COURSE SYLLABUS

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

Conduct deep FedRAMP package due diligence, manage CSP accountability and continuous monitoring obligations, and design enterprise governance programs for multi-cloud federal portfolios.

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/courses/fedramp-for-agency-buyers-package-due-diligence-and-cloud-security-program-management-advanced-course-self-paced

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

Course Outline

Module 1: Authorization Package Deep Due Diligence – SSP and SAR Analysis

- SSP completeness assessment: critical fields, control implementation statement quality, and boundary documentation adequacy.
- SAR structure and quality indicators: assessment scope coverage, finding severity calibration, and evidence documentation standards.
- Reading SAR findings critically: distinguishing material vs. administrative findings, and assessing remediation commitments.
- CSP assessment team qualifications: 3PAO accreditation, assessor independence, and conflict-of-interest flags.
- Package age and currency: when a package is too old to rely on and how to request updated evidence from CSPs.

Module 2: Penetration Test Report Analysis and Risk Acceptance

- FedRAMP penetration test requirements: scope, methodology, and reporting standards per FedRAMP Penetration Test Guidance.
- Reading pen test findings: CVSS scoring, exploitability context, and remediation commitment adequacy.
- High and Critical pen test findings: when they block authorization vs. when they can be accepted with conditions.
- CSP pen test remediation tracking: POA&M integration, re-test requirements, and agency notification obligations.
- Conducting agency-specific supplemental testing: when to commission additional testing before reuse authorization.

Module 3: POA&M Health Assessment and CSP Accountability

- POA&M quality indicators: milestone specificity, aging item patterns, deviation request volume, and false-positive rates.
- Analyzing POA&M velocity: remediation rate trends and what slow-moving POA&Ms signal about CSP program maturity.
- Deviation requests: understanding false positive, operational requirement, and risk adjustment requests, and when to reject them.
- Agency POA&M oversight rights: what agencies can contractually demand in terms of POA&M access and updates.
- Escalation pathways: when to escalate POA&M concerns to FedRAMP PMO and what remedies are available.

Module 4: Customer Responsibility Matrix Engineering – Closing Inherited Control Gaps

- CRM deep structure: responsibility categories (CSP, Agency, Shared), implementation parameter constraints, and evidence requirements.
- Identifying CRM gaps: controls where CSP implementation doesn't fully satisfy agency requirements.
- Developing agency supplemental control implementations: documenting what the agency must add beyond the CRM.
- Parameter constraints in inherited controls: where CSP ODPs limit agency flexibility and what to do about it.
- CRM negotiation: requesting CSP documentation updates, supplemental implementation guidance, and contractual commitments.

Module 5: Agency ATO Documentation for FedRAMP-Leveraged Systems

- Agency ATO package structure for FedRAMP reuse: leveraged ATO memo, supplemental SSP sections, and agency-specific control documentation.
- System boundary for leveraged services: what enters the agency's authorization boundary when using a FedRAMP CSP.
- Agency-specific risk assessment: identifying residual risks beyond what the FedRAMP package covers.
- Interconnection documentation for FedRAMP services: ISA development and agency-to-CSP data flows.
- ISSO responsibilities post-authorization: continuous monitoring obligations, CSP deliverable tracking, and change management.

Module 6: FedRAMP Continuous Monitoring – Agency Obligations and CSP Oversight

- Monthly ConMon deliverables: vulnerability scans, POA&M updates, and inventory reports, including agency review obligations.
- Annual assessment cycle: what the 3PAO assesses annually, agency participation rights, and how to use results.
- Significant change notification: what triggers SCN, review timeline, and agency authorization impact assessment.
- CSP ConMon performance metrics: what constitutes adequate ConMon performance and when to escalate.
- ConMon automation: API access to FedRAMP Package Access Request System (PARS) and automated deliverable tracking.

Module 7: Cloud Incident Response – Agency-CSP Coordination Framework

- FedRAMP incident notification requirements: breach notification timelines, severity classification, and US-CERT coordination.
- Agency IR responsibilities in CSP environments: evidence collection limitations, investigation coordination, and communication obligations.
- CSP IR capabilities assessment: what to evaluate in CSP IR documentation before authorization.
- Multi-tenant incident scenarios: isolation guarantees, cross-tenant impact assessment, and agency notification rights.
- Contractual IR obligations: SLA provisions, forensic evidence access rights, and post-incident reporting requirements.

Module 8: FedRAMP High Baseline and DoD IL4/IL5 – Sensitive Workload Requirements

- FedRAMP High baseline: additional controls, stricter parameters, and enhanced CSP obligations vs. Moderate.
- DoD IL4 and IL5 data impact levels: covered defense information (CDI), CUI categories, and authorization requirements.
- FedRAMP High authorized service marketplace: current availability, capability gaps, and procurement considerations.
- DISA PA (Provisional Authorization) process: DoD-specific authorization pathway and relationship to FedRAMP.
- On-premises and government community cloud options: when FedRAMP High doesn't meet mission requirements.

Module 9: Enterprise Cloud Security Governance – Portfolio Management

- Enterprise cloud portfolio inventory: tracking FedRAMP authorizations, expiration dates, SCN impact, and agency ISSOs.
- Risk aggregation across CSPs: identifying enterprise-level risks from common vulnerabilities across multiple cloud services.
- Cloud vendor management: security performance metrics, contractual enforcement, and vendor relationship governance.
- Cloud security investment planning: connecting FedRAMP oversight costs to IT budget planning and exhibit 53 reporting.
- Board-level cloud risk reporting: communicating cloud security posture in business terms to agency executives.

Module 10: Emerging FedRAMP Developments – Rev 5, Automation, and OSCAL

- FedRAMP Rev 5 transition: updated baselines, new CSP requirements, and agency impact of the 800-53 Rev 5 baseline migration.
- OSCAL (Open Security Controls Assessment Language): machine-readable package format, agency tooling, and automation

opportunities.

- FedRAMP automation pilot: continuous authorization objectives and what automated CSP monitoring means for agency oversight.
- AI/ML services and FedRAMP: current authorization gaps for AI services and OMB M-24-10 overlay development status.
- Sovereign cloud and international data residency: emerging agency requirements for cloud services handling sensitive data abroad.

Module 11: Procurement Strategy and Contractual Cloud Security Protections

- FedRAMP-specific contract provisions beyond standard FAR, including security incident response SLAs, data portability, and forensic evidence access.
- Cloud security in BPA, IDIQ, and task order vehicles: how to embed security requirements in multi-year contract vehicles.
- Exit and migration planning: contractual data return requirements, format standards, and timeline obligations for cloud exits.
- Evaluating CSP financial stability and continuity risk: what happens when a FedRAMP-authorized CSP is acquired or discontinued.
- Cybersecurity supply chain risk in cloud contracts: software provenance requirements, subprocessor disclosure, and foreign ownership flags.

Module 12: Capstone – Enterprise Cloud Security Program Leadership Simulation

- Capstone scenario overview: agency CISO managing an 8-CSP cloud portfolio with a recent incident, a pending FedRAMP Rev 5 transition, a new FedRAMP High acquisition, and an upcoming IG evaluation.
- Integration challenge: balancing ongoing ConMon oversight, incident response coordination, Rev 5 transition management, and new authorization due diligence simultaneously.
- Program leadership decision-making: prioritization under resource constraints, vendor accountability, and executive communication.
- After-action and improvement planning: translating simulation outcomes into enterprise program improvements.