COURSE SYLLABUS

CCSK Exam Preparation Course (Self-Paced)

Build the vendor-neutral cloud security knowledge the current CCSK exam covers, from architecture to Zero Trust and AI.

> Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/ccsk-exam-preparation-course-self-paced



support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: Cloud Computing Concepts and Architectures

- Lessons:
  - Cloud Service Models and Deployment Models
  - The Shared Responsibility Model and the CSA Enterprise Architecture Model
  - Cloud Actors, Roles, and Core Terminology
- Applied activity: Given a short scenario describing an organization's planned use of three different cloud services, learners identify which service model applies to each and mark which security responsibilities sit with the provider versus the customer.

Module 2: Cloud Governance

- Lessons:
  - Governance Structures and Strategic Alignment
  - Policy Creation and Ownership
  - Vendor Management and Multi-Cloud Compliance
- Applied activity: Learners review a described multi-cloud vendor relationship and identify one governance policy gap that would need to be closed before onboarding a second provider.

Module 3: Risk, Audit, and Compliance

- Lessons:
  - Cloud Risk Management and Risk Registries
  - Evaluating Cloud Service Providers and Audit Scope
  - Compliance, Jurisdiction, and the Cloud Controls Matrix
- Applied activity: Learners use a simplified Cloud Controls Matrix excerpt to check whether a described provider's published controls cover a specific compliance requirement, and log the result in a short risk registry entry.

Module 4: Organization Management

- Lessons:
  - Managing a Cloud Footprint Across Providers
  - Cloud Security Roles and the Management Plane
  - Shadow IT and Governance Gaps
- Applied activity: Learners review a described scenario in which a business unit adopts a cloud service outside of IT's visibility and recommend one step to bring it under governance.

Module 5: Identity and Access Management

- Lessons:
  - Identity Verification and Federation
  - Access Controls and Least Privilege
  - IAM Coordination Between Organization and Provider
- Applied activity: Learners review a described set of user entitlements against actual job duties and identify which permissions should be removed.

Module 6: Security Monitoring

- Lessons:
  - Monitoring Techniques and Telemetry Collection
  - Cloud Security Posture Management
  - AI Assisted Monitoring and Alert Triage
- Applied activity: Learners review a described set of monitoring alerts and prioritize which one to investigate first, explaining why.

Module 7: Infrastructure and Networking

- Lessons:
  - Cloud Network Fundamentals and Infrastructure as Code
  - Zero Trust Principles in the Cloud
  - Secure Access Service Edge
- Applied activity: Learners review a described cloud network diagram built on a perimeter based model and identify one change that would move it toward a Zero Trust design.

Module 8: Cloud Workload Security

- Lessons:
  - Securing Virtual Machines and Containers
  - Serverless Workload Security
  - Securing AI Application Workloads
- Applied activity: Learners review a described container deployment pipeline and identify the point where an image scan should be added to catch a known vulnerability before deployment.

Module 9: Data Security

- Lessons:
  - Cloud Storage Security and the Data Lifecycle
  - Encryption and Key Management
  - AI Specific Data Security Considerations
- Applied activity: Learners review a described cloud storage configuration and identify whether encryption and key management meet a stated data sensitivity requirement.

Module 10: Application Security

- Lessons:
  - Secure Development Practices and Architecture Design
  - Application Security Testing Approaches
  - DevSecOps and CI/CD Security
- Applied activity: Learners review a described continuous integration pipeline and recommend where to insert a security testing gate without stalling releases.

Module 11: Incident Response and Resilience

- Lessons:
  - Cloud Incident Response Best Practices
  - Provider and Customer Response Roles
  - Organizational Recovery and Resilience Planning
- Applied activity: Learners work through a short cloud incident scenario and decide which response steps they can take directly and which require opening a request with the cloud provider.

Module 12: Related Technologies and Strategies

- Lessons:
  - Zero Trust as a Strategic Approach
  - Artificial Intelligence and Generative AI in the Cloud
  - Bringing It Together: Study Priorities Across the 12 Domains
- Applied activity: Learners evaluate a described generative AI feature being added to a cloud application and identify one new security consideration it introduces that a traditional feature would not.