SC240 ISACA CRISC Vorbereitung

Kurzbeschreibung:

CRISC (Certified in Risk and Information Systems Control) ist eine weltweit anerkannte managementorientierte Zertifizierung, die IT-Fachspezialisten auf die einzigartigen Herausforderungen des IT- und Unternehmensrisikomanagements vorbereitet und diese als strategischen Partner für Unternehmen positioniert. Die CRISC-Zertifizierung belegt Ihre Qualifikation als Experte in der Identifizierung und Bewertung von IT-Risiken im Unternehmen sowie in der Implementierung und Überwachung von Informationssystem-Kontrollen.

Der Workshop **SC240 ISACA CRISC Vorbereitung** bereitet Sie intensiv auf die ISACA-Prüfung zur Erlangung der CRISC-Zertifizierung 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 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: 3 Tage

Preis: 2390 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%)**
  - ♦ ◊ Organisationsführung
    - ◊ · Organisationsstrategie, Ziele
    - · Organisationsstruktur, Rollen und Verantwortlichkeiten
    - · Unternehmenskultur
    - · Richtlinien und Standards
    - · Arbeitsprozesse
    - · Organisatorisches Vermögen
  - ◊ Risiko-Governance
    - ◊ · Enterprise Risk Management und Risk Management Framework
    - · Drei Verteidigungslinien
    - · Risikoprofil
    - · Risikobereitschaft und Risikotoleranz
    - · Gesetzliche, behördliche und vertragliche Anforderungen
    - · Berufsethik des Risikomanagements

- ♦ **Domain 2 - IT-Risikobewertung (20%)**
  - ♦ ◊ IT-Risikoidentifikation
    - ◊ · Risikoereignisse (z. B. beitragende Bedingungen, Schadensergebnis)
    - · Bedrohungsmodellierung und Bedrohungslandschaft
    - · Schwachstellen- und Kontrollmangelanalyse (z. B. Ursachenanalyse)
    - · Entwicklung von Risikoszenarien
  - ◊ IT-Risikoanalyse und -bewertung
    - ◊ · Risikobewertungskonzepte, Standards und Frameworks
    - · Gefahrenregister
    - · Methoden der Risikoanalyse
    - · Business-Impact-Analyse
    - · Inhärentes und Restrisiko

- ♦ **Domain 3 - Risikoreaktion und Berichterstattung (32%)**
  - ♦ ◊ Risikoreaktion
    - ◊ · Risikobehandlungs-/Risikoreaktionsoptionen
    - · Risiko- und Kontrollbesitz
    - · Risikomanagement von Drittanbietern
    - · Problem-, Finding- und Ausnahmemanagement
    - · Management neu auftretender Risiken
  - ◊ Design und Implementierung von Kontrollen
    - ◊ · Kontrolltypen, Standards und Frameworks
    - · Design, Auswahl und Analyse von Kontrollen
    - · Kontrollimplementierung
    - · Kontrolltests und Wirksamkeitsbewertung
  - ◊ Risikoüberwachung und Berichterstattung
    - ◊ · Risikobehandlungspläne
    - · Datenerfassung, -aggregation, -analyse und -validierung
    - · Risiko- und Kontrollüberwachungstechniken
    - · Risiko- und Kontrollberichtstechniken (Heatmap, Scorecards, Dashboards)
    - · Leistungskennzahlen
    - · Key Risk Indicators (KRIs)
    - · Key Control Indicators (KCIs)

- ♦ **Domain 4 - Informationstechnologie und Sicherheit (22%)**
  - ♦ ◊ Grundsätze der Informationstechnologie
    - ◊ · Unternehmensstruktur
    - · IT Operations Management (z. B. Änderungsmanagement, IT-Assets, Probleme, Vorfälle)
    - · Projektmanagement
    - · Disaster-Recovery-Management (DRM)
    - · Datenlebenszyklusmanagement
    - · Lebenszyklus der Systementwicklung (SDLC)
    - · Aufkommende Technologien
  - ◊ Grundsätze der Informationssicherheit
    - ◊ · Informationssicherheitskonzepte, Frameworks und Standards
    - · Sensibilisierungsschulung für Informationssicherheit
    - ·

· Wirtschaftskontinuitätsmanagement
· Datenschutz und Datenschutzgrundsätze