Certificate of Cloud Security Knowledge (CCSK) Foundation

Duration: 16 Hours (2 Days)

Overview

The Certificate of Cloud Security Knowledge (CCSK) Foundation course is an in-depth educational program designed for individuals who want to gain a strong understanding of cloud security. It covers key concepts, best practices, and provides a comprehensive framework for securing cloud environments. Module 1 lays the groundwork by defining cloud computing, exploring Reference and architecture models, and detailing the scope and responsibilities of cloud security. Module 2 delves into Governance, risk management, and the impact of service and deployment models on cloud risks.With a focus on legal issues in Module 3, learners understand data protection laws like the GDPR, cross-border data transfer restrictions, and the complexities of electronic discovery. Modules 4 through 14 cover compliance, Audit management, information Governance, business continuity, infrastructure security, virtualization, incident response, Application security, Data security, Encryption, Identity management, and Security as a Service. The course equips learners with the necessary tools and knowledge to effectively manage security in a cloud computing environment, providing a solid foundation for professionals looking to enhance their skills in the rapidly evolving domain of cloud security.

Audience Profile

The CCSK Foundation course provides in-depth knowledge on cloud security for IT professionals looking to enhance their expertise.

- IT Security Professionals
- Cloud Security Architects
- Governance and Compliance Analysts
- Risk Management Officers
- IT Auditors
- Network Architects
- Cybersecurity Analysts
- Data Privacy Officers
- Legal Professionals specializing in IT
- Cloud Computing Consultants
- Cloud Service Providers
- IT Managers and Administrators
- Incident Response Team Members
- Application Developers with a focus on cloud applications
- Systems Engineers and Administrators
- Enterprise Architects
- Business Continuity and Disaster Recovery Specialists

Course Syllabus

Contents Day 1

1. Cloud computing concepts and Architectures

- Defining Cloud Computing
- Definitional Model
- Reference and Architecture Models
- Logical Model
- Cloud Security Scope, Responsibilities, and Models

2. Governance and Enterprise Risk Management

- Tools of Cloud Governance
- Enterprise Risk Management
- The Effects of Service Model and Deployment Model
- Cloud Risk Management Tools

3. Legal issues, Contracts and Electronic Discovery

- Legal Frameworks Governing Data Protection and Privacy
- Restrictions to Cross-border Data Transfers
- Regional Examples
- EUROPEAN UNION
- AND EUROPEAN
- ECONOMIC AREA
- General Data Protection Regulation (GDPR)
- Contracts and Provider Selection
- Internal Due Diligence
- Monitoring, Testing, and Updating
- External Due Diligence
- Reliance on Third-Party Audits and Attestations
- Electronic Discovery
- Searchability and E-Discovery Tools
- Data Retention Laws and Record Keeping Obligations

4. Compliance and Audit Management

- How Cloud Changes Compliance
- Audit Management
- How Cloud Changes Audit Management

5. Information Governance

- Cloud Information Governance Domains
- The Data Security Lifecycle
- Locations and Entitlements
- Functions, Actors, and Controls

6. Management Plane and Business Continuity

- Business Continuity and Disaster Recovery in the Cloud
- Architect for Failure
- Management Plane Security
- Securing the Management Plane
- Business Continuity Within the Cloud Provider

Contents Day 2

7. Infrastructure Security

- Cloud Network Virtualization
- Challenges of Virtual Appliances
- SDN Security Benefits
- Microsegmentation and the Software Defined Perimeter
- Immutable Workloads

8. Virtualization and Containers

- Cloud Provider Responsibilities
- Cloud User Responsibilities
- Management Infrastructure

9. Incident Response

- Incident Response Lifecycle
- How the Cloud Impacts IR

10. Application Security

- Introduction to the Secure Software Development Lifecycle and
- Cloud Computing
- Impact on Vulnerability Assessment
- Impact on Penetration Testing

11. Data Security and Encryption

- Cloud Data Storage Types
- Managing Data Migrations to the Cloud
- Securing Data in the Cloud

12. Identity, Entitlement and Access Management

- IAM Standards for Cloud Computing

13. Security as a service

14. Related Technologies