gewährleisten.

Kapitel 4
Kontext der Organisation

Berücksichtigt interne und externe Faktoren, die Erwartungen der Stakeholder und den Umfang der Nutzung des KI-Systems.

Kapitel 5
Leiterschaft

Umreißt die Verantwortung der obersten Führungsebene für Politik, Ressourcen und die Förderung einer verantwortungsvollen KI-Kultur.

Kapitel 6
Planung

Es geht darum, wie die Organisation KI-Risiken und -Chancen identifiziert und darauf reagiert und KI-Ziele festlegt.

Kapitel 7
Unterstützung

Umfasst die Ressourcen, die Kompetenz, das Bewusstsein, die Kommunikation und die Dokumentation, die für eine wirksame Governance erforderlich sind.

Kapitel 8
Operation

Legt fest, wie KI-bezogene Kontrollen implementiert werden, einschließlich Risikobewertungen und Bewertungen der Systemauswirkungen.

Kapitel 9
Leistungsbewertung

Erfordert Überwachung, Messung, interne Audits und Managementprüfung zur Bewertung der Systemleistung.

Kapitel 10
Verbesserung

Erläutert den Ansatz der Organisation zur kontinuierlichen Verbesserung, zum Umgang mit Nichtkonformität und zu Korrekturmaßnahmen.

In den meisten Fällen verwenden diese Kapitel den gleichen Kerntext, unabhängig von der Norm, auf die sie angewendet werden, und haben gemeinsame Begriffe und Definitionen, um die Konsistenz und Kompatibilität zwischen den Managementsystemnormen zu fördern. Bei der ISO 42001-Norm gewährleistet dies, dass die AI-Governance in eine vertraute und bewährte Managementsystemstruktur eingebettet ist.

Berücksichtigung der Anforderungen von ISO 42001 im Kontext von AI

Wie andere ISO-Normen für Managementsysteme besteht auch die ISO 42001 aus den Abschnitten 4 bis 10, die Bereiche wie Kontext, Führung, Planung, Unterstützung und kontinuierliche Verbesserung abdecken. Was die ISO 42001 einzigartig macht, ist die Art und Weise, wie diese vertrauten Konzepte auf die Herausforderungen und Risiken im Zusammenhang mit künstlicher Intelligenz zugeschnitten sind.

In den folgenden Abschnitten wird zusammengefasst, wie die Kapitel im Zusammenhang mit KI gelten – von ethischer Governance und Datentransparenz bis hin zu Risikomanagement und Lebenszyklusüberwachung.

Kontext der Organisation

ISO 42001 fordert Organisationen auf, den Umfang ihres KI-Managementsystems zu definieren, indem sie ihren internen und externen Kontext verstehen. Dazu gehören rechtliche Verpflichtungen, branchenspezifische KI-Risiken, kulturelle und ethische Normen, Erwartungen der Stakeholder und die Rolle der Organisation im KI-Lebenszyklus – ob als Entwickler, Anwender oder Nutzer. Diese Erkenntnisse bestimmen die Art und Weise, wie KI gesteuert wird, und helfen dabei, die relevanten Kontrollen zu bestimmen. Die Unternehmen sollten auch prüfen, ob ihr Ansatz von allgemeineren gesellschaftlichen Fragen wie dem Klimawandel oder der digitalen Gerechtigkeit beeinflusst werden sollte.

Leadership und Governance

Eine Kernanforderung der ISO 42001 ist ein sichtbares und nachhaltiges Engagement der Unternehmensleitung für einen verantwortungsvollen Umgang mit KI. Die Unternehmensleitung muss eine klare KI-Politik festlegen, Ziele setzen, die mit den Unternehmenswerten übereinstimmen, und sicherstellen, dass die Rollen und Verantwortlichkeiten über den gesamten KI-Lebenszyklus hinweg definiert sind. Dazu gehört auch die Beaufsichtigung von Risikobewertungen, Folgenabschätzungen und dem Einsatz von KI, insbesondere in sensiblen oder risikoreichen Kontexten. Ein aktives Engagement der Unternehmensspitze trägt dazu bei, dass die Governance im gesamten Unternehmen verankert ist und nicht nur als nachträglicher Gedanke behandelt wird.

Ethik und Transparenz

Ethische Überlegungen sind durchgängig eingebettet ISO 42001. Organisationen müssen nachweisen, wie sie die potenziellen Auswirkungen von KI auf den Einzelnen und die Gesellschaft bewerten und behandeln. Dies beinhaltet die Berücksichtigung von Fairness, Nichtdiskriminierung und menschlicher Autonomie sowie den Datenschutz und die Transparenz der Ergebnisse. Es müssen Kontrollen vorhanden sein, um unbeabsichtigte Folgen zu erkennen und abzumildern, und die Nachweise für diese Praktiken müssen dokumentiert, überwacht und regelmäßig aktualisiert werden.

Risiko- und Chancenmanagement

Organisationen müssen KI-spezifische Risiken bewerten und behandeln – einschließlich solcher, die sich auf die Einhaltung von Vorschriften, den Ruf und die Sicherheit auswirken – und gleichzeitig Chancen für Innovationen und Verbesserungen erkennen. ISO 42001 erkennt an, dass die Risikobereitschaft und die Definitionen je nach Branche variieren können, so dass der Rahmen anpassbar ist. Wichtig ist, dass Entscheidungen bewusst getroffen werden, sich an Richtlinien orientieren und im Laufe der Zeit auf ihre Wirksamkeit hin überprüft werden.

Kontinuierliche Verbesserung

ISO 42001 folgt dem PDCA-Modell (Plan-Do-Check-Act). Das bedeutet, dass kontinuierliche Verbesserung nicht optional ist, sondern fest verankert ist. Organisationen müssen die Leistung ihres KI-Systems überwachen, interne Audits durchführen und die Governance-Prozesse regelmäßig überprüfen. Ganz gleich, ob es sich um eine Korrekturmaßnahme oder eine Anpassung an regulatorische Änderungen handelt, das Ziel besteht darin, die Eignung, Angemessenheit und Wirksamkeit des KI-Management systems ständig zu verbessern.

ISO 42001 Anhang A Kontrollen

Verantwortungsvolle KI in die Tat umsetzen

Zusätzlich zu den 10 Hauptkapitel enthält ISO 42001 eine Reihe von unterstützenden Kontrollzielen in Anhang A. Diese Kontrollen sollen Organisationen bei der Umsetzung praktischer, überprüfbarer Maßnahmen helfen, die eine vertrauenswürdige Entwicklung und Nutzung von KI unterstützen.

Die Kontrollen in Anhang A sind in 10 Kategorien unterteilt:

- **Politik in Bezug auf KI** – Gewährleistung einer klaren Absicht und Ausrichtung der Führung
- **Interne Organisation** – Festlegung von Führungsaufgaben und Zuständigkeiten
- **Ressourcen** – Verwaltung der in der KI verwendeten Tools, Daten und Infrastruktur
- **Folgenabschätzungen** – Bewertung der Risiken für den Einzelnen und die Gesellschaft
- **Aufsicht über den Lebenszyklus** – Abstimmung des Systemdesigns auf ethische und regulatorische Ziele
- **Daten für KI-Systeme** – Qualität, Herkunft und Relevanz sicherstellen
- **Informationen für interessierte Parteien** – Förderung von Transparenz und Verantwortlichkeit
- **Nutzung von KI-Systemen** – Verwaltung von Umfang, Absicht und Schutzmaßnahmen
- **Beziehungen zu Dritten** – Festlegung von Erwartungen an Lieferanten und Partner
- **Dokumentation und Rückverfolgbarkeit** – zur Unterstützung der Erklärbarkeit und Nachvollziehbarkeit

Diese Kontrollbereiche bilden die praktische Grundlage für die Umsetzung von ISO 42001. Sie können an die verschiedenen Reifegrade und die Komplexität von KI angepasst werden und sind ein wichtiger Bestandteil von Bereitschaftsbewertungen und Zertifizierungen.

Umsetzung von ISO 42001

Schwerpunktbereiche für die Operationalisierung Ihres AI-Management-Systems

ISO 42001 bietet einen Rahmen für die Umsetzung verantwortungsvoller und effektiver AI-Managementpraktiken unter Verwendung des PDCA-Modells (Plan-Do-Check-Act) – eine zentrale Grundlage für alle auf Annex SL basierenden ISO-Normen.

Der Standard unterstützt die Entwicklung eines Managementsystems für künstliche Intelligenz (Artificial Intelligence Management System, AIMS) durch miteinander verknüpfte Managementprozesse, einschließlich:

- **Bewusstseinsbildung**

  Unternehmen sollten ihr Bewusstsein schärfen, indem sie ihre Teams schulen, um die Vorteile, Risiken und ethischen Überlegungen der KI zu verstehen – von den Entwicklern bis zu den Entscheidungsträgern.

- **Verantwortung**

  Es müssen klar definierte Rollen und Verantwortlichkeiten zugewiesen werden, um sicherzustellen, dass die KI-Governance über den gesamten Systemlebenszyklus hinweg verstanden und verankert wird

- **Antwort**

  Es sollte rechtzeitig und koordiniert gehandelt werden, um Risiken zu bewältigen, auf die Auswirkungen des KI-Systems zu reagieren und bei Bedarf Korrekturmaßnahmen zu ergreifen.

- **Risikobewertung**

  Die mit KI-Systemen verbundenen Risiken – einschließlich technischem Versagen, unbeabsichtigten Ergebnissen oder Missbrauch – müssen auf strukturierte, evidenzbasierte Weise bewertet werden.

- **Systementwurf und -entwicklung**

  KI-Systeme müssen im Einklang mit dokumentierten Richtlinien und Prozessen entwickelt und eingesetzt werden, die eine ethische Nutzung, Transparenz und Rechenschaftspflicht während des gesamten Lebenszyklus unterstützen.

- **Governance und Kontrolle**

  Unternehmen sollten bei der Verwaltung von KI einen ganzheitlichen Ansatz verfolgen, der Datenqualität, Erklärbarkeit, Fairness, Zuverlässigkeit und menschliche Kontrolle umfasst.

- **Neubewertung und kontinuierliche Verbesserung**

  Im Rahmen des PDCA-Modells sollte die Leistung regelmäßig überwacht und überprüft werden. Interne Audits und Management-Reviews tragen dazu bei, dass das AIMS weiterhin die Ziele erreicht und sich an neue Risiken und Vorschriften anpasst.

Erstellen Sie Ihren Fahrplan mit ISO 42001

Schaffung der Grundlagen für eine wirksame KI-Governance

Die Umsetzung von ISO 42001 beginnt mit einer klaren Zielsetzung und einer starken Unterstützung durch die Führung. Diese ersten Schritte tragen dazu bei, dass Ihr KI-Managementsystem (AIMS) sowohl praktisch als auch auf die Ziele Ihrer Organisation abgestimmt ist.

1. Engagement von Führungskräften gewinnen

Die Geschäftsleitung muss die AIMS anführen und klare Ziele festlegen, die definieren, wie der Erfolg für Ihr Unternehmen aussieht. Ganz gleich, ob es darum geht, die Aufsicht zu verbessern, die Erwartungen der Aufsichtsbehörden zu erfüllen oder Vertrauen aufzubauen – die Führung sollte die Ressourcen und die Richtung vorgeben, die erforderlich sind, um den verantwortungsvollen Einsatz von KI im gesamten Unternehmen zu verankern.

2. Verstehen Sie Ihren AI-Kontext

Bewerten Sie, wie KI in Ihrem Unternehmen entwickelt, eingesetzt oder genutzt wird. Berücksichtigen Sie rechtliche Verpflichtungen, branchenspezifische Risiken und die Erwartungen der Stakeholder. Diese Erkenntnisse sollten in Ihre Ressourcenplanung einfließen – einschließlich der Zeit, der Fähigkeiten und des Budgets, die für einen verantwortungsvollen und effektiven Umgang mit KI erforderlich sind.

3. Bewertung des Schulungsbedarfs

KI-Governance umfasst technische, ethische, rechtliche und operative Bereiche. Binden Sie funktionsübergreifende Teams ein und sorgen Sie für maßgeschneiderte Schulungen – von der Sensibilisierung breiterer Teams bis hin zu Audit-Schulungen für Spezialisten. Der Aufbau von Fähigkeiten über alle Rollen hinweg ist der Schlüssel zu einer effektiven, skalierbaren Implementierung.

4. Definieren Sie den AIMS-Anwendungsbereich

Klären Sie, welche Teams, Systeme und geografischen Standorte Ihr AIMS abdecken soll – einschließlich intern entwickelter KI, Tools von Drittanbietern und risikoreicher Anwendungsfälle. Ein klar definierter Geltungsbereich sorgt dafür, dass Ihre Governance zielgerichtet und zweckmäßig ist.

5. Ihre AIMS planen und umsetzen

Entwicklung eines realistischen Umsetzungsplans, der den Zeitplan, die Zuständigkeiten und die erforderlichen Ressourcen umfasst. Führen Sie die notwendigen Kontrollen, Dokumentationen und Governance-Prozesse ein. Planen Sie regelmäßige Überprüfungen, Feedbackschleifen und Leistungsüberwachung ein, um sicherzustellen, dass sich Ihr AIMS mit Ihrem Unternehmen und der KI-Landschaft weiterentwickelt.

6. Durchführung einer Gap-Analyse

Überprüfen Sie Ihre derzeitigen Governance-, Risiko- und Compliance-Rahmenbedingungen, um festzustellen, wo Ihre Organisation den Standard bereits erfüllt – und wo Lücken oder Schwachstellen bestehen. Anhand dieser Erkenntnisse lassen sich Prioritäten für Verbesserungen setzen und Doppelarbeit vermeiden.

7. Buchen Sie Ihr Zertifizierungsaudit

Sobald Ihr AIMS eingerichtet ist, planen Sie Ihr ISO 42001-Zertifizierungsaudit mit LRQA. Unser zweistufiger Prozess wird Ihr Systemdesign und Ihre Implementierung bewerten und Ihnen helfen, Ihren Stakeholdern gegenüber Verantwortlichkeit, Integrität und verantwortungsvolle Innovation zu demonstrieren.

8. Kontinuierliche Verbesserung einbetten und Reaktion

Ein ausgereiftes AIMS umfasst mehr als die anfängliche Umsetzung – es erfordert Mechanismen für kontinuierliches Lernen und Verbesserung. Führen Sie Feedbackschleifen, regelmäßige Audits und Leistungsmetriken ein, um sich an die sich entwickelnden KI-Risiken und -Technologien anzupassen. Implementieren Sie einen KI-spezifischen Reaktionsplan für Vorfälle, um sicherzustellen, dass auf Fehler, Verzerrungen oder Systemausfälle schnell, transparent und effektiv reagiert wird.

Integration von ISO 42001 in bestehende Managementsysteme

Bauen Sie auf dem auf, was bereits funktioniert. Verstärken Sie Ihre Governance in den Bereichen KI und Informationssicherheit.

Für viele Organisationen ist ISO 42001 kein Ausgangspunkt – es ist eine natürliche Erweiterung. Wenn Sie bereits nach ISO 27001 zertifiziert sind, sind Sie in einer guten Position, um ISO 42001 effizient und effektiv zu integrieren.

ISO 27001 bietet ein bewährtes Rahmenwerk für das Management von Informationssicherheitsrisiken, und die darin enthaltenen Kontrollmechanismen für die Vertraulichkeit, Integrität und Verfügbarkeit von Daten unterstützen direkt viele der Anforderungen von ISO 42001. Durch die Kombination der beiden Normen können Sie einen einheitlichen Governance-Ansatz schaffen, der sowohl Ihre Informations- als auch Ihre KI-bezogenen Risiken berücksichtigt.

Warum Integration sinnvoll ist

Gemeinsame Struktur

ISO 42001 folgt dem Annex SL-Rahmen – der gleichen übergeordneten Struktur, die auch in ISO 27001, ISO 9001, ISO 45001 und anderen verwendet wird. Dies ermöglicht Konsistenz in den Bereichen Politik, Führung, Planung, Betrieb und Bewertung.

Effiziente Ressourcennutzung

Die Integration trägt dazu bei, Doppelarbeit bei Audits, Dokumentation und internen Überprüfungen zu vermeiden. Teams können Berichte, Ziele und Kontrollen aufeinander abstimmen und so die Einhaltung von Vorschriften optimieren und die Aufsicht verbessern.

Abgestimmtes Risikomanagement

Beide Normen erfordern einen risikobasierten Ansatz. Während sich ISO 27001 auf Informationsgüter konzentriert, erweitert ISO 42001 diesen Ansatz auf KI-Systeme – einschließlich der Art und Weise, wie Daten für deren Training, Validierung und Betrieb verwendet werden.

Stärkere Widerstandsfähigkeit des Systems

Ein integrierter Ansatz macht es einfacher, systemische Probleme zu erkennen, sie ganzheitlich zu lösen und Kunden, Aufsichtsbehörden und Partnern gegenüber ein gemeinsames Governance-Modell zu demonstrieren.

Unsere ISO 42001-Dienstleistungen

Ausbildung

Erweitern Sie Ihr Wissen über die ISO 42001-Norm mit einer Reihe von Kursen, die für unterschiedliche Erfahrungsstufen konzipiert sind und in verschiedenen Lernformen angeboten werden.

Gap-Analyse

Ein optionaler Service, bei dem einer unserer fachkundigen Auditoren Ihnen hilft, kritische, risikoreiche oder schwache Bereiche Ihres Systems vor der Zertifizierung zu identifizieren.

Zertifizierung

Wir bewerten Ihr AI-Management-System (AIMS) gemäß den Anforderungen der ISO 42001.

Integrierte Bewertungen

Wenn Sie mehrere Managementsysteme eingeführt haben, könnten Sie von einem integrierten Audit- und Überwachungsprogramm profitieren – eine effizientere und kostengünstigere Art des Risikomanagements.

Verfügbare Kurse anzeigen

Warum mit uns arbeiten?

LRQA unterstützt Unternehmen bei der Entwicklung robuster, zukunftsfähiger Risikomanagementprogramme, die eine sichere, verantwortungsvolle und effektive Einführung von KI und Technologie ermöglichen.

Von der Sicherstellung der Einhaltung der sich entwickelnden KI-Vorschriften bis hin zur Stärkung der Datensicherheit und der Einbettung von Best Practices in die Governance bieten wir die Sicherheit, die erforderlich ist, um Innovationen mit Zuversicht voranzutreiben – und helfen Unternehmen, KI und Technologie zu integrieren und gleichzeitig Risiken proaktiv zu managen.

Fachwissen vor Ort

Unsere Lösungen werden von einem globalen Expertenteam bereitgestellt, das sich auf Cybersicherheit, Compliance und Risikomanagement in der Lieferkette spezialisiert hat. Sie helfen Ihnen dabei, KI-bezogene Risiken zu navigieren, die sich entwickelnden regulatorischen Anforderungen zu erfüllen und verantwortungsvolle KI-Praktiken in Ihren Betrieb zu integrieren.

Kontinuierliche Sicherung

KI-gesteuerte Risiken erfordern eine kontinuierliche Überwachung. Unser Ansatz für das Risikomanagement in Echtzeit ermöglicht eine proaktive Problemlösung, die Geschäftsunterbrechungen reduziert und die Widerstandsfähigkeit erhöht. Unser vernetztes Lösungsportfolio für das Risikomanagement hilft Unternehmen, über die regulatorischen Anforderungen hinauszugehen und das KI-Risikomanagement in das Tagesgeschäft zu integrieren.

Lösungsorientierte Partnerschaften

Wir zertifizieren nicht nur – wir arbeiten mit Ihnen zusammen, um die KI-Governance in Ihre breitere Risiko- und Compliance-Strategie zu integrieren. Unser maßgeschneiderter Ansatz stellt sicher, dass KI und Technologie zu nachhaltigem Wachstum beitragen und gleichzeitig die sich entwickelnden rechtlichen und ethischen Erwartungen erfüllen.

Datengesteuerte Entscheidungsfindung

Wir nutzen digitale Plattformen und Analysen, um tiefere Einblicke in KI-Risiken in Ihrem Unternehmen zu gewinnen. Unsere menschliche Intelligenz, die durch datengesteuerte Tools ergänzt wird, hilft Unternehmen, Schwachstellen zu erkennen, zukünftige Risiken vorherzusagen und fundierte Entscheidungen zu treffen.

Über LRQA

LRQA ist einer der führenden globalen Partner, der seit Jahrzehnten unübertroffenes Fachwissen in den Bereichen Begutachtung, Beratung, Inspektion und Cybersicherheitsdienstleistungen zusammenbringt.

Unsere lösungsbasierten Partnerschaften werden durch datengestützte Erkenntnisse unterstützt, die unseren Kunden helfen, ihre größten geschäftlichen Herausforderungen zu lösen. Die preisgekrönten Compliance-, Lieferketten-, Cybersicherheits- und ESG-Spezialisten von LRQA sind in mehr als 150 Ländern mit einem Team von mehr als 5.000 Mitarbeitern tätig und helfen mehr als 61.000 Kunden in fast allen Branchen, Risiken zu antizipieren, zu mindern und zu managen, wo immer sie tätig sind.

Bei allem, was wir tun, setzen wir uns dafür ein, eine bessere Zukunft für unsere Mitarbeitenden, unsere Kunden, unsere Gemeinden und unseren Planeten zu gestalten.

Kontakt aufnehmen

Kontaktieren Sie uns Besuchen Sie **lrqa.com/de-de** für weitere Informationen oder senden Sie eine E-Mail an **info.de@lrqa.com**

LRQA Deutschland GmbH
Bonner Str. 12
51379 Leverkusen
Deutschland