COURSE SYLLABUS

Cloud Security Certificate Program

A two-course live path through federal cloud security: fundamentals and FedRAMP context, then architecture and hardening taught against real recent cloud breaches.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/certificates/cloud-security-certificate-program

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

Course Outline

This package includes these courses

- Cloud Security Fundamentals for Federal Employees (6 Hours)
- Cloud Security Architecture & Hardening: Build It Secure, Keep It Secure Course (10 Hours)

Cloud Security Fundamentals for Federal Employees

A jargon-free grounding in how federal cloud services get secured and where one party's responsibility ends and the other's begins.

- Describe cloud service models and the core concepts behind federal cloud use
- Explain what FedRAMP does within federal cloud governance
- Put the shared responsibility model to work against real scenarios
- Identify the essential identity, access, and data-protection practices in the cloud
- Describe secure configuration and vulnerability management
- Explain cloud monitoring, incident reporting, and risk response

Cloud Security Architecture & Hardening: Build It Secure, Keep It Secure Course

An intermediate, two-part cloud security course separating secure design from secure operations, anchored to real recent cloud breaches.

- Cloud security architecture, trust boundaries, and shared responsibility applied to real control ownership
- Human versus workload identity, least privilege, and entitlement management
- Segmented cloud networks and Zero Trust per NIST SP 800-207 and 800-207A
- Data protection at rest, in transit and in processing, and the key lifecycle
- Secure configuration baselines and drift detection
- Hardening compute, containers and serverless workloads, images and registries
- Application and API security, service-to-service trust, and secrets handling

- Logging and detection coverage across identity, network, workload and admin activity
- Resilience, recovery, and preparing for compromised identities and trust anchors
- Producing and defending a prioritized cloud-hardening plan