

SC221 ISACA CISM Human Factor Edition

Kurzbeschreibung:

Inspired by CISO-Alliance & exklusiv bei qSkills: Ein einzigartiger Lehrgang, der Wissen und Methoden für die wertvolle CISM-Zertifizierung der ISACA vermittelt und ergänzt um relevante Softskills im Bereich der Führung und Kommunikation, Kenntnissen von Methoden und Werkzeugen zur Klarheit und Selbstführung sowie Verständnis für kritische oder dynamische Situationen.

Zielgruppe:

Der Workshop richtet sich an Informationssicherheitsexperten, die eine fundierte Berufserfahrung durch umfassende Tätigkeit auf dem Gebiet der Informationssicherheit erworben haben und besonders fordernde Szenarien souverän meistern müssen. Fachkräfte mit fünf oder mehr Jahren Berufserfahrung in der aktiven Ausgestaltung der betrieblichen Informationssicherheit werden sich durch die Möglichkeit zu dieser Zertifizierung angesprochen fühlen.

Zu den Berufsbezeichnungen gehören:

- CISO
- CSO
- IR/SOC-Leads
- Projektleiter
- BCM-Manager
- IS-Risikomanager

Voraussetzungen:

Um die Zertifizierung eines CISM erhalten zu können, müssen folgende Anforderungen erfüllt sein:

- Erfolgreicher Abschluss der CISM-Prüfung
- Beachtung des Codes of Professional Ethics von ISACA
- Nachweis von mind. fünf Jahren Berufserfahrung auf dem Gebiet der Informationssicherheit
- Nachweis der ständigen beruflichen Weiterbildung (Continuing Professional Education (CPE) Policy)

Sonstiges:

Dauer: 5 Tage

Preis: 3450 Euro plus MwSt.

Ziele:

- Intensive Vorbereitung auf die ISACA CISM Zertifizierung
- sowie darüber hinaus:
 - ◆ Verständnis für menschliches Verhalten in Ausnahmesituationen
 - ◆ Einblick in psychologische Aspekte, soziale Dynamiken als Teil des Lösungsportfolio erkennen
 - ◆ Souveränität im Ausnahmezustand: Klare Entscheidungsmodelle, um Führung auch unter Druck zu ermöglichen

- ◆ Komplexität reduzieren: typische Verhaltensmuster, Stressfaktoren & Rollenkonflikte identifizieren und begegnen
- ◆ Einfluss über Kommunikationsströme, Entscheidungskaskaden und Betriebsklima

Darüber hinaus bildet der Kurs eine hervorragende Basis für weitere Aufbaukurse, z.B.:

- **SC510 Cyber Security Emergency Training für CISOs und Security Professionals**
- **SC520 Human Factor in Cyber Security**

Inhalte/Agenda:

- ◆ **Domain 1 - Informationssicherheits-Governance**
 - ◆ ◇ Überblick über Unternehmens-Governance
 - ◆ ◇ Unternehmenskultur, -strukturen, -rollen und -verantwortlichkeiten
 - ◆ ◇ Rechtliche, regulatorische und vertragliche Anforderungen
 - ◆ ◇ Informationssicherheitsstrategie
 - ◆ ◇ Frameworks und Standards der Informations-Governance
 - ◆ ◇ Strategische Planung
- ◆ ◇
- ◆ **Domain 2 — Risikomanagement im Rahmen der Informationssicherheit**
 - ◆ ◇ Risiko- und Bedrohungslandschaft
 - ◆ ◇ Schwachstellen- und Kontrolldefizitanalyse
 - ◆ ◇ Risikoeinschätzung, -bewertung und -analyse
 - ◆ ◇ Reaktion auf Informationsrisiken
 - ◆ ◇ Risikoüberwachung, Berichterstattung und Kommunikation
- ◆ ◇
- ◆ **Human Factor**
 - ◆ ◇ Grundlagen Human Factor
 - ◆ ◇ kognitive Verzerrungs- & Entscheidungsfallen
 - ◆ ◇ Kommunikation & Führungsrolle in Ausnahmesituationen
 - ◆ ◇ Kultur & Persönliches
- ◆ ◇
- ◆ **Domain 3 — Entwicklung und Verwaltung von Informationssicherheitsprogrammen**
 - ◆ ◇ IS-Programmentwicklung und Ressourcen
 - ◆ ◇ Standards und Frameworks für Informationssicherheit
 - ◆ ◇ Definition einer Roadmap für ein IS-Programm
 - ◆ ◇ Kennzahlen für das IS-Programm
 - ◆ ◇ IS-Programmmanagement
 - ◆ ◇ IS-Sensibilisierung und -Schulung
 - ◆ ◇ Integration des Sicherheitsprogramms in den IT-Betrieb
 - ◆ ◇ Programmkommunikation, Berichterstattung und Leistungsmanagement
- ◆ ◇
- ◆ **Domain 4 — Incident Management im Rahmen der Informationssicherheit**
 - ◆ ◇ Übersicht über Incident Management und Incident Response
 - ◆ ◇ Pläne für Incident Management und Incident Response
 - ◆ ◇ Klassifizierung/Kategorisierung von Vorfällen
 - ◆ ◇ Incident-Management-Operationen, Tools und Technologien
 - ◆ ◇ Untersuchung, Bewertung, Eindämmung und Kommunikation von Vorfällen
 - ◆ ◇ Beseitigung von Vorfällen, Wiederherstellung und Überprüfung
 - ◆ ◇ Geschäftliche Auswirkungen und Kontinuität
 - ◆ ◇ Wiederherstellungsplanung (DRP)
 - ◆ ◇ Schulung, Tests und Bewertung