CCSK v5 Curriculum

CCSK Foundation and CCSK Plus Course Outline

CCSK Foundation v5 Curriculum

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.

Domain 1: **Cloud Computing Concepts & Architectures**

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

- Domain 1: Cloud Computing Concepts & Architectures
- Introduction
- Learning Objectives
- 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
  - 1.2.2.1 Infrastructure as a Service (IaaS)
  - 1.2.2.2 Platform as a Service (PaaS)
  - 1.2.2.3 Software as a Service (SaaS)
  - 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.

- Domain 2: Cloud Governance and Strategies
- Introduction
- Learning Objectives
- 2.1. Cloud Governance
- 2.2 The Governance Hierarchy
  - 2.2.1 Cloud Security Frameworks
  - 2.2.2 Policies

Domain 3:
Risk, Audit, & Compliance

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

- Domain 3: Risk, Audit, & Compliance
- Introduction
- Learning Objectives
- 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.

- Domain 4: Organization, Tenancy, & Enterprise Management
- Introduction
- Learning Objectives
- 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.

- Domain 5: Identity and Access Management
- Introduction
- Learning Objectives
- 5.1 Fundamental Terms
- 5.2 Federation
    - 5.2.1 Common Federation Standards
    - 5.2.2 How Federated Identity Management Works
    - 5.2.3 Managing Users & Identities for Cloud Computing
- 5.3 Strong Authentication & Authorization
    - 5.3.1 Authentication & Credentials
    - 5.3.2 Entitlement & Access Management
    - 5.3.3 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.

- Domain 6: Security Monitoring
- Introduction
- Learning Objectives
- 6.1 Cloud Monitoring
    - 6.1.1 Logs & Events
- 6.2 Beyond Logs - Posture Management
- 6.3 Cloud Telemetry Sources
    - 6.2.1 Management Plane Logs
    - 6.2.2 Service & Application Logs
    - 6.2.3 Resource Logs
    - 6.2.4 Cloud Native Tools
- 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.

- Domain 7: Infrastructure & Networking
- Introduction
- Learning Objectives
- 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

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.

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.

- Domain 9: Data Security
- Introduction
- Learning Objectives
- 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 Cloud Data Key Management Strategies
  - 9.3.2 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.

- Domain 10: Application Security
- Introduction
- Learning Objectives
- 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

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.

- Domain 11: Incident Response
- Introduction
- Learning Objectives
- 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.

- Domain 12: Related Technology and Strategies
- Introduction

- Learning Objectives
- 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
    - Next Steps

Learn More about CCSK Foundation

To learn more about the CCSK Foundation course structure, benefits, and available classes, visit https://cloudsecurityalliance.org/education/ccsk.

CCSK Plus v5 Curriculum

The CCSK Plus contains all the material in the foundation course with the addition of hands-on labs.

The CCSK Plus builds on the foundation class with expanded material and offers extensive hands-on activities that reinforce classroom instruction. Students engage in a scenario of bringing a fictional organization securely into the cloud, which gives them the opportunity to apply their knowledge by performing a series of activities that would be required in a real-world environment. Labs are available in either Azure or AWS.

Lab Material Outline

Core Account Security

Learn what to configure in the first 5 minutes of opening a new cloud account and enable security controls such as MFA, basic monitoring, and IAM.

IAM & Monitoring In-Depth

Expand on your work in the first lab and implement more-complex identity management and monitoring. This includes expanding IAM with Attribute Based Access Controls, implementing security alerting, and understanding how to structure enterprise-scale IAM and monitoring.

Network & Instance Security

Create a virtual network (VPC) and implement a baseline security configuration. You will also learn how to securely select and launch a virtual machine (instance), run a vulnerability assessment in the cloud, and connect to the instance.

Encryption & Storage Security

Expand your deployment by adding a storage volume encrypted with a customer managed key. You will also learn how to secure snapshots and other data.

Application Security & Federation

Finish the technical labs by completely building out a 2-tier application and implementing federated identity using OpenID.

Risk & Provider Assessment

Practice using the CSA Cloud Controls Matrix and STAR registry to evaluate risk and select a cloud provider.

Learn More about CCSK Plus

To learn more about the CCSK Plus course structure, benefits, and available classes, visit https://cloudsecurityalliance.org/education/ccsk-plus.