

Federal RMF Practitioner Certificate Program

All of what it takes to carry a federal system through the Risk Management Framework, from categorization to an authorization to operate.

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-rmf-practitioner-certificate-program>



support@graduateschool.edu •
[\(888\) 744-4723](tel:(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)

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