COURSE SYLLABUS

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

Assess FedRAMP-authorized cloud services, drive the agency ATO process, and hold shared security responsibilities together across the service lifecycle.

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/fedramp-for-agency-buyers-authorization-process-and-cloud-service-selection-course



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

Course Outline

Module 1: FedRAMP Authorization Framework and Policy Landscape

- FedRAMP Modernization Act (2022): statutory authority, PMO structure, and accelerated authorization requirements.
- Authorization paths: JAB Provisional ATO, Agency ATO, and FedRAMP Connect program.
- FedRAMP impact levels: Low, Moderate, High, and LI-SaaS, including selection criteria and compliance implications.
- Cloud service provider obligations: continuous monitoring, significant change notification, and annual assessment requirements.
- FedRAMP Rev 5 transition: 800-53 Rev 5 alignment timeline and new control requirements.

Module 2: FedRAMP Marketplace – Service Evaluation and Risk-Informed Selection

- FedRAMP Marketplace navigation: search criteria, authorization status indicators, and package availability.
- Evaluating authorized service listings: CSP contact information, authorization date, 3PAO name, and package currency.
- Risk-informed cloud service selection: aligning impact level with data classification, user population, and mission criticality.
- Comparing CSP security postures: using SAR findings and POA&M aging as selection inputs.
- Procurement integration: incorporating FedRAMP requirements into RFIs, RFPs, and contract evaluation criteria.

Module 3: FedRAMP Security Package Review – SSP, SAR, and POA&M

- FedRAMP SSP structure: system description, boundary diagram, control implementation statements, and customer responsibility matrix.
- Reviewing control implementation quality: what to look for in CSP-provided vs. customer-responsible control sections.
- Security Assessment Report (SAR) analysis: finding severity distribution, 3PAO methodology, and open risk items.
- POA&M review: aging items, false positive justifications, milestone credibility, and risk acceptance documentation.
- Package red flags: indicators of inadequate security, stale documentation, or assessment scope limitations.

Module 4: Shared Responsibility – Control Inheritance and Customer Obligations

- FedRAMP shared responsibility model: inherited, shared, and customer-owned controls.
- Customer Responsibility Matrix (CRM): how to read it, what it requires agencies to implement.

- Inheriting controls from IaaS/PaaS to SaaS: multi-tier inheritance chains and documentation requirements.
- Customer-responsible control implementation: commonly missed controls (AC-2, AU-2, IR-6).
- Documenting inherited controls in the agency SSP: required detail level.

Module 5: Agency ATO Process for FedRAMP-Authorized Services

- Agency ATO leverage: using the FedRAMP package as the foundation, distinguishing what's inherited from what's new.
- Residual risk identification and agency risk acceptance: what the AO is accepting.
- System Security Plan additions: agency-specific controls, boundary additions, and data flow documentation.
- Security Assessment scope for agency ATOs: what requires reassessment vs. what can leverage 3PAO work.
- ATO documentation requirements: FedRAMP-specific elements for agency authorization packages.

Module 6: FedRAMP Continuous Monitoring – Vulnerability Management and Annual Assessments

- FedRAMP continuous monitoring requirements: monthly vulnerability scans, annual penetration testing, and configuration compliance.
- Reviewing CSP continuous monitoring deliverables: what agencies should verify in monthly scan results.
- Significant change notifications: what triggers a notification and agency review obligations.
- Annual assessment cycle: 3PAO scope, methodology, and year-over-year changes.
- CSP non-compliance: escalation procedures and revocation of agency authorization.

Module 7: Cloud Incident Response Under FedRAMP Shared Obligations

- FedRAMP incident reporting requirements: 1-hour detection notification and US-CERT reporting elements.
- Shared incident response: what agencies do vs. what CSPs do, including roles, timelines, and escalation procedures.
- Evidence preservation in cloud incidents: cloud-specific forensics challenges and CSP cooperation requirements.
- Agency obligations when a CSP has an incident: data breach notification and alternative processing.
- Coordinating with CISA and US-CERT during a cloud security incident affecting federal data.

Module 8: Multi-Cloud, Integration Scenarios, and FedRAMP Compliance Capstone

- Multi-cloud and hybrid environments: authorization strategy for complex deployment architectures.
- FedRAMP and AI/ML services: emerging requirements for cloud-based AI platforms processing federal data, as a preview of the Advanced course.
- Containerized workloads: boundary documentation challenges, as a preview of the Advanced course.
- Third-party APIs and integrations: FedRAMP applicability and inherited risk.