SC225 ISACA Advanced in AI Security Management (AAISM) Vorbereitung

Kurzbeschreibung:

Der Kurs **SC225 ISACA Advanced in AI Security Management (AAISM) Vorbereitung** vermittelt ein umfassendes Verständnis von Risiken, Kontrollen und Governance-Anforderungen beim Einsatz von Künstlicher Intelligenz in Unternehmensumgebungen. Er kombiniert etablierte Security-Management-Praktiken mit KI-spezifischen Herausforderungen wie Datenmanagement, Modelltraining, Ethik und Compliance und bereitet gezielt auf die offizielle AAISM-Zertifizierung vor.

Zielgruppe:

Der Kurs **SC225 ISACA Advanced in AI Security Management (AAISM) Vorbereitung** richtet sich an:

- Inhaber einer aktiven CISM oder CISSP Zertifizierung
- Nachgewiesene Erfahrung in Security- oder Beratungsfunktionen
- Erfahrung in der Bewertung, Implementierung und Wartung von KI-Systemen

Voraussetzungen:

Um an dem Kurs **SC225 ISACA Advanced in AI Security Management (AAISM) Vorbereitung** teilnehmen zu können, sollten Sie folgende Voraussetzungen erfüllen:

- Inhaber einer aktiven CISM oder CISSP Zertifizierung
- Mehrjährige Berufserfahrung im Bereich IT-Sicherheitsmanagement
- Grundkenntnisse zur Architektur und Funktionsweise von KI-Systemen

Sonstiges:

Dauer: 2 Tage

Preis: 1650 Euro plus Mwst.

Ziele:

Nach Abschluss des Kurses **SC225 ISACA Advanced in AI Security Management (AAISM) Vorbereitung** sind die Teilnehmenden in der Lage:

- Die Prinzipien von KI-Governance und Programm-Management zu erläutern
- Methoden des KI-Risikomanagements anzuwenden, einschließlich Risikobewertung, Behandlung und Monitoring
- KI-Technologien, Datenflüsse und Lebenszyklusphasen auf Sicherheitsimplikationen zu prüfen
- Ethische, sicherheitsrelevante und datenschutzbezogene Aspekte in KI-Deployments zu integrieren
- Sich effektiv auf die AAISM Zertifizierungsprüfung vorzubereiten

Inhalte/Agenda:

- ♦ **Domäne 1: KI-Governance und Programm-Management (31 %)**
  - ♦ ◊ Stakeholder-Aspekte, Branchenrahmenwerke und regulatorische Anforderungen
    ◊ KI-bezogene Strategien, Richtlinien und Verfahren
    ◊ KI-Asset- und Daten-Lebenszyklus-Management
    ◊ Entwicklung und Management von KI-Sicherheitsprogrammen
    ◊ Business Continuity und Incident Response
- ♦ ◊
- ♦ **Domäne 2: KI-Risikomanagement (31 %)**
  - ♦ ◊ KI-Risikobewertung, Schwellenwerte und Behandlung
    ◊ KI-Bedrohungs- und Schwachstellenmanagement
    ◊ KI-Lieferanten- und Supply-Chain-Management
- ♦ ◊
- ♦ **Domäne 3: KI-Technologien und -Kontrollen (38 %)**
  - ♦ ◊ KI-Sicherheitsarchitektur und -design
    ◊ KI-bezogene Strategien, Richtlinien und Verfahren
    ◊ Kontrollen des Datenmanagements
    ◊ Kontrollen zu Datenschutz, Ethik, Trust & Safety
    ◊ Sicherheitskontrollen und Monitoring
- ♦ ◊