COURSE SYLLABUS

Security Control Assessor Certificate Program

Grow into the independent assessor an authorizing official can lean on — from assessment plan through to a Security Assessment Report that holds up.

> 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/security-control-assessor-certificate-program

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

Course Outline

This package includes these courses

- RMF Foundations: From Risk to Authorization (8 Hours)
- NIST 800-53: Advanced Assessment, Tailoring, and Enterprise Program Management Course (18 Hours)
- Security Control Assessor (SCA) Practitioner: The Assessment Lifecycle (14 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: Advanced Assessment, Tailoring, and Enterprise Program Management Course

This advanced course builds the practitioner command needed to lead a federal NIST 800-53 control program, from deep-dive assessment through to enterprise governance. Participants develop 800-53A assessment methodology, advanced ODP tailoring, control overlays for specialized environments, and cross-framework integration, leaving ready to run complex federal security programs.

- Advanced 800-53A assessment methodology, covering evidence sufficiency standards, determination statements, and assessment case mapping.
- Organization-Defined Parameter (ODP) tailoring with risk-based rationale and the documentation an Authorizing Official requires.
- Control overlays for specialized environments, including cloud, OT/ICS, AI/ML, and privacy-intensive systems.
- Automated assessment integration through 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, covering ownership models, evidence management, metrics, and continuous improvement processes.

Security Control Assessor (SCA) Practitioner: The Assessment Lifecycle

An authorizing official's decision rests on the independent judgment of the security control assessor. This advanced course develops that craft end to end — establishing independence, setting scope, tailoring NIST SP 800-53A procedures, and carrying out examination, interview, and test methods — so findings survive scrutiny, culminating in a complete Security Assessment Report.

- Explain an SCA's authority, independence, and exercise of professional judgment
- Set assessment scope and trace controls back to requirements
- Build a Security Assessment Plan and tailor SP 800-53A procedures to it
- Put examine, interview, and test methods to work effectively
- Weigh whether evidence is sufficient across control families and types
- Assess common, inherited, and hybrid controls
- Write up findings, determine control effectiveness, and produce a Security Assessment Report