COURSE SYLLABUS

Federal Cybersecurity Authorization Professional: Cloud & FedRAMP Authorization Certificate Program

Build the RMF core first, then specialize in authorizing and sustaining secure federal cloud services.

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/federal-cybersecurity-authorization-professional-cloud-and-fedramp-authorization

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

Course Outline

This package includes these courses

- RMF Foundations: From Risk to Authorization (8 Hours)
- NIST 800-53: Control Selection, Implementation, and Security Planning Course (12 Hours)
- FISMA & Continuous Monitoring Fundamentals Course (8 Hours)
- 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)

RMF Foundations: From Risk to Authorization

Work through every stage of the NIST Risk Management Framework, from setting a system's impact level to signing off on its authorization to operate.

- Describe what the NIST RMF is for and how it ties risk to an authorization decision
- Recognize the principal RMF roles and what each one is accountable for
- Set a system's impact level using FIPS 199
- Choose and tailor a control baseline against NIST SP 800-53B
- Trace how controls are implemented, assessed, and documented
- Read an authorization decision and the residual risk it accepts
- Account for the part continuous monitoring plays in keeping an authorization current

NIST 800-53: Control Selection, Implementation, and Security Planning Course

This course gives federal security practitioners what they need to choose, tailor, and document NIST SP 800-53 Rev 5 controls for federal information systems. Participants write implementation statements across the highest-impact control families, prepare evidence that will stand up to assessment, and produce compliant POA&M entries rooted in 800-53A assessment procedures.

- Baseline selection and tailoring drawn from NIST SP 800-53B, covering scoping guidance, compensating controls, and organization-defined parameters.
- SSP implementation statements for the AC, IA, AU, CM, IR, and SC control families that satisfy 800-53A evidence sufficiency standards.
- Privacy controls and Supply Chain Risk Management (SR) family requirements for the federal systems they apply to.
- Assessment readiness through 800-53A procedures, covering evidence collection standards and finding severity classification.
- POA&M development with milestone tracking, resource estimates, and a clear link to FISMA reporting.

FISMA & Continuous Monitoring Fundamentals Course

An ATO is a beginning, not an ending — federal systems must be watched continuously, with weaknesses tracked and risk reported to leadership over time. This intermediate course grounds Information Security Continuous Monitoring (NIST SP 800-137) in FISMA accountability: design an ISCM strategy, work findings through POA&Ms, and build the metrics and reporting that make ongoing authorization possible.

- Explain how FISMA assigns accountability and structures oversight
- Design an ISCM strategy that aligns to NIST SP 800-137
- Put asset, configuration, and vulnerability visibility in place
- Keep control assessment and supporting evidence current
- Produce security metrics and risk reporting aimed at leadership
- Work findings and POA&Ms in priority order, driven by risk
- Describe ongoing authorization and how an ISCM program gets evaluated

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