CCSP – Certified Cloud Security Professional

Course Outline

1) Cloud Concepts Architecture and Design

- State the essential characteristics of cloud computing
- Describe the fundamental cloud computing services
- Describe the cloud computing reference architectures
- Explain cloud computing activities
- Compare cloud service capabilities and models
- Describe cloud deployment models
- Summarize economic characteristics of cloud computing
- Evaluate cloud computing ROI and KPI metrics
- Summarize cloud computing security concepts
- Describe key security considerations for each service model
- Analyze key cloud service provider contractual relationship documents

2) Cloud Governance Legal Risk and Compliance

- Explain the issues with international conflict of law
- Interpret guidelines for digital forensics
- Identify the fundamentals of data privacy regulatory/legislative mandates
- Summarize audit process, methodologies and cloud-ready adaptations
- Describe risk management related to cloud services
- Identify due care/diligence activities related to service contracts

3) Cloud Data Security

- Discuss cloud data security concepts
- Describe cryptography
- Explain data discovery and classification technologies
- Interpret cloud data storage architectures
- Analyze information rights management
- Assess cloud data security strategies
- Compare solutions for cloud data retention, deletion and archival policies
- Explain basic security concepts in the cloud

4) Cloud Platform and Infrastructure Security

- Compare cloud infrastructure components
- Select standard practices for implementing a secure data center design
- Assess risks, vulnerability, threats and attacks in the cloud environment
- Discover components for planning and implementing security controls
- Evaluate the design and plan for cloud infrastructure security controls
- Appraise appropriate identity and access management (IAM) solutions
- Recommend business continuity and disaster recovery (BCDR) standards

5) Cloud Application Security

- Explain training and awareness solutions for application security
- Assess challenges in the secure software development life cycle (SDLC) process

- Select a threat model for securing software development
- Demonstrate cloud software assurance and validation
- Choose verified secure software
- Explain the specifics of a cloud application architecture

6) Cloud Security Operations

- Analyze what is used to manage and operate physical and logical infrastructure of a cloud environment
- Discuss operational controls and standards
- Identify methodologies for supporting digital forensics
- Identify critical communication needs with relevant parties
- Define auditability, traceability and accountability of security-relevant data events
- Select requirements to implement secure operations