Certified Cloud Security Professional (CCSP)

Duration: 40 Hours (5 Days)

Overview

The Certified Cloud Security Professional (CCSP) course is a globally recognized certification program designed for IT and security professionals to validate their expertise in cloud security. It encompasses a comprehensive curriculum that addresses the best practices and standards for securing cloud environments. Through lessons on cloud computing concepts, Cloud reference architecture, and Security principles, learners gain a deep understanding of the architectural concepts and design requirements of cloud systems. The course also delves into Cloud data security, teaching students about Data lifecycle management, protection strategies, and compliance with data protection laws for sensitive information like PII.Further, it covers cloud platform & infrastructure security, emphasizing the importance of disaster recovery and risk management. In Cloud application security, participants learn about Secure software development life-cycle and IAM solutions. The operations module prepares learners to manage cloud infrastructure, ensure Regulatory compliance, and handle digital evidence. Lastly, the legal & compliance section provides insights into legal risks, privacy issues, and Vendor management in the cloud. This comprehensive course equips professionals with the necessary skills to safeguard cloud environments effectively.

Audience Profile

The Certified Cloud Security Professional (CCSP) course is designed for IT professionals seeking specialized skills in cloud security.

- Job roles and audience for the course:
- IT Security Professionals
- Cloud Security Architects
- Cybersecurity Analysts
- Cloud Engineers
- IT Auditors
- Security Consultants
- Network Architects
- System Engineers
- Security Architects
- Enterprise Architects
- Risk Compliance Managers
- Chief Information Security Officers (CISO)
- Data Privacy Officers
- Cloud Consultants
- IT Directors/Managers

Course Syllabus

Architectural Concepts & Design Requirements

- Cloud computing concepts & definitions based on the
- ISO/IEC 17788 standard; security concepts and principles relevant to secure cloud computing.
- Understand Cloud Computing Concepts

- Describe Cloud Reference Architecture
- Understand Security Concepts Relevant to Cloud Computing
- Understand Design Principles of Secure Cloud Computing
- Identify Trusted Cloud Services

Cloud Data Security

- Concepts, principles, structures, and standards used to design, implement,monitor, and secure,
- operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality,
- integrity, and availability in cloud environments.
- Understand Cloud Data Lifecycle
- Design and Implement Cloud Data Storage Architectures
- Design and Apply Data Security Strategies
- Understand and Implement Data Discovery and Classification Technologies
- Design and Implement Relevant Jurisdictional Data Protections for Personally Identifiable Information (PII)
- Design and Implement Data Rights Management
- Plan and Implement Data Retention, Deletion, and Archiving Policies
- Design and Implement Auditability, Traceability and Accountability of Data Events

Cloud Platform & Infrastructure Security

- Knowledge of the cloud infrastructure components,both the physical
- and virtual, existing threats, and mitigating and developing plans to deal with those threats.
- Comprehend Cloud Infrastructure Components
- Analyze Risks Associated to Cloud Infrastructure
- Design and Plan Security Controls
- Plan Disaster Recovery and Business Continuity Management

Cloud Application Security

- Processes involved with cloud software assurance and validation; andthe use of
- verified secure software.
- Recognize the need for Training and Awareness in Application Security
- Understand Cloud Software Assurance and Validation
- Use Verified Secure Software
- Comprehend the Software Development Life-Cycle (SDLC) Process
- Apply the Secure Software Development Life-Cycle
- Comprehend the Specifics of Cloud Application Architecture
- Design Appropriate Identity and Access Management (IAM) Solutions

Operations

- Identifying critical information and the execution of selected measures that eliminate or reduce adversary
- exploitation of it; requirements of cloud architecture to running and managing that infrastructure; definition of controls over
- hardware, media, and the operators with access privileges as well as the auditing and monitoring are the mechanisms, tools
- and facilities.

- Support the Planning Process for the Data Center Design
- Implement and Build Physical Infrastructure for Cloud Environment
- Run Physical Infrastructure for Cloud Environment
- Manage Physical Infrastructure for Cloud Environment
- Build Logical Infrastructure for Cloud Environment
- Run Logical Infrastructure for Cloud Environment
- Manage Logical Infrastructure for Cloud Environment
- Ensure Compliance with Regulations and Controls (e.g., ITIL, ISO/IEC 20000-1)
- Conduct Risk Assessment to Logical and Physical Infrastructure
- Understand the Collection, Acquisition and Preservation of Digital Evidence
- Manage Communication with Relevant Parties

Legal & Compliance

- Addresses ethical behavior and compliance with regulatory frameworks. Includes investigative
- measures and techniques, gathering evidence (e.g., Legal Controls, eDiscovery, and Forensics); privacy issues and audit
- process and methodologies; implications of cloud environments in relation to enterprise risk management.
- Understand Legal Requirements and Unique Risks within the Cloud Environment
- Understand Privacy Issues, Including Jurisdictional Variation
- Understand Audit Process, Methodologies, and Required Adaption's for a Cloud Environment
- Understand Implications of Cloud to Enterprise Risk Management
- Understand Outsourcing and Cloud Contract Design
- Execute Vendor Management