COURSE SYLLABUS

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 examine, interview, and test methods — so findings survive scrutiny, culminating in a complete Security Assessment Report.

> 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/courses/security-control-assessor-sca-practitioner



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

Course Outline

Module 1: SCA Authority, Independence, and Professional Judgment

Examine the security control assessor's mandate, required independence, and responsibility to apply sound professional judgment.

Module 2: Assessment Scope, System Context, and Control Traceability

Define the assessment scope, establish system context, and trace security controls to applicable requirements.

Module 3: Developing the Security Assessment Plan

Build a Security Assessment Plan that documents the assessment approach, objectives, procedures, resources, and schedule.

Module 4: Tailoring Assessment Procedures, Depth, and Coverage

Adapt NIST SP 800-53A assessment procedures, depth, and coverage to the system's characteristics and risk profile.

Module 5: Executing Examine, Interview, and Test Procedures

Apply examine, interview, and test methods to collect and validate assessment evidence.

Module 6: Evaluating Technical, Administrative, and Physical Evidence

Evaluate the relevance, reliability, and sufficiency of technical, administrative, and physical evidence.

Module 7: Assessing Common, Inherited, and Hybrid Controls

Assess shared control responsibilities across common, inherited, and hybrid control implementations.

Module 8: Validating Vulnerability and Technical-Test Results

Confirm the accuracy, relevance, and potential impact of vulnerability scan results and other technical findings.

Module 9: Documenting Findings and Determining Control Effectiveness

Write clear, evidence-based findings and determine whether controls are implemented correctly and operating effectively.

Module 10: Risk Analysis, Deficiency Prioritization, and POA&M Review

Analyze risk, prioritize identified deficiencies, and review Plans of Action and Milestones for completeness and appropriateness.

Module 11: Developing the Security Assessment Report Capstone

Produce a complete Security Assessment Report that documents assessment results, findings, risk implications, and supporting evidence.