COURSE SYLLABUS

NIST 800-53: Control Selection, Implementation, and Security Planning Course (Self-Paced)

Implement and assess security and privacy controls for federal information systems.

> 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/nist-800-53-control-selection-implementation-and-security-planning-course-self-paced



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

Course Outline

Module 1: 800-53 Rev 5 Structure, Baselines, and Tailoring

- Control anatomy: ID, title, control text, discussion, enhancements, references, and related controls.
- Rev 5 key changes: outcome-based language, new SR family, privacy integration, and technology-neutral scope.
- Baseline selection from NIST SP 800-53B: Low, Moderate, High, and Privacy Baseline.
- Tailoring: scoping guidance, compensating controls, organization-defined parameter assignments, and overlay application.
- Documenting tailoring decisions in the SSP with rationale, including what auditors require.

Module 2: Access Control (AC) and Identification & Authentication (IA)

- AC-2 Account Management: provisioning, periodic review, and automated notification requirements.
- AC-3 Access Enforcement and AC-17 Remote Access: RBAC, ABAC, and VPN/ZTNA controls.
- IA-2 MFA requirements: phishing-resistant methods under OMB M-22-09 and PIV/CAC compliance.
- IA-5 Authenticator Management: password policies, certificate lifecycle, and credential rotation.
- Common AC/IA SSP deficiencies: generic statements, missing enforcement mechanisms, and undocumented exceptions.

Module 3: Audit & Accountability (AU) and System & Communications Protection (SC)

- AU-2 Event Logging: selecting auditable events for common federal system types, including web, database, and VPN.
- AU-3 Audit Record Content: required fields and correlation identifiers for SIEM integration.
- AU-6 Audit Review: automated alerting thresholds and review frequency requirements.
- SC-7 Boundary Protection: firewall policy documentation and DMZ architecture controls.
- SC-8 and SC-28: transmission and data-at-rest encryption standards, including TLS 1.2/1.3 and AES-256 requirements.

Module 4: Configuration Management (CM), Contingency Planning (CP), and Incident Response (IR)

- CM-2 Baseline Configuration and CM-6 Configuration Settings: DISA STIG and CIS Benchmark integration.
- CM-7 Least Functionality: disabling unnecessary ports, protocols, and services.
- CP-2 Contingency Plan: RTO/RPO requirements, test frequency, and plan update triggers.

- IR-4 Incident Handling: detection, analysis, containment, eradication, and recovery procedures.
- IR-6 Incident Reporting: US-CERT timelines and FISMA reporting obligations under OMB M-17-25.

Module 5: Privacy Controls and the Supply Chain Risk Management (SR) Family

- Privacy control families: PT, SE, IP, and UL, including applicability criteria for PII-processing systems.
- Privacy Overlay: when it applies and how it changes the control baseline.
- Senior Agency Official for Privacy (SAOP): coordination obligations and PT-1 policy requirements.
- SR family overview: SR-1 through SR-11, including SCRM policy, supplier controls, and provenance requirements.
- SBOM (Software Bill of Materials) requirements under EO 14028 and SR-4 Provenance control.

Module 6: SSP Quality, Evidence Collection, and Assessment Readiness

- SSP quality standards: the 'how, where, who, when' test for every implementation statement.
- Evidence types by 800-53A assessment method: examine, interview, and test, and what counts as sufficient.
- Screenshot and configuration evidence standards: date stamps, system identifiers, and annotated callouts.
- Common SSP errors that cause assessment failures: generic language, missing inheritance, and stale documentation.
- Using GRC tools (eMASS, Xacta, Archer) to maintain SSP currency and evidence version control.

Module 7: NIST SP 800-53A – Assessment Procedures and SAR Development

- 800-53A assessment objectives, methods, and objects: how to read and apply assessment procedures.
- Assessment planning: sample size selection, coverage rationale, and interview protocol design.
- Finding severity classification: high, moderate, and low, including criteria, examples, and borderline cases.
- SAR structure: executive summary, methodology section, findings table, and risk rating.
- SAR-to-POA&M traceability: linking each finding to a remediation action with closure criteria.

Module 8: POA&M Management, Continuous Monitoring, and Capstone

- POA&M required fields under OMB M-04-25: weakness, source, responsible office, scheduled completion, milestones, and resources.
- POA&M aging management: false positive handling, milestone extensions, and escalation procedures.
- FISMA reporting linkage: connecting POA&M data to CyberScope metrics and IG compliance assessments.
- Continuous monitoring schedule design: frequency selection, automated data source integration, and CDM dashboard alignment.