AI600 AI Governance, Risk & Compliance für Führungskräfte

Kurzbeschreibung:

Das Training zeigt Führungskräften praxisnah, wie Organisationen den EU AI Act systematisch einordnen und in belastbare Governance-, Risiko- und Compliance-Strukturen überführen. Im Fokus stehen High-Risk-AI, Überschneidungen mit DSGVO, NIS2, DORA, MDR und IVDR sowie die praktische Umsetzung mit durchgängigem Fallbeispiel. ISO/IEC 42001, NIST AI RMF, Compliance-Roadmap und Praxisübungen unterstützen den direkten Transfer in die eigene Organisation.

Zielgruppe:

Das Training **AI600 AI Governance, Risk & Compliance für Führungskräfte** richtet sich an:

- CISO
- IT Senior Manager
- KI-Entscheider
- GRC-Strategen

Voraussetzungen:

Für die Teilnahme am Kurs **AI600 AI Governance, Risk & Compliance für Führungskräfte** sind keine Vorkenntnisse erforderlich.

Sonstiges:

Dauer: 2 Tage

Preis: 2350 Euro plus Mwst.

Ziele:

Nach Abschluss des Kurses **AI600 AI Governance, Risk & Compliance für Führungskräfte** sind Sie in der Lage,

- den EU AI Act einzuordnen und auf die eigene Organisation anzuwenden
- AI-Systeme nach Risiko zu klassifizieren und High-Risk-AI-Systeme zu identifizieren
- zentrale Compliance-Anforderungen praxisnah umzusetzen
- Anforderungen an technische Dokumentation und Data Governance zu bewerten
- regulatorische Überschneidungen mit DSGVO, NIS2, DORA, MDR und IVDR zu erkennen
- ISO/IEC 42001 und das NIST AI RMF für eine wirksame AI Governance zu nutzen
- AI-Governance-Strukturen, Rollen und Verantwortlichkeiten in der Organisation zu definieren
- Anforderungen an FRIA, Transparenz, Logging, Post-Market-Monitoring und Incident Management einzuordnen
- eine Compliance-Roadmap für die eigene Organisation zu entwickeln

Inhalte/Agenda:

- **Der EU AI Act - Die neue regulatorische Realität verstehen**
  - Einführung & Kontext
    - · Grundprinzipien & Ziele
    - · Das Risikoklassifizierungssystem
    - · Zeitplan & Durchsetzung
    - · Sanktionen
  - Bewertung der Fallstudie: Risikokategorisierung & Rollendefinition
  - **Praxisübung:** Die Teilnehmer klassifizieren die KI-Systeme auf Basis der Fallstudie (plus optional: Anwendungsfälle aus eigenen beruflichen Erfahrungen)

- **Fokus: Hochrisiko-KI**
  - EU AI Act Artikel 8-15: Was Compliance tatsächlich umfasst
  - Anforderungen an die technische Dokumentation (Anhang-IV-Durchgang)
  - Anforderungen an Data Governance und Datenqualität
  - **Praxisübung:** Compliance-Anforderungen auf das Hochrisiko-System der Fallstudie abbilden

- **Verwandte Regulierung & EU Digital Omnibus on AI (Digital-Omnibus-Verordnung zur KI)**
  - KI-Haftungsrahmen
    - · Aktueller Stand & regulatorische Lücken
  - Regulatorisches Ökosystem
    - · GDPR-Schnittmenge: Automatisierte Entscheidungsfindung (Art. 22), Datenschutz durch Technikgestaltung
    - · Sektorspezifische Überlagerungen: Finanzdienstleistungen (DORA, MiFID), Gesundheitswesen (MDR, IVDR), kritische Infrastrukturen
    - · Cybersecurity Act & NIS2: Sicherheitsanforderungen für KI-Systeme
    - · Digital Services Act: Plattformverantwortlichkeiten für KI-generierte Inhalte
  - Das AI Omnibus Package
    - · Welche Änderungen vorgeschlagen werden – und was diese bedeuten würden
  - Diskussion: Identifizierung der regulatorischen Schnittstellenpunkte Ihrer Organisation

- **ISO42001 als Enabler**
  - Warum ISO 42001 für die Compliance mit dem AI Act wichtig ist
  - Kernkomponenten von ISO 42001
  - Abbildung von ISO auf den EU AI Act
  - Positionierung von ISO 42001

- **NIST AI RMF als Übersetzer**
  - Warum NIST AI RMF für die Compliance mit dem EU AI Act
    - · Die vier Kernfunktionen: GOVERN; MAP; MEASURE; MANAGE
  - Operationalisierung der Risikobewertung
  - NIST als gemeinsame Sprache
  - Vorschau auf die praktische Anwendung

- **Gestaltung der Governance-Struktur**
  - Governance-Anforderungen: Rollen, Verantwortlichkeiten, Rechenschaftspflicht
  - Organisationsmodelle: Zentrales AI Office vs. verteilte Zuständigkeit
  - Grundlegende Elemente des Policy-Frameworks
  - **Praxisübung:** Gestaltung des Betriebsmodells für die AI Governance der Organisation in der Fallstudie

- **Deep Dive 1: Operationalisierung des Risikomanagements**
  - NIST AI RMF Deep Dive: Funktionen Map, Measure, Manage, Govern
  - Konformitätsbewertungsprozess nach dem EU AI Act
  - Methodik der Grundrechte-Folgenabschätzung (FRIA)

- **Deep Dive 2: Dokumentation & Transparenz**
  - Pakete für die technische Dokumentation (Art. 11)
  - Transparenzpflichten und Anforderungen an Nutzerinformationen
  - Anforderungen an Aufzeichnungsführung und Logging
  - Praxisübung: Dokumentations-Framework für das Hochrisiko-System der Fallstudie erstellen

- **Deep Dive 3: Post-Market-Monitoring & Incident Management**
  - Anforderungen an die laufende Überwachung

- ◊ Pflichten zur Incident-Meldung
- ◊ Bewertung von Änderungen und wesentlichen Änderungen
- ◊ Praxisübung: Post-Market-Monitoring-Plan für die Organisation der Fallstudie entwerfen

♦ **Ihre Compliance-Roadmap**

- ◊ Governance für Drittparteien und Lieferanten (Berücksichtigung externer KI-Tools in der Fallstudie)
- ◊ Pfade der Konformitätsbewertung und Einbindung benannter Stellen
- ◊ Change Management und Stakeholder-Kommunikation
- ◊ Praxisübung: Die Teilnehmer arbeiten an der Compliance-Roadmap ihrer eigenen Organisation und übertragen die Erkenntnisse aus der Fallstudie auf ihren Kontext

♦ **Wrap-up & Action Planning**

- ◊ Wichtigste Erkenntnisse
- ◊ Ressourcenpaket und nächste Schritte
- ◊ Q&A und Peer Learning
- ◊