COURSE SYLLABUS

Cloud & FedRAMP Authorization Certificate Program

Assess, authorize, and sustain secure federal cloud services — and stay ahead of FedRAMP's move to the 20x model.

> 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-and-fedramp-authorization-certificate-program

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

Course Outline

This package includes these courses

- Cloud Security Fundamentals for Federal Employees (6 Hours)
- FedRAMP for Agency Buyers: Authorization Process and Cloud Service Selection (Intermediate) Course (12 Hours)
- FedRAMP for Agency Buyers: Package Due Diligence and Cloud Security Program Management (Advanced) Course (18 Hours)
- FedRAMP Modernization: Transitioning from Rev5 to 20x & CR26 (12 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

FedRAMP for Agency Buyers: Authorization Process and Cloud Service Selection (Intermediate) Course

This course gives federal program managers, contracting officers, and ISSOs what they need in practice to weigh FedRAMP-authorized cloud services, drive the agency ATO process, and stay on top of continuing compliance obligations. Participants learn to review FedRAMP security packages, document shared responsibility, and oversee continuous monitoring across the cloud service lifecycle.

- FedRAMP authorization framework, covering JAB versus Agency ATO paths, impact levels, and the FedRAMP Marketplace.
- Security package review: weighing SSPs, SARs, and POA&Ms for cloud service selection and risk acceptance.
- Shared responsibility and control inheritance documentation between agencies and cloud service providers.
- Agency ATO development for FedRAMP-authorized services, covering residual risk identification and AO risk acceptance.
- FedRAMP continuous monitoring obligations, covering monthly vulnerability scans, significant change notifications, and annual assessments.
- Cloud incident response under FedRAMP shared obligations, including US-CERT notification and CSP coordination.

FedRAMP for Agency Buyers: Package Due Diligence and Cloud Security Program Management (Advanced) Course

This advanced course develops the execution command and enterprise leadership needed to run a federal cloud security program at scale. Participants carry out deep authorization package due diligence, weigh CSP accountability, engineer customer responsibility documentation, and build the governance structures that keep cloud security risk in view across multi-CSP federal portfolios.

- Authorization package due diligence: SSP and SAR analysis, penetration test report review, and POA&M health assessment.
- Customer Responsibility Matrix engineering: spotting inherited control gaps and writing agency supplemental documentation.
- Agency ATO documentation for FedRAMP-leveraged systems, covering residual risk assessment and interconnection documentation.
- FedRAMP continuous monitoring program design, covering CSP deliverable oversight, significant change notifications, and escalation procedures.
- Enterprise cloud security governance, covering portfolio risk aggregation, vendor management, and executive-level reporting.
- Procurement strategy and contractual cloud security protections, covering incident response SLAs, data portability, and supply chain risk provisions.

FedRAMP Modernization: Transitioning from Rev5 to 20x & CR26

Get clear on what FedRAMP's shift to 20x and the Consolidated Rules for 2026 actually change, and leave with a transition roadmap. Timed to the January 1, 2027 CR26 deadline.

- Explain CR26 and the FedRAMP modernization timeline running through 2028
- Set Rev5 authorization against 20x certification
- Describe the new certification classes and what changes about boundaries
- Modernize packages around Security Decision Records and structured data
- Put Key Security Indicators and automated validation to work
- Draft a Rev5-to-20x transition roadmap