COURSE SYLLABUS

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.

> 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/cloud-security-fundamentals-for-federal-employees



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

Course Outline

Module 1: Federal Cloud Concepts and Service Models

Review cloud computing fundamentals and compare Infrastructure as a Service, Platform as a Service, and Software as a Service models for federal use.

Module 2: Federal Cloud Governance and FedRAMP Fundamentals

Examine how FedRAMP establishes standardized security assessment, authorization, and continuous monitoring requirements for federal cloud services.

Module 3: Shared Responsibility and Agency Accountability

Define security responsibilities across cloud service providers and federal agencies and identify areas of shared accountability.

Module 4: Identity, Access, and Data Protection in the Cloud

Apply identity and access management principles and data protection practices within federal cloud environments.

Module 5: Secure Cloud Configuration and Vulnerability Management

Implement secure configuration, system hardening, vulnerability scanning, and remediation practices for cloud services.

Module 6: Cloud Monitoring, Incident Reporting, and Risk Response

Monitor cloud environments, report security incidents, and coordinate risk response activities between providers and agencies.

Module 7: Evaluating a Federal Cloud Service Capstone

Assess a cloud service for federal use by evaluating its service model, security responsibilities, controls, monitoring capabilities, and risk considerations.