SC200 ISC2 CCSP Vorbereitung

Kurzbeschreibung:

IT-Sicherheitsprofis erwerben die notwendigen Fähigkeiten zur Steuerung von Cloudumgebungen und kommerziellen Clouddiensten und werden gezielt auf die ISC2 CCSP-Zertifizierung vorbereitet. Vermittelt werden grundlegende Bausteine der Cloud-Sicherheit auf Infrastruktur-, Plattform- und SaaS-Ebene. Der Kurs zeigt, wie Cloud-Security-Kompetenz durch eine global anerkannte Zertifizierung nachgewiesen werden kann.

Zielgruppe:

Sie haben bereits Erfahrung im Umgang mit Clouds der großen Hyperscaler und wollen Ihre Sicherheitskenntnisse bestätigen? Oder sind Sie bereits sicherheitszertifiziert und wollen Ihre Kenntnisse im Bereich der Cloud nachweisen? Dann ist die CCSP-Zertifizierung Ihre neue Qualifikation!

Der Kurs ist bedingt auch für (Quer-)Einsteiger mit sehr soliden Cloud IT-Kenntnissen und Experten der IT-Security geeignet - Architekten, erfahrene Systemintegratoren sowie Cloud-Administratoren mit ausgeprägtem Security Knowhow sind Kandidaten für dieses Security-Training.

Voraussetzungen:

Praktische Vorkenntnisse im Bereich Security und Cloud sind für dieses Training zwingende Voraussetzung. Solide Kenntnisse der Sicherheit von Cloud-Anwendungen, virtualisierten Betriebssystemen, Cloud-Infrastrukturkomponenten und/oder Cloud-Plattformen werden benötigt. Grundlegende Kenntnisse der Informationssicherheit und ihrer Schutzziele sowie IT-Sicherheit sind von Vorteil. Technische Vorkenntnisse über relevante Standards erleichtern den erfolgreichen Abschluss der CCSP-Zertifizierung.

Um als Professional die Zertifizierungsprüfung zum international anerkannten CCSP anzugehen, sind Vorkenntnisse der Security-Kernthemen erforderlich!

Sonstiges:

Dauer: 5 Tage

Preis: 3450 Euro plus Mwst.

Ziele:

In unserem Kurs lernen Sie, Ihre sensiblen Cloud-Daten zu schützen, und die von ISC2 vorgegebenen sechs Bereiche des CCSP (Certified Cloud Security Professional) zu meistern:

1) Cloud-Architektur und Gestaltung der Cloud
2) Datensicherheit in der Cloud
3) Plattform- & Infrastruktursicherheit in der Cloud
4) Anwendungssicherheit für Cloud-Applikationen
5) Compliance-Anforderungen für Cloud-Nutzung
6) Sicherer Betrieb von Cloud-Infrastrukturen

Inhalte/Agenda:

- ♦ **Domäne 1: Architekturkonzept und Designanforderungen an die Cloud** ~ 17 %
- ♦ ◊ Verständnis für Cloud Computing Konzepte
  ◊ Beschreibung der Cloud Referenzarchitektur
  ◊ Verständnis für relevante Securitykonzepte des Cloudcomputing
  ◊ Verständnis für Designprinzipien des Secure Cloudcomputing
  ◊ Identifikation vertrauenswürdiger Cloudservices

♦ **Domäne 2: Cloud Datensicherheit** ~ 20 %
- ♦ ◊ Der Cloud Lifecycle für Daten
  ◊ Design und Implementierung von Cloud Datenspeicher-Architekturen
  ◊ Verstehen und Implementieren von Datenerhebungs- und Klassifikationstechnologien
  ◊ Design und Implementieren relevanter rechtlicher Datenschutzmaßnahmen
  ◊ Design und Implementieren von DRM
  ◊ Planen & Implementieren von Datenhaltungspolicies
  ◊ Design und Implementieren von Auditfähigkeit & Nachvollziehbarkeit von Daten-Events

♦ **Domäne 3: Cloud Plattform Infrastruktur-Sicherheit** ~ 17 %
- ♦ ◊ Verständnis für die Cloud Infrastrukturen
  ◊ Risiken der Nutzung von Cloud Infrastrukturen
  ◊ Design und Planung von Security Controls
  ◊ Planung von Disaster Recovery & Business Continuity Management Maßnahmen

♦ **Domain 4: Cloud Applikations-Sicherheit** ~ 17 %
- ♦ ◊ Bedarf für Training und Awareness in Applikations-Sicherheit erkennen
  ◊ Cloud Softwarevalidierung und -prüfung verstehen
  ◊ Nutzung von verifizierter Software
  ◊ Den Software Development Life Cycle (SDLC) Prozess verstehen
  ◊ Den Secure Software Development Life Cycle anwenden
  ◊ Die Spezifika der Cloud Applikationsarchitektur verstehen
  ◊ Angemessene Identity & Access Management (IAM) Lösungen entwickeln

♦ **Domäne 5: Betrieb von Cloud-Instanzen** ~ 16 %
- ♦ ◊ Den Planungsprozess für Cloud Data Center begleiten
  ◊ Implementierung und Aufbau physischer Infrastrukturen für die Cloud
  ◊ Betrieb physischer Infrastrukturen für die Cloud
  ◊ Verwaltung physischer Infrastrukturen für die Cloud
  ◊ Management logischer Infrastrukturen für die Cloud
  ◊ Sicherstellung der Compliance mit regulatorischen Anforderungen und Controls
  ◊ Durchführung von Risk Assessments an logischen oder physischen Infrastrukturen
  ◊ Sammlung und Schutz von Digital Evidence
  ◊ Kommunikation mit relevanten Partnern

♦ **Domäne 6: Rechtliche Fragen und Compliance** ~ 13 %
- ♦ ◊ Rechtliche Anforderungen und Risiken der Cloud
  ◊ Datenschutz und Varianzen der Jurisdiktion
  ◊ Den Auditprozess und seine Methodologien auf die Cloud anwenden
  ◊ Die Implikationen der Cloud auf das Enterprise Risk Management verstehen
  ◊ Outsourcing und Cloud-Vertragsdesign verstehen
  ◊ Vendor Management ausüben

♦ **Systematische Prüfungsvorbereitung**
- ♦ ◊ Umfang und roter Faden für die Prüfungsvorbereitung
  ◊ Vorstellung der Materialien zur Prüfungsvorbereitung
  ◊ Diskussion der Beispiel-Fragen auf Prüfungs-Niveau
  ◊ Mindset für die Vorbereitung und die Prüfung
  ◊ Rolle/Verantwortung - aus der die Fragen in der Prüfung i.d.R. zu beantworten sind
  ◊ Strategie/Taktiken zur Beantwortung der Fragen
  ◊ Zeitmanagement für die Prüfung

♦ **Hinzu kommen ein Review und Q&A Sessions, und es werden Tipps und Lernmethoden aufgezeigt.**
- ♦