SC220 ISACA CISM Vorbereitung

Kurzbeschreibung:

IT-Profis mit Fachwissen in IS/IT-Sicherheit und -Kontrolle erwerben fundierte Kenntnisse zur Planung, Umsetzung und Steuerung von Informationssicherheitskonzepten. Behandelt werden alle Inhalte der CISM-Prüfung, ergänzt durch intensive Vorbereitung auf Ablauf und Anforderungen. Ziel ist die erfolgreiche Zertifizierung als Certified Information Security Manager (CISM).

Zielgruppe:

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

Zu den Berufsbezeichnungen gehören:

- CISO
- CSO
- IT-Administratoren
- Sicherheitsexperten
- Risikomanager und Berater

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: 4 Tage

Preis: 2950 Euro plus Mwst.

Ziele:

Dieser Workshop bereitet Sie intensiv auf die die ISACA-Prüfung zur Erlangung der CISM-Zertifizierung vor.

Inhalte/Agenda:

- ♦ **Domain 1 - Informationssicherheits-Governance (17%)**
- ♦ ◊ 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 (20%)**
- ♦ ◊ Risiko- und Bedrohungslandschaft
  ◊ Schwachstellen- und Kontrolldefizitanalyse
  ◊ Risikoeinschätzung, -bewertung und -analyse
  ◊ Reaktion auf Informationsrisiken
  ◊ Risikoüberwachung, Berichterstattung und Kommunikation

♦ **Domain 3 — Entwicklung und Verwaltung von Informationssicherheitsprogrammen (33%)**
- ♦ ◊ 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 (30%)**
- ♦ ◊ 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
- ♦ ◊