

## ***AI135 KI-Auditor gemäß ISO/IEC 42001, VDE SPEC 90012, TÜV AI.AM***

### **Kurzbeschreibung:**

Teilnehmende erhalten eine praxisnahe Einführung in die Bewertung und Prüfung von KI-Systemen nach aktuellen rechtlichen und technischen Standards. Vermittelt werden EU AI Act, ISO/IEC 42001, Datenschutzgesetze und praxisorientierte Prüfverfahren. Behandelt werden Risikobewertung, Konformitätsprüfung und spezialisierte Methoden wie VDE SPEC 90012 und TÜV AI Assessment Matrix.

### **Zielgruppe:**

- KI-Auditoren
- Compliance-Beauftragte
- Verantwortliche für die Einführung und Umsetzung von ISO/IEC 42001:2023
- KI-Beauftragte
- KI-Berater

### **Voraussetzungen:**

- Vorheriger Besuch des **AI120 AIMS-Implementierung gemäß ISO/IEC 42001:2023** oder Erfahrung mit Managementsystemen sowie vorherige grundlegende Befassung mit der ISO/IEC 42001:2023
- Vorheriger Besuch des **SC135 Interner Auditor** oder vergleichbare Auditkenntnisse

### **Sonstiges:**

**Dauer:** 3 Tage

**Preis:** 2390 Euro plus Mwst.

### **Ziele:**

- Verständnis für die Grundlagen und Funktionsweise von KI-Systemen erlangen.
- Überblick über den rechtlichen Rahmen, insbesondere den EU AI Act und seine Risikoklassifizierung, gewinnen.
- Kenntnis der Anforderungen an Konformitätsbewertungen und Dokumentationen für KI-Systeme erlangen.
- Fähigkeit, technische Aspekte von KI-Systemen wie Modellvalidierung, Bias-Erkennung und Performance-Bewertung zu analysieren.
- Einblick in Prüfmethode und spezifische Verfahren wie die VDE SPEC 90012 und TÜV AI.Lab Assessment Matrix gewinnen.
- Fähigkeit, ethische, sicherheitstechnische und regulatorische Anforderungen auf eigene KI-Systeme anzuwenden.
- Praktische Kenntnisse zur Durchführung von Audits und Qualitätssicherungsmaßnahmen erwerben.

Darüber hinaus bildet der Kurs eine gute Basis für weitere Kurse, z.B.:

- AI100 KI-Beauftragter
- AI060 KI GRC Specialist

## Inhalte/Agenda:

### • Modul 1: Grundlagen und rechtlicher Rahmen

- ♦ Einführung in KI-Systeme
  - ♦ Arten von KI-Systemen und ihre Anwendungen
  - ♦ Grundlegende KI-Architektur und Funktionsweise
  - ♦ Aktuelle Entwicklungen und Trends
- ♦
- ♦ Rechtliche Grundlagen
  - ♦ EU AI Act und seine Auswirkungen
    - Risikoklassifizierung nach EU AI Act
    - Was sind Konformitätsbewertungen
    - Konformitätsbewertungsverfahren für die verschiedenen Level
    - Definitionserklärung minimales Risiko vs. kein Risiko
    - Anforderungen an Konformitätsbewertungsstellen
    - Dokumentationsanforderungen und technische Unterlagen
    - Konformitätserklärung und CE-Kennzeichnung
    - Identifikation und Bewertung von KI-spezifischen Risiken
    - Aktives und passives Risikomanagement
  - ♦ Internationale Regulierungen und Standards
    - ♦ KI-Managementsysteme nach ISO/IEC 42001
      - Struktur und Anforderungen der ISO 42001
      - Integration in bestehende Managementsysteme
      - Prozesslandschaft und Dokumentationspyramide
      - Rollen und Verantwortlichkeiten
  - ♦ Datenschutzrechtliche Anforderungen (DSGVO)
- ♦

### Modul 2: Technische Aspekte und Prüfmethoden

- ♦ Ethische Bewertung von KI-Systemen
  - ♦ Relevanz von ethischen Bewertungen
  - ♦ Konzeptuelle Übersicht
- ♦ Technische Evaluation von KI-Systemen
  - ♦ Bewertung von Trainingsdaten und Datenpipelines
  - ♦ Modellvalidierung und Performance-Metriken
  - ♦ Bias-Erkennung und –Bewertung
- ♦ Sicherheit und Robustheit
  - ♦ Cybersicherheit für KI-Systeme
  - ♦ Adversarial Attacks und Verteidigungsstrategien
  - ♦ Systemstabilität und Fehlertoleranz
- ♦ Qualitätssicherung und Audit-Grundlagen
  - ♦ Kontinuierliche Überwachung
  - ♦ Prinzipien und Methoden des KI-Audits
  - ♦ Audit-Trail und Nachvollziehbarkeit
- ♦

### Modul 3: Prüfverfahren für KI-Systeme – Theorie & Praxis

- ♦ VDE SPEC 90012
- ♦ TÜV AI.AM

### Zertifikatsprüfung