COURSE SYLLABUS

Federal RMF Practitioner Certificate Program (Self-Paced)

Everything you need to take a federal system through the full Risk Management Framework, from categorization to an authorization to operate.

> 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-rmf-practitioner-certificate-program-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)
- Contingency Planning and Cyber Resilience Course (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

Contingency Planning and Cyber Resilience Course (Self-Paced)

Build a contingency plan that works when systems go down, from business impact analysis through recovery and testing.

- Explain the seven-step NIST contingency planning process and what each step produces.
- Distinguish business continuity, disaster recovery, and incident response plans and identify when each applies.
- Conduct a business impact analysis to identify critical systems and set recovery objectives.
- Set a recovery time objective and a recovery point objective for a given system.
- Select preventive controls that reduce the likelihood or impact of a disruption.
- Compare backup and alternate site strategies and choose one that fits a stated budget and risk tolerance.
- Apply recovery strategy considerations specific to cyber incidents, including ransomware.
- Draft the core sections of a contingency plan document, including activation and recovery procedures.
- Write a recovery procedure clear enough for someone unfamiliar with the system to follow.
- Distinguish tabletop, walkthrough, and functional exercises and select the right one for a given organization.
- Identify events that should trigger a contingency plan update.
- Explain how an individual contingency plan supports a broader organizational cyber resilience program.
- Evaluate a contingency plan document for missing or vague sections.