COURSE SYLLABUS

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

Apply advanced 800-53A assessment techniques, build control overlays for cloud, OT, and AI/ML systems, and develop the enterprise governance skills to manage a federal security controls program.

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/courses/nist-800-53-advanced-assessment-tailoring-and-enterprise-program-management-course-self-paced

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

Course Outline

Module 1: Advanced Control Assessment Methodology – 800-53A Deep Dive

- 800-53A assessment procedure structure: assessment objectives, determination statements, and potential assessment methods.
- Examine, interview, and test: evidence sufficiency standards and documentation requirements for each method.
- Assessment case mapping: linking determination statements to control implementations and evidence artifacts.
- Depth and coverage parameters: what ‘basic,’ ‘focused,’ and ‘comprehensive’ assessment mean in practice.
- Common assessment failures: scope gaps, evidence insufficiency, and other-than-satisfied determination errors.

Module 2: Organization-Defined Parameters – Advanced Tailoring Decisions

- ODP taxonomy: selection ODPs, assignment ODPs, and their impact on control meaning and assessment.
- Risk-based ODP rationale: what makes an ODP defensible vs. arbitrary, and documentation standards.
- High-risk ODPs: AC-2(j) account review frequency, AU-11 audit log retention, CA-7 monitoring frequency, SI-3 malicious code scanning.
- ODP consistency across the SSP: ensuring related controls use compatible parameters and document dependencies.
- AO-level ODP decisions: which ODPs require Authorizing Official approval vs. ISSO-level determination.

Module 3: Control Tailoring, Scoping Guidance, and Compensating Controls

- Scoping considerations: technology-related, physical infrastructure, public access, scalable, and common control scoping.
- Compensating controls: when they’re allowed, documentation requirements, and assessment of compensating control effectiveness.
- Control not applicable (NA) determinations: criteria, documentation, and AO approval requirements.
- Parameter-based tailoring vs. control removal: the difference in risk exposure and documentation burden.
- Overlay interaction with tailoring: how overlays override baseline tailoring and the precedence hierarchy.

Module 4: Cross-Family Control Integration and Dependency Analysis

- Control dependencies: how failures in foundational controls (AC-2, IA-5, AU-2) cascade to dependent controls.
- Defense-in-depth architecture through 800-53: mapping layered controls across access, boundary, and audit families.
- Control synergies: how complementary controls create compounding protection when implemented together.
- Inherited control gaps: identifying where inheritance assumptions break and system-specific controls must compensate.
- Control interaction with architecture: how architectural decisions (cloud, zero trust, microservices) change control applicability.

Module 5: Control Overlays – Building and Applying Specialized Control Sets

- NIST overlay concept: what overlays are, who creates them, and how they interact with Low/Moderate/High baselines.
- Published federal overlays: Intelligence Community, DoD, privacy, cloud, ICS/OT, and AI/ML overlays.
- Building a custom overlay: scope definition, control additions, parameter constraints, and implementation guidance format.
- Overlay documentation requirements: purpose, applicability, tailoring rationale, and AO approval process.
- Overlay application in assessment: how assessors treat overlay-added controls vs. baseline controls.

Module 6: Automated Control Assessment – SCAP, STIGs, and Vulnerability Integration

- SCAP content: XCCDF checklists, OVAL definitions, and CPE dictionaries, including structure and federal use.
- DISA STIGs and SRGs: scope, applicability, and how STIG findings map to 800-53 control deficiencies.
- Nessus/ACAS automated scanning: scan configuration, authenticated vs. unauthenticated scans, and result interpretation.
- Integrating automated findings with 800-53A evidence: correlation, deduplication, and manual validation requirements.
- Automation limitations: what scanners miss and why manual assessment remains essential for high-impact controls.

Module 7: Privacy Controls – PT and IP Family Deep Dive

- PT (Processing and Transparency) family: PT-1 through PT-8, including purpose, implementation, and assessment approaches.
- IP (Individual Participation) family: IP-1 through IP-6, including FOIA/Privacy Act alignment and practical implementation.
- Privacy risk assessment integration with security assessment: joint assessment planning and finding coordination.
- System of Records Notice (SORN) and Privacy Impact Assessment (PIA) as control evidence: what ISSOs must verify.
- Coordinating with agency Privacy Officers: roles, evidence handoffs, and joint finding resolution.

Module 8: Specialized Environment Application – Cloud, OT, and AI/ML Control Sets

- Cloud control application: FedRAMP-specific control enhancements, inherited control documentation, and CSP assessment evidence.
- OT/ICS control tailoring: 800-82 overlay application, availability-first parameter adjustments, and compensating controls for legacy PLCs.
- AI/ML control application: SA-8 AI engineering principles, SR family supply chain controls for models, and AT-2(5) AI awareness.
- Mobile and remote work control application: AC-20, IA-3, and SC-8 enhanced parameters for dispersed workforce environments.
- Multi-environment system challenges: when a single system spans cloud, on-prem, and OT, including boundary and inheritance documentation.

Module 9: Enterprise Control Inheritance Architecture and Common Control Providers

- Common Control Provider (CCP) roles: agency-level, program-level, and site-level CCPs and their authorization relationships.
- Inheritable control catalog: developing and maintaining an agency's catalog of available inherited controls.
- Inheritance documentation: how SSPs reference inherited controls, what evidence is required, and when inheritance breaks down.
- Control inheritance gaps: identifying when an inherited control doesn't fully satisfy a system's implementation requirements.
- CCP authorization: how CCPs maintain their own authorization and what triggers a CCP reauthorization that cascades to inheriting systems.

Module 10: Cross-Framework Control Mapping – CSF, FedRAMP, CMMC, and Sector Requirements

- NIST CSF to 800-53 mapping: using NIST's published crosswalk to satisfy CSF outcomes through control implementation.
- FedRAMP control baseline differences: FedRAMP-specific parameter requirements and how they interact with agency tailoring.
- CMMC Level 2 to 800-53 mapping: satisfying CMMC practices through existing 800-53 control implementations.
- HIPAA, PCI DSS, and sector-specific requirements: using 800-53 as a common framework to satisfy multiple compliance obligations.

- Cross-framework efficiency: designing a single control implementation that satisfies multiple framework requirements simultaneously.

Module 11: Control Program Governance, Ownership, and Continuous Improvement

- Control ownership model: assigning system owner, ISSO, and operational owner responsibilities for each control family.
- Control evidence management: documentation standards, evidence retention policies, and audit-ready file organization.
- Control program metrics: measuring implementation completeness, assessment coverage, and finding remediation velocity.
- Continuous control improvement: feeding assessment findings, incident data, and threat intelligence into control enhancement cycles.
- CISO-level program governance: control steering committee, ODP standardization decisions, and enterprise policy management.

Module 12: Capstone – Full Control Program Simulation

- Capstone scenario overview: agency undergoing major system deployment, FedRAMP transition, OT component addition, and upcoming assessment.
- Integration challenge: applying advanced tailoring, overlays, inheritance architecture, and cross-framework mapping to a single complex program.
- Program leadership decision-making: assessment prioritization, resource allocation, and risk acceptance sequencing.
- After-action and improvement planning: translating simulation outcomes into real-world program improvements.