SC240 ISACA CRISC Vorbereitung

Kurzbeschreibung:

Teilnehmende erhalten eine praxisnahe Vorbereitung auf die ISACA CRISC-Zertifizierung. Vermittelt werden Kenntnisse zur Identifikation, Bewertung und Steuerung von IT- und Unternehmensrisiken sowie zur Implementierung und Überwachung von Informationssystem-Kontrollen. Behandelt wird die intensive Vorbereitung auf die offizielle Prüfung.

Zielgruppe:

Der Workshop richtet sich an Fachexperten, die sich auf dem Gebiet von IT-Risikomanagement und Enterprise Risk Management weiterbilden wollen und mindestens 3 Jahre einschlägige Berufserfahrung in den Gebieten von Risikomanagement sowie Interner Kontrolle im IT-Umfeld gesammelt haben.

Zu den Berufsbezeichnungen gehören:

- IT-Experten
- IT-Auditoren
- Interne Revisoren und Abschlussprüfer
- Risikomanager und Berater
- Sicherheitsadministratoren
- IT-Sicherheitsanalysten

Voraussetzungen:

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

- Erfolgreicher Abschluss der CRISC-Prüfung
- Beachtung des Codes of Professional Ethics von ISACA
- Nachweis von mind. drei Jahren Berufserfahrung auf den Gebieten Risikomanagement sowie IT-Kontrolle
- 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 CRISC-Zertifizierung vor.

Inhalte/Agenda:

- ♦ **Domain 1 - Governance (26%)**
  - ♦ ◊ Organisations-Governance
    - ◊ · Strategie, Ziele und Vorgaben
      · Organisationsstruktur, Rollen und Verantwortlichkeiten
      · Organisationskultur und Ethik
      · Richtlinien und Standards
      · Geschäftsprozesse und Resilienz
      · Organisationsweites Asset Management
    - ◊ Risiko-Governance
    - ◊ · Enterprise Risk Management
      · Verteidigungslinien
      · Risikoprofil
      · Risikobereitschaft und Risikotoleranz
      · Risikorahmenwerke, gesetzliche, regulatorische und vertragliche Anforderungen

  - ♦ **Domain 2 - Risikoanalyse (22%)**
  - ♦ ◊ Risikobehandlung
    - ◊ · Optionen der Risikobehandlung
      · Threat Modeling und Bedrohungslandschaft
      · Schwachstellenmanagement
      · Entwicklung und Bewertung von Risikoszenarien
    - ◊ Risikoanalyse
    - ◊ · Konzepte und Standards der Risikoanalyse
      · Business Impact Analysis (BIA)
      · Risikoregister
      · Methodologien der Risikoanalyse
      · Inhärentes, Restrisiko und aktuelles Risiko

  - ♦ **Domain 3 - Risikobehandlung und -berichterstattung (32%)**
  - ♦ ◊ Risikobehandlung
    - ◊ · Optionen der Risikobehandlung
      · Risiko- und Kontrollverantwortung
      · Lieferanten- und Supply-Chain-Risikomanagement
      · Management von Problemen, Feststellungen, Ausnahmen und Freistellungen
    - ◊ Design und Implementierung von Kontrollen
    - ◊ · Kontrollrahmenwerke, -arten und -standards
      · Gestaltung, Auswahl, Implementierung und Analyse von Kontrollen
      · Methodologien für Kontrolltests
    - ◊ Risikomonitoring und -berichterstattung
    - ◊ · Risikomaßnahmenpläne
      · Datenerfassung, -aggregation, -analyse und -validierung
      · Kennzahlen für Risiko und Kontrolle
      · Techniken für Monitoring und Berichterstattung zu Risiko und Kontrolle
      · Monitoring und Berichterstattung zu aufkommenden Risiken

  - ♦ **Domain 4 - Technologie und Sicherheit (20%)**
  - ♦ ◊ Technologieprinzipien
    - ◊ · Technologie-Roadmaps und Enterprise Architecture (EA)
      · Betriebsmanagement
      · System Development Life Cycle (SDLC)
      · Data Lifecycle Management
      · Portfolio- und Projektmanagement
      · Technologische Resilienz und Notfallreaktion/-wiederherstellung
      · Neue Technologien
    - ◊ Grundlagen der Informationssicherheit
    - ◊ · Sicherheitskonzepte, -rahmenwerke und -standards
      · Sensibilisierung und Schulung zu Sicherheit/Risiko
      · Grundlagen des Datenschutzes und der Datensicherheit
  - ♦ ◊