CCSK Foundation v5 Curriculum

The CCSK certificate is highly regarded as the benchmark for cloud security expertise. It provides a comprehensive and unbiased understanding of how to effectively secure data in the cloud. Earning the CCSK certificate is the first step in preparing for other cloud certifications. The CCSK will give you the knowledge required to develop a security program that meets international standards. The newly updated certificate will prove your skills in Zero Trust, DevSecOps, Cloud Telemetry and Security Analytics, Artificial Intelligence, and more.

Covering 12 domains of critical cloud security knowledge, this lectures-only class covers the core concepts, best practices, and recommendations for securing an organization on the cloud regardless of the provider or platform.
Course Duration- 2 Days

Domain 1:

Cloud Computing Concepts & Architectures

Describes and defines cloud computing, sets baseline terminology, and details the overall controls, deployment, and architectural models.

● 1.1 Defining Cloud Computing ○ 1.1.1 Abstraction & Orchestration

● 1.2 Cloud Computing Models ○ 1.2.1 Essential Characteristics
○ 1.2.2 Cloud Service Models
○ 1.2.3 Cloud Deployment Models
○ 1.2.4 CSA Enterprise Architecture Model

● 1.3 Cloud Security Scope, Responsibilities, & Models ○ 1.3.1 Shared Security Responsibility Model

Domain 2:

Cloud Governance

Focuses on cloud governance with an emphasis on the role of security and how enterprise governance helps align the strategic, tactical, and operational capabilities of information and technology with the business objectives.

● 2.1. Cloud Governance

● 2.2 The Governance Hierarchy ○ 2.2.1 Aligning with Requirements, Standards, Best Practices, & Contractual Obligations

○ 2.2.2 Consulting with Key Stakeholders for Cloud Security Strategy Alignment

● 2.3 Cloud Security Frameworks ○ 2.3.1 Cloud Controls Matrix

○ 2.3.2 CSA Security, Trust, Assurance, and Risk (STAR) Registry

● 2.4 Policies

Domain 3:

Risk, Audit, & Compliance

Focuses on cloud security, risk, audit, and compliance, including evaluating cloud service providers and establishing cloud risk registries.

● 3.1. Cloud Risk Management ○ 3.1.1 Cloud Risks

○ 3.1.2 Understanding Cloud Risk Management

○ 3.1.3 Assessing Cloud Services

○ 3.1.4 The Cloud Register

● 3.2 Compliance & Audit ○ 3.2.1 Jurisdictions

○ 3.2.2 Cloud-Relevant Laws & Regulations Examples

○ 3.2.3 Compliance Inheritance

○ 3.2.4 Artifacts of Compliance

● 3.3 Governance, Risk, Compliance Tools & Technologies

Domain 4:

Organization Management

Focuses on managing your entire cloud footprint, including securing and validating service provider deployments.

● 4.1 Organization Hierarchy Models ○ 4.1.1 Definitions

○ 4.1.2 Organization Capabilities Within a Cloud Service Provider

○ 4.1.3 Building a Hierarchy Within a Provider

● 4.2 Managing Organization-Level Security Within a Provider ○ 4.2.1 Identity Provider & User/Group/Role Mappings
○ 4.2.2 Common Organization Shared Services

● 4.3 Considerations for Hybrid & Multi-Cloud Deployments ○ 4.3.1 Organization Management for Hybrid Cloud Security
○ 4.3.2 Organization Management for Multi-Cloud Security
○ 4.3.3 Organization Management for SaaS Hybrid & Multi-Cloud

Domain 5:

Identity & Access Management

Focuses primarily on IAM between an organization and cloud providers or between cloud providers and services.

● 5.1 How IAM Is Different in the Cloud
● 5.2 Fundamental Terms
● 5.3 Federation ○ 5.3.1 Common Federation Standards
○ 5.3.2 How Federated Identity Management Works
○ 5.3.3 Managing Users & Identities for Cloud Computing

● 5.4 Strong Authentication & Authorization ○ 5.4.1 Authentication & Credentials
○ 5.4.2 Entitlement & Access Management
○ 5.4.3 Privileged User Management

Domain 6:

Security Monitoring

Presents unique security monitoring challenges and solutions for cloud environments, emphasizing the distinct aspects of cloud telemetry, management plane logs, service and resource logs, and the integration of advanced monitoring tools.

● 6.1 Cloud Monitoring ○ 6.1.1 Logs & Events

● 6.2 Beyond Logs - Posture Management ○ 6.2.1 Management Plane Logs
○ 6.2.2 Service & Application Logs

○ 6.2.3 Resource Logs
○ 6.2.4 Cloud Native Tools

● 6.3 Cloud Telemetry Sources
● 6.4 Collection Architectures ○ 6.4.1 Log Storage & Retention
○ 6.4.2 Cascading Log Architecture

● 6.5 AI for Security Monitoring

Domain 7:
Infrastructure & Networking
Focuses on managing the overall infrastructure footprint and network security, including the CSP's infrastructure security responsibilities.
● 7.1 Cloud Infrastructure Security ○ 7.1.1 Foundational Infrastructure Security Techniques
○ 7.1.2 CSP Infrastructure Security Responsibilities
○ 7.1.3 Infrastructure Resilience

● 7.2 Cloud Network Fundamentals ○ 7.2.1 Cloud Networks are Software-Defined Networks
○ 7.2.2 Cloud Connectivity

● 7.3 Cloud Network Security & Secure Architectures ○ 7.3.1 Preventative Security Measures
○ 7.3.2 Detective Security Measures

● 7.4 Infrastructure as Code (IaC)
● 7.5 Zero Trust for Cloud Infrastructure & Networks ○ 7.5.1 Software-Defined Perimeter & ZT Network Access

● 7.6 Secure Access Service Edge (SASE)

Domain 8:

Cloud Workload Security

Focuses on the related set of software and data units that are deployable on some type of infrastructure or platform.

● 8.1 Introduction to Cloud Workload Security ○ 8.1.1 Types of Cloud Workloads
○ 8.1.2 Impact on Workload Security Controls

● 8.2 Securing Virtual Machines ○ 8.2.1 Virtual Machine Challenges & Mitigations
○ 8.2.2 Creating Secure VM Images with Factories
○ 8.2.3 Snapshots & Public Exposures/Exfiltration

● 8.3 Securing Containers ○ 8.3.1 Container Image Creation
○ 8.3.2 Container Networking
○ 8.3.3 Container Orchestration & Management Systems
○ 8.3.4 Container Orchestration Security
○ 8.3.5 Runtime Protection for Containers

● 8.4 Securing Serverless and Function as a Service ○ 8.4.1 FaaS Security Issues
○ 8.4.2 IAM for Serverless
○ 8.4.3 Environment Variables & Secrets

● 8.5 Securing AI Workloads ○ 8.5.1 AI-System Threats
○ 8.5.2 AI Risk Mitigation and Shared Responsibilities

Domain 9:

Data Security

Addresses the complexities of data security in the cloud, covering essential strategies, tools, and practices for protecting data in transit and at rest.

● 9.1 Primer on Cloud Storage ○ 9.1.1 Volume/Block Storage
○ 9.1.2 Object Storage
○ 9.1.3 Database Storage
○ 9.1.4 Other Types of Storage

● 9.2 Data Security Tools and Techniques ○ 9.2.1 Data Classification
○ 9.2.2 Identity and Access Management
○ 9.2.3 Access Policies
○ 9.2.4 Encryption and Key Management
○ 9.2.5 Data Loss Prevention
● 9.3 Cloud Data Encryption at Rest
○ 9.3.1 Application Level Encryption
○ 9.3.2 Cloud Data Key Management Strategies
○ 9.3.3 Data Encryption Recommendations
● 9.4 Data Security Posture Management
● 9.5 Object Storage Security
● 9.6 Data Security for Artificial Intelligence
○ 9.6.1 AI as a Service

Domain 10:
Application Security
Focuses on the unique challenges and opportunities presented by application security in the cloud environment from the initial design phase to ongoing maintenance.
● 10.1 Secure Development Lifecycle ○ 10.1.1 SDLC Stages
○ 10.1.2 Threat Modeling
○ 10.1.3 Testing: Pre-Deployment
○ 10.1.4 Testing: Post Deployment

● 10.2 Architecture’s Role in Secure Cloud Applications ○ 10.2.1 Cloud Impacts on Architecture-Level Security
○ 10.2.2 Architectural Resilience

● 10.3 Identity & Access Management and Application Security ○ 10.3.1 Secrets Management

● 10.4 Dev Ops & DevSecOps ○ 10.4.1 CI/CD Pipeline and Shift Left
○ 10.4.2 Web Application Firewalls & API Gateways

Domain 11:
Incident Response & Resilience
Focuses on identifying and explaining best practices for cloud incident response and resilience that security professionals may reference when developing their own incident plans and processes.
● 11.1 Incident Response
○ 11.1.1 Incident Response Lifecycle

● 11.2 Preparation ○ 11.2.1 Incident Response Preparation & Cloud Service Providers
○ 11.2.2 Training for Cloud Incident Responders

● 11.3 Detection & Analysis ○ 11.3.1 Cloud Impact on Incident Response Analysis
○ 11.3.2 Cloud System Forensics

● 11.4 Containment, Eradication, & Recovery ○ 11.4.1 Containment
○ 11.4.2 Eradication
○ 11.4.3 Recovery

● 11.5 Post Incident Analysis

Domain 12:
Related Technologies & Strategies
Introduces the foundational concepts and focuses on developing a strategic cybersecurity approach to Zero Trust and Artificial Intelligence.
● 12.1 Zero Trust ○ 12.1.1 Technical Objectives of Zero Trust
○ 12.1.2 Zero Trust Pillars & Maturity Model
○ 12.1.3 Zero Trust & Cloud Security

- 12.2 Artificial Intelligence ○ 12.2.1 Characteristics of AI Workloads ○ 12.1.2 How AI Intersects with Cloud Security

- Next Steps