COURSE SYLLABUS

Cloud & FedRAMP Authorization Certificate Program (Self-Paced)

Evaluate, authorize, and maintain secure federal cloud services — and get ahead of FedRAMP's move to the 20x model.

> 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/certificates/cloud-and-fedramp-authorization-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)
- FedRAMP for Agency Buyers: Authorization Process and Cloud Service Selection Course (Self-Paced) (12 Hours)
- FedRAMP for Agency Buyers: Package Due Diligence and Cloud Security Program Management Course (Self-Paced) (18 Hours)
- FedRAMP Modernization: Transitioning from Rev5 to 20x & CR26 (Self-Paced) (12 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

FedRAMP for Agency Buyers: Authorization Process and Cloud Service Selection Course (Self-Paced)

This course equips federal program managers, contracting officers, and ISSOs with the practical skills to evaluate FedRAMP-authorized cloud services, execute the agency ATO process, and manage ongoing compliance obligations. Participants learn to

review FedRAMP security packages, document shared responsibility, and oversee continuous monitoring throughout the cloud service lifecycle.

- FedRAMP authorization framework, including JAB vs. Agency ATO paths, impact levels, and the FedRAMP Marketplace.
- Security package review: evaluating 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, including residual risk identification and AO risk acceptance.
- FedRAMP continuous monitoring obligations, including 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 Course (Self-Paced)

This advanced course develops the execution mastery and enterprise leadership skills needed to manage a federal cloud security program at scale. Participants conduct deep authorization package due diligence, evaluate CSP accountability, engineer customer responsibility documentation, and build the governance structures required to manage cloud security risk 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: identifying inherited control gaps and developing agency supplemental documentation.
- Agency ATO documentation for FedRAMP-leveraged systems, including residual risk assessment and interconnection documentation.
- FedRAMP continuous monitoring program design, including CSP deliverable oversight, significant change notifications, and escalation procedures.
- Enterprise cloud security governance, including portfolio risk aggregation, vendor management, and executive-level reporting.
- Procurement strategy and contractual cloud security protections, including incident response SLAs, data portability, and supply chain risk provisions.

FedRAMP Modernization: Transitioning from Rev5 to 20x & CR26 (Self-Paced)

Understand what FedRAMP's move to 20x and the Consolidated Rules for 2026 change, and build a transition roadmap. Timed to the January 1, 2027 CR26 deadline.

- Explain CR26 and the FedRAMP modernization timeline through 2028
- Contrast Rev5 authorization with 20x certification
- Describe the new certification classes and boundary changes
- Modernize packages using Security Decision Records and structured data
- Apply Key Security Indicators and automated validation
- Build a Rev5-to-20x transition roadmap