Certified Cloud Security Professional (CCSP)

Overview:

In this constantly evolving and not to forget extremely competing world of cloud, one faces unique security challenges on almost day-to-day basis with regards to unaccustomed threats to sensitive data or a less equipped internal team.

CCSP certification course at RPS targets to pass on the understanding of information, cyber, software and cloud computing infrastructure security. Explaining the cloud computing concepts, cloud reference architecture, cloud computing security concepts and cloud services are the focus area of the Certified Cloud Security Professional course delivery.

Therefore, an earned CCSP certification helps you prove to yourself and your employers about the in-depth knowledge, understanding and hands on experience that you have achieved with cloud security architecture, design, operations and service orchestration.
Upon course completion, you will accomplish:
Instant Credibility and Differentiation
Unique recognition
Fill the unknown gap in your knowledge and helps you stay ahead
Career Advancement
Ensures you're better equipped to protect sensitive data in a global environment.

Pre-requisite:

The candidates who are enrolling for this course must have five years of working experience in the field of Information security and also with CCSP CBK domains. All those who fail to fulfil the eligibility criteria can take the exam to become an associate of (ISC)2 and can start working towards getting the experience to get the desired certification.

Course Objective:

After completing this course, you will be able to:

- Describe the physical and virtual components of and identify the principle technologies of cloud based systems.
- Define the roles and responsibilities of customers, providers, partners, brokers and the various technical professionals that support cloud computing environments.
- Identify and explain the five characteristics required to satisfy the NIST definition of cloud computing.
- Differentiate between various as a Service delivery models and frameworks that are incorporated into the cloud computing reference architecture.
- Discuss strategies for safeguarding data, classifying data, ensuring privacy, assuring compliance with regulatory agencies and working with authorities during legal investigations.
- Contrast between forensic analysis in corporate data centre and cloud computing environments.
- Evaluate and implement the security controls necessary to ensure confidentiality, integrity and availability in cloud computing.
- Identify and explain the six phases of the data lifecycle.
- Explain strategies for protecting data at rest and data in motion.
- Describe the role of encryption in protecting data and specific strategies for key management.

- Compare a variety of cloud based business continuity / disaster recovery strategies and select an appropriate solution to specific business requirements.
- Contrast security aspects of Software Development Life Cycle in standard data center and cloud computing environments.
- Describe how federated identity and access management solutions mitigate risks in cloud computing systems.
- Conduct gap analysis between baseline and industry standard best practices.
- Develop Service Level Agreements (SLA) for cloud computing environments.
- Conduct risk assessments of existing and proposed cloud-based environments.
- State the professional and ethical standards of (ISC)^2 and the Certified Cloud Security Professional.

Course Content:

Domain 1: Cloud Concepts, Architecture, and Design (17%)

- Understand cloud computing concepts
- Describe cloud reference architecture
- Understand security concepts relevant to cloud computing
- Understand design principles of secure cloud computing
- Evaluate cloud service providers

Domain 2: Cloud Data Security (20%)

- Describe cloud data concepts
- Design and implement cloud data storage architectures
- Design and apply data security technologies and strategies
- Implement data discovery
- Plan and implement data classification
- Design and implement Information Rights Management (IRM)
- Plan and implement data retention, deletion and archiving policies
- Design and implement auditability, traceability and accountability of data events

Domain 3: Cloud Platform & Infrastructure Security (17%)

- Comprehend cloud infrastructure and platform components
- Design a secure data center
- Analyze risks associated with cloud infrastructure and platforms
- Plan and implementation of security controls
- Plan business continuity (BC) and disaster recovery (DR)

Domain 4: Cloud Application Security (17%)

- Advocate training and awareness for application security
- Describe the Secure Software Development Life Cycle (SDLC) process
- Apply the Secure Software Development Life Cycle (SDLC)
- Apply cloud software assurance and validation
- Use verified secure software
- Comprehend the specifics of cloud application architecture
- Design appropriate Identity and Access Management (IAM) solutions

Domain 5: Cloud Security Operations (16%)

- Build and implement physical and logical infrastructure for cloud environment
- Operate and maintain physical and logical infrastructure for cloud environment
- Implement operational controls and standards (e.g., Information Technology Infrastructure Library (ITIL), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 20000-1)
- Support digital forensics
- Manage communication with relevant parties
- Manage security operations

Domain 6: Legal, Risk and Compliance (13%)

- Articulate legal requirements and unique risks within the cloud environment
- Understand privacy issues
- Understand audit process, methodologies, and required adaptations for a cloud environment
- Understand implications of cloud to enterprise risk management
- Understand outsourcing and cloud contract design