SC220 ISACA CISM Vorbereitung

Kurzbeschreibung:

Der Workshop **SC220 ISACA CISM Vorbereitung** richtet sich an IT-Profis mit technischem Fachwissen und Erfahrungen in den Bereichen IS/IT-Sicherheit und -Kontrolle. Die CISM-Zertifizierung belegt Ihre Qualifikation hinsichtlich der Planung, der Umsetzung sowie der Steuerung und Überwachung von Informationssicherheitskonzepten und genießt global hohe Anerkennung.

Dieser Workshop bereitet Sie intensiv auf die Inhalte und den Ablauf der Prüfung zum **ISACA CISM (Certified Information Security Manager)** vor. Die kostenpflichtige Prüfung besteht aus 150 Fragen, die innerhalb von vier Stunden bearbeitet werden müssen. Die Prüfung kann online oder in einem der autorisierten PSI-Testzentren durchgeführt werden.

Kurssprache: Wahlweise Deutsch oder Englisch
Kursunterlagen: Englisch
Prüfungssprache: Englisch

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 durch 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: 2790 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%)**
- ♦ ◊ Unternehmensführung
  - ◊ · Unternehmenskultur
  - · Organisationsstrukturen, Rollen und Zuständigkeiten
  - · Gesetzliche, behördliche und vertragliche Anforderungen
- ◊ Informationssicherheitsstrategie
  - ◊ · Entwicklung einer Informationssicherheitsstrategie
  - · Information Governance Frameworks und Standards
  - · Strategische Planung (z. B. Budgets, Ressourcen, Business Case)

- ♦ **Domain 2 — Risikomanagement für Informationssicherheit (20%)**
- ♦ ◊ Risikobewertung der Informationssicherheit
  - ◊ · Risiko- und Bedrohungslandschaft
  - · Schwachstellen- und Kontrollmangelanalyse
  - · Risikobewertung und -analyse
- ◊ Reaktion auf das Risiko der Informationssicherheit
  - ◊ · Risikobehandlungs-/Risikoreaktionsoptionen
  - · Risiko- und Kontrollbesitz
  - · Risikoüberwachung und Berichterstattung

- ♦ **Domain 3 — Informationssicherheitsprogramm (33%)**
- ♦ ◊ Entwicklung von Informationssicherheitsprogrammen
  - ◊ · Informationssicherheitsprogramm-Ressourcen (z. B. Personen, Tools, Technologien)
  - · Identifizierung und Klassifizierung von Informations-Assets
  - · Industriestandards und Frameworks für Informationssicherheit
  - · Informationssicherheitsrichtlinien, Verfahren und Richtlinien
  - · Metriken des Informationssicherheitsprogramms
- ◊ Verwaltung des Informationssicherheitsprogramms
  - ◊ · Design und Auswahl von Informationssicherheitskontrollen
  - · Implementierung und Integration von Informationssicherheitskontrollen
  - · Prüfung und Bewertung der Informationssicherheitskontrolle
  - · Sensibilisierung und Schulung für Informationssicherheit
  - · Verwaltung externer Dienste (z. B. Anbieter, Lieferanten, Dritte, Vierte Parteien)
  - · Kommunikation und Berichterstattung des Informationssicherheitsprogramms

- ♦ **Domain 4 — Informationssicherheits-Vorfallmanagement (30%)**
- ♦ ◊ Bereitschaft zum Vorfallmanagement
  - ◊ · Incident-Response-Plan
  - · Business-Impact-Analyse (BIA)
  - · Geschäftskontinuitätsplan (BCP)
  - · Notfallwiederherstellungsplan (DRP)
  - · Vorfallklassifizierung/-kategorisierung
  - · Incident-Management-Training, -Tests und -Evaluierung
- ◊ Vorfallmanagementvorgänge
  - ◊ · Incident-Management-Tools und -Techniken
  - · Untersuchung und Bewertung von Vorfällen
  - · Methoden zur Eindämmung von Vorfällen
  - · Mitteilungen zur Reaktion auf Vorfälle (z. B. Meldung, Benachrichtigung, Eskalation)
  - · Beseitigung und Wiederherstellung von Vorfällen
  - · Überprüfungspraktiken nach einem Vorfall
- ♦ ◊ ·