

Halderstone



Trainingsmodul

Steuerung von KI-Lebenszyklus & Data Governance auditieren

Steuerungsmassnahmen im KI-Lebenszyklus und in der Data Governance von Beschaffung bis Überwachung und Änderungen bewerten



Führt Ihr Audit über Papier hinaus hin zu belastbaren Nachweisen über den Lebenszyklus?

Überblick

Ein Audit eines KI-Managementsystems wird unzuverlässig, wenn Nachweise über den Lebenszyklus fragmentiert sind: Die Herkunft der Daten ist unklar, Entscheidungen zu Training und Validierung sind nicht reproduzierbar, Bereitstellungen umgehen die Änderungssteuerung, und die Überwachung erkennt keine Drift. In der Praxis entsteht so Scheinsicherheit: Steuerungsmassnahmen sind vorhanden, regeln aber nicht, was über den KI-Lebenszyklus tatsächlich geschieht.

Dieses normbezogene Auditmodul zeigt, wie Steuerungsmassnahmen für den Lebenszyklus und die Data Governance im Kontext von ISO/IEC 42001 zu auditieren sind: worauf zu achten ist, wo Nachweise typischerweise liegen, wie sich Lebenszyklusphasen verbinden lassen und wie die Wirksamkeit unter Veränderung zu beurteilen ist. Es ist so angelegt, dass es im Auditorenpfad zu ISO/IEC 42001 eigenständig funktioniert. Allgemeine Auditmethodik und allgemeine Methoden für Managementsysteme werden vorausgesetzt und nur kurz referenziert.



Zielgruppe

- Auditinteressierte, die KI-Managementsysteme gemäss ISO/IEC 42001 nach bewährten Praktiken auditieren wollen
- Praktizierende Auditfachleute für ISO/IEC 42001, die ihr Auditwissen, ihr Urteilsvermögen und ihre Wirksamkeit stärken wollen

Ist dieses Modul für Sie das Richtige?

Es passt gut für Sie, wenn Sie...

- beurteilen möchten, ob Steuerungsmassnahmen zum KI-Lebenszyklus über reale Systemänderungen hinweg funktionieren.
- die Herkunftsnachweise, Training und Validierung beurteilen wollen.
- die Rückverfolgbarkeit von der Datenbeschaffung bis zu Bereitstellung und Überwachung in den Fokus stellen.
- Änderungssteuerung und Drifterkennung in der Praxis auditieren möchten.
- Ihre Auditschlussfolgerungen zur Wirksamkeit von KI-Steuerungsmassnahmen stärken möchten.

Es passt möglicherweise weniger gut für Sie, wenn Sie...

- KI-Governance-Rahmen oder Lebenszyklusprozesse entwerfen möchten.
- Hinweise zur Modellentwicklung oder Datenentwicklung suchen.
- sich vor allem auf das KI-Risikomanagement oder ethische Designaktivitäten konzentrieren.
- nicht vorhaben, Steuerungsmassnahmen zum KI-Lebenszyklus nach ISO/IEC 42001 zu auditieren.

Lernergebnisse

Zentrale Lernergebnisse

- KI-Systeme von der Datenbeschaffung über Training, Validierung, Bereitstellung und Überwachung entlang von Nachweiswegen über den Lebenszyklus nachverfolgen
- Nachweisquellen je Lebenszyklusphase erkennen und beurteilen, ob sie stimmig, vollständig und nutzbar sind
- Die Wirksamkeit von Steuerungsmassnahmen unter Veränderung beurteilen (Versionen, Datenaktualisierungen, Konfigurationsänderungen und operative Drift)

Zusätzliche Fähigkeiten

- Einzelne Steuerungsmängel von systemischen Schwächen in Governance und Lebenszyklussteuerung unterscheiden
- Typische Schwachstellen in den Steuerungsmassnahmen für Lebenszyklus und Data Governance erkennen, die zu Scheinsicherheit in KI-Kontrollen führen
- Eine belastbare Auditschlussfolgerung dazu formulieren, ob Aufsichtsmechanismen über den gesamten Lebenszyklus wie vorgesehen funktionieren

Agenda

Audit des KI-Lebenszyklus in der Praxis

Wie Lebenszyklusphasen als Nachweiswege statt als Übung zur Prozessgestaltung betrachtet werden, mit Fokus auf Angemessenheit und Wirksamkeit der Steuerungsmassnahmen über alle Phasen hinweg

Steuerungsmassnahmen für Datenbeschaffung und Herkunftsnachweis

Wie Nachweise zu Beschaffung, Rechten, Einschränkungen, Rückverfolgbarkeit und Qualitätskontrollen beurteilt werden; Warnsignale sind unklare Herkunft, unkontrollierte Drittanbieterdaten und unbekannte Weiterverwendung

Steuerungsmassnahmen für Training und Validierung

Wie Nachweise zu Datensatzauswahl, Reproduzierbarkeit, Ergebnissen und Freigaben beurteilt werden; typische Schwachstellen sind unkontrollierte Experimente, inkonsistente Validierung und undokumentierte Modellauswahl

Bereitstellung und Änderungssteuerung

Wie Nachweise zu Freigabeentscheidungen, Versionierung, Rollbackfähigkeit und Funktionstrennung beurteilt werden; besondere Aufmerksamkeit ist nötig, wenn Modelle oder Plattformen extern betrieben werden

Überwachung, Drift und operative Aufsicht

Wie nachgewiesen wird, dass Zweck und Überwachung zum Betrieb passen, einschliesslich Alarmen, Vorfällen und Korrekturmassnahmen; Driftmuster umfassen Datendrift, Leistungsdrift und stille Veränderungen im Umfeld

Nachweise zu Governance und Verantwortlichkeit über den Lebenszyklus

Wie Entscheidungsaufzeichnungen zeigen, wer was auf Basis welcher Nachweise und Einschränkungen freigegeben hat, samt Aufsichtsmechanismen für Ausnahmen, Notfalländerungen und offene Punkte

Praxisworkshop mit Auditsimulation

Anwendung der erlernten Konzepte, Methoden und Ansätze in einem realistischen Praxisfall

Enthaltene Unterlagen

Lernunterlagen

- Foliensatz
- Workbook für Teilnehmende

Vorlagen & Werkzeuge

- Tool für die Planung von Auditgesprächen
- Checkliste für dokumentierte Informationen
- Stichprobentool
- Arbeitsblätter für Auditanalyse
- Sammlung typischer Schwachstellen
- KI-Prompt-Sammlung

Bestätigung

- Teilnahmebestätigung

Vorbereitungshinweise

Vorausgesetzter Hintergrund

Dieses Modul setzt voraus, dass Auditoren bereits in einem Auditauftrag arbeiten und nachweisbasiert urteilen können. Es setzt ausserdem grundlegende KI-Lebenszykluskenntnisse voraus, etwa zu typischen Artefakten, Versionierungskonzepten und dazu, was Drift im Betrieb bedeutet.

Hilfreicher Hintergrund umfasst:

- Nachweiskette, Stichprobenurteil und Denken in Angemessenheit versus Wirksamkeit
- Vertrautheit damit, wie dokumentierte Informationen strukturiert sind und als Auditnachweis genutzt werden
- Grundverständnis von Artefakten im KI-Lebenszyklus (Datenquellen, Trainingsläufe, Bewertungsergebnisse, Bereitstellungsversionen, Überwachungsausgaben)

Vorbereitungsmodule

Grundlagen (je nach Vorwissen)

Hilfreich, wenn Sie mit den zugrunde liegenden Konzepten noch wenig vertraut sind

- Audit-Grundsätze
- KI-Systeme & Architekturen

Unterstützend (optional)

Hilfreich, aber nicht erforderlich, um wirksam teilnehmen zu können

- Betriebliche Steuerung auditieren
- Grenzen & Fehlermodi von KI

Organisatorisches

Verfügbare Sprachen

- Englisch
- Deutsch

Durchführung - Standard

- Virtueller Live-Unterricht
- Blended Learning (E-Learning + Live)

Durchführung - individuell

- Vor-Ort-Durchführung bei Ihnen
- Inhalte angepasst an Ihre Organisation



Halderstone

Halderstone by Langer & Co

Zürcherstrasse 2

CH-8852 Altendorf

Schweiz

info@halderstone.com

www.halderstone.com