COURSE SYLLABUS

Federal Cybersecurity Authorization Professional: Cloud & FedRAMP Authorization Certificate Program (Self-Paced)

Master the RMF core, then specialize in authorizing and maintaining secure federal cloud services.

> 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/federal-cybersecurity-authorization-professional-cloud-and-fedramp-authorization-self-paced



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

Course Outline

This package includes these courses

- RMF Foundations: From Risk to Authorization (Self-Paced) (6 Hours)
- NIST 800-53: Control Selection, Implementation, and Security Planning Course (Self-Paced) (12 Hours)
- FISMA & Continuous Monitoring Fundamentals Course (Self-Paced) (6 Hours)
- 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)

RMF Foundations: From Risk to Authorization (Self-Paced)

Learn the full NIST Risk Management Framework lifecycle, from categorizing a system to authorizing it to operate.

- Explain the purpose of the NIST RMF and how it links risk to authorization
- Identify the key RMF roles and their responsibilities
- Categorize a system's impact level using FIPS 199
- Select and tailor a control baseline using NIST SP 800-53B
- Describe how controls are implemented, assessed, and documented
- Interpret an authorization decision and residual-risk acceptance
- Explain continuous monitoring's role in maintaining an authorization

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

Paced)

This course equips federal security practitioners with the skills to select, tailor, and document NIST SP 800-53 Rev 5 controls for federal information systems. Participants build implementation statements across the highest-impact control families, prepare assessment-ready evidence, and develop compliant POA&M entries grounded in 800-53A assessment procedures.

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

FISMA & Continuous Monitoring Fundamentals Course (Self-Paced)

An authorization to operate isn't the finish line—federal systems must be monitored 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: you'll design an ISCM strategy, manage findings through POA&Ms, and build the metrics and reporting that support ongoing authorization.

- Explain FISMA accountability and oversight structures
- Design an ISCM strategy aligned to NIST SP 800-137
- Establish asset, configuration, and vulnerability visibility
- Manage ongoing control assessment and evidence
- Build security metrics and risk reporting for leadership
- Manage findings and POA&Ms with a risk-based approach
- Describe ongoing authorization and how to evaluate an ISCM program

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