COURSE SYLLABUS

Cloud Security Certificate Program (Self-Paced)

A two-course self-paced path through federal cloud security: the fundamentals and FedRAMP context first, then cloud security architecture and hardening built on real recent 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-self-paced

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

Course Outline

This package includes these courses

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

Cloud Security Fundamentals for Federal Employees (Self-Paced)

As agencies shift workloads to the cloud, the whole workforce needs a working grasp of how cloud security differs from on-premises security. This foundational course covers cloud service models, FedRAMP's role in federal cloud governance, and the shared responsibility model, then moves through identity and data protection, secure configuration, vulnerability management, and monitoring and incident reporting, closing with a capstone that evaluates a federal cloud service.

- Describe cloud service models and core federal cloud concepts
- Explain FedRAMP's role in federal cloud governance
- Apply the shared responsibility model to real scenarios
- Identify core 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 (Self-Paced)

Intermediate cloud security in two parts — designing the secure cloud, then hardening the workloads and operations — taught against real recent cloud breaches.

- Trust boundaries, shared responsibility, and real control ownership
- Human, workload and service identities, least privilege, and entitlement management

- Network segmentation and Zero Trust per NIST SP 800-207 and 800-207A
- Data protection at rest, in transit and in processing, and key lifecycle management
- Secure configuration baselines and configuration drift detection
- Compute, container and serverless hardening, with image and registry protection
- Application and API security, service-to-service trust, and secrets handling
- Security logging and detection across identity, network, workload and admin activity
- Resilience, recovery, and readiness for compromised identities and accounts
- Building and defending a prioritized cloud-hardening plan