SC230 ISACA CISA Vorbereitung

Kurzbeschreibung:

IT-Auditoren erwerben fundierte Kenntnisse zur Prüfung, Kontrolle und Bewertung von IT- und Geschäftssystemen. Vermittelt wird der risikobasierte Ansatz zur Planung, Durchführung und Berichterstattung von Audits. Behandelt werden die fünf von ISACA definierten Domänen und praxisnahe Methoden, um sich gezielt und strukturiert auf die CISA-Zertifizierung vorzubereiten.

Zielgruppe:

Hegen Sie den Wunsch, Ihre beruflichen Leistungen zu verbessern oder in eine neue Position aufzusteigen? Die Erlangung des Titels eines CISA wird Sie gegenüber anderen Kandidaten hervorheben und Ihnen einen Wettbewerbsvorteil verschaffen. Der Workshop richtet sich an alle, die die Zertifizierung zum CISA erfolgreich bestehen möchten.

Zu den Berufsbezeichnungen gehören:

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

Voraussetzungen:

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

- Erfolgreicher Abschluss der CISA-Prüfung
- Beachtung des Codes of Professional Ethics von ISACA
- Nachweis von mindestens fünf Jahren Erfahrung im Bereich IS/IT-Prüfung, Kontrolle, Assurance oder Sicherheit.

Sonstiges:

Dauer: 4 Tage

Preis: 2950 Euro plus Mwst.

Ziele:

Dieser Workshop **SC230 ISACA CISA Vorbereitung** bereitet Sie intensiv auf die die ISACA-Prüfung zur Erlangung der CISA-Zertifizierung vor.

Inhalte/Agenda:

- ♦ **Domain 1 - Prüfungsprozess für Informationssysteme (18%)**
- ♦ ◊ Planung
  - ◊ · IS-Audit-Standards, -Richtlinien und -Ethikkodizes
  - · Arten von Audits, Beurteilungen und Reviews
  - · Risikobasierte Auditplanung
  - · Arten von Audits und Überlegungen
- ◊ Ausführung
  - ◊ · Audit-Projektmanagement
  - · Auditprüfung und Stichprobenmethodik
  - · Audit Techniken zur Beweiserhebung
  - · Audit Datenanalyse
  - · Berichts- und Kommunikationstechniken
  - · Qualitätssicherung und Verbesserung des Prüfungsprozesses

♦ **Domain 2 - Governance & Management von IT (18%)**

- ♦ ◊ IT-Governance und IT-Strategie
  - ◊ · Gesetze, Vorschriften und Industriestandards
  - · Organisatorische Struktur, IT-Governance und IT-Strategie
  - · IT-Richtlinien, -Standards, -Verfahren und -Leitlinien
  - · Unternehmensarchitektur und Überlegungen
  - · Unternehmensrisikomanagement (ERM)
  - · Datenschutzprogramm und -prinzipien
  - · Datenmanagement und Klassifizierung
- ◊ IT-Management
  - ◊ · IT-Ressourcenmanagement
  - · Akquise und Management von IT-Dienstleistern
  - · Überwachung und Berichterstattung der IT-Performance
  - · Qualitätssicherung und Qualitätsmanagement der IT

♦ **Domain 3 - Akquisition, Entwicklung und Implementierung von Informationssystemen (12%)**

- ♦ ◊ Erwerb und Entwicklung von Informationssystemen
  - ◊ · Projektsteuerung und -management
  - · Business Case und Durchführbarkeitsanalyse
  - · Systementwicklungsmethoden
  - · Kontrollidentifikation und -design
- ◊ Implementierung von Informationssystemen
  - ◊ · Systembereitschafts- und Implementierungstests
  - · Implementierung Konfigurations- und Release-Management
  - · Systemmigration, Bereitstellung der Infrastruktur und Datenkonvertierung
  - · Überprüfung nach der Implementierung

♦ **Domain 4 - Betrieb von Informationssystemen und Business Resilience (26%)**

- ♦ ◊ Betrieb von Informationssystemen
  - ◊ · IT-Komponenten
  - · IT-Asset-Management
  - · Auftragsplanung und Produktionsprozessautomatisierung
  - · Systemschnittstellen
  - · End-user Computing und Shadow IT
  - · Systemverfügbarkeit und Kapazitätsmanagement
  - · Problem- und Vorfallmanagement
  - · IT-Änderungs-, Konfigurations- und Patch-Management
  - · Operatives Log-Management
  - · IT-Service-Level-Management
  - · Datenbank-Management
- ◊ Business Resilience
  - ◊ · Business-Impact-Analyse (BIA)
  - · System- und operationelle Widerstandsfähigkeit
  - · Datensicherung, -speicherung und -wiederherstellung
  - · Business Kontinuitätsplan (BCP)
  - · Notfallwiederherstellungspläne (DRP)

♦ **Domain 5 - Schutz von Informationswerten (26%)**

- ♦ ◊

◊ Sicherheit und Kontrolle von Informationsvermögen

◊ · Richtlinien, Rahmenwerke, Standards und Leitlinien für die Sicherheit von Informationswerten
· Physischer Zugang und Umgebungskontrollen
· Identity und Access Management
· Netzwerk- und Endpunktsicherheit
· Prävention von Datenverlusten
· Datenverschlüsselung
· Public Key Infrastructure (PKI)
· Cloud und virtualisierte Umgebungen
· Mobile, Wireless und Internet-of-Things Devices

◊ Verwaltung von Sicherheitsereignissen

◊ · Schulungen und Programme zur Sensibilisierung für Sicherheitsfragen
· Angriffsmethoden und -techniken für Informationssysteme
· Tools und Techniken für Sicherheitstests
· Sicherheitsüberwachungsprotokolle, -tools und -techniken
· Management von Sicherheitsvorfällen
· Beweissicherung und Forensik

♦ **Übungsfragen/Wiederholung/CISA-Prüfungsvorbereitung**

♦