COURSE SYLLABUS

Federal Cybersecurity Authorization Professional: Security Control Assessor Certificate Program (Self-Paced)

Master the RMF core, then specialize as the independent assessor an authorizing official relies on.

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-security-control-assessor-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)
- NIST 800-53: Advanced Assessment, Tailoring, and Enterprise Program Management Course (Self-Paced) (18 Hours)
- Security Control Assessor (SCA) Practitioner: The Assessment Lifecycle (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

NIST 800-53: Advanced Assessment, Tailoring, and Enterprise Program Management Course (Self-Paced)

This advanced course builds the practitioner mastery required to lead a federal NIST 800-53 control program from deep-dive assessment through enterprise governance. Participants develop skills in 800-53A assessment methodology, advanced ODP tailoring, control overlays for specialized environments, and cross-framework integration, preparing them to manage complex federal security programs with confidence.

- Advanced 800-53A assessment methodology, including evidence sufficiency standards, determination statements, and assessment case mapping.
- Organization-Defined Parameter (ODP) tailoring with risk-based rationale and Authorizing Official documentation requirements.
- Control overlays for specialized environments, including cloud, OT/ICS, AI/ML, and privacy-intensive systems.
- Automated assessment integration using SCAP, DISA STIGs, and vulnerability scanners alongside manual 800-53A evidence.
- Enterprise control inheritance architecture with Common Control Providers and cross-framework mapping to CSF, FedRAMP, and CMMC.
- Control program governance, including ownership models, evidence management, metrics, and continuous improvement processes.

Security Control Assessor (SCA) Practitioner: The Assessment Lifecycle (Self-Paced)

The security control assessor makes the independent judgment an authorizing official relies on. This advanced course develops that craft end-to-end—establishing independence, scoping the assessment, tailoring NIST SP 800-53A procedures, and executing examination, interview, and test methods—so you can evaluate evidence, validate technical results, and write

findings that withstand scrutiny, culminating in a complete Security Assessment Report.

- Explain SCA authority, independence, and professional judgment
- Scope an assessment and trace controls to requirements
- Develop a Security Assessment Plan and tailor SP 800-53A procedures
- Apply examine, interview, and test methods effectively
- Evaluate evidence sufficiency across control families and types
- Assess common, inherited, and hybrid controls
- Document findings, determine control effectiveness, and produce a Security Assessment Report