Security Control Assessment and Assurance

GRC301

Assess whether security controls work, from the evidence an organization supplies: criteria, determination statements, evidence quality, sampling, findings and assurance reports another assessor can reproduce.

Modules	20
Lessons	125
Phases	4
Free preview	Course Orientation (5 lessons)

The method

One organization, one quarter. Every lesson reads the same evidence pack: standards, exports, tickets, logs, interview notes and a supplier report from one fictional company, with the gaps, contradictions and weak items a real submission has. The figures on every page agree because they come from the same files.

Method first, frameworks as criteria. The assessment method is NIST SP 800-53A Rev. 5: examine, interview and test, with depth, coverage and determination statements. The criteria come from whichever standard an exercise names: the organization's own, or ISO/IEC 27001, SOC 2, NIST CSF 2.0, NIST SP 800-53 or the CIS Controls.

Practiced in templates you keep. Each lesson ends on assessment work on the evidence pack, and each module on an exercise with a worked debrief, 11 in all. Seven templates, from the assessment plan to the retest record, are free downloads with a completed example each. The course ends on a 40-question exam.

Full syllabus

Phase 1: Foundations

Course Orientation FREE PREVIEW

What a security control assessment decides and how this course teaches it: determinations and their reasons, the evidence pack, the seven assessment templates, and one control taken from its clause to a draft finding.

1. 0.1 The Purpose of a Control Assessment
2. 0.2 Determinations and Their Reasons
3. 0.3 The Evidence Pack
4. 0.4 The Assessor's Templates
5. 0.5 A First Determination

Assessment and Assurance

What an assessment can conclude, settled before the evidence is read: criteria, design and operating effectiveness, assessment against audit, the limits of assurance, objectivity, the SP 800-53A procedure, and the assessment brief.

1. 1.1 Control Objectives and Criteria
2. 1.2 Design, Implementation and Operating Effectiveness
3. 1.3 Assessment, Audit and Review
4. 1.4 Assurance and Its Limits
5. 1.5 Objectivity and the Assessor
6. 1.6 Assessment Procedures in NIST SP 800-53A
7. 1.7 The Assessment Brief
8. 1.8 Exercise: The MFA Coverage Figure

Scope and Assessment Planning

Turning a brief into a scoped plan: business services and their systems, boundaries, the assessment period, dependencies and inherited controls, criteria, stakeholders, and assembling the plan.

1. 2.1 From Business Service to Systems
2. 2.2 Boundaries
3. 2.3 Choosing the Assessment Period
4. 2.4 Dependencies and Inherited Controls
5. 2.5 Selecting and Mapping Criteria
6. 2.6 Stakeholders and Responsibilities
7. 2.7 Assembling the Plan
8. 2.8 Exercise: Scope the Finance Access Assessment

Phase 2: Tests and Evidence

Turning Requirements into Tests

Turning criteria into a control test matrix: determination statements, observable conditions, test procedures, acceptance criteria, vague tests, tests for different kinds of control, and the matrix.

1. 3.1 From the Criteria Map to Statements
2. 3.2 Observable Conditions
3. 3.3 Test Procedures
4. 3.4 Acceptance Criteria
5. 3.5 Vague Tests, and Fixing Them
6. 3.6 Tests for Different Kinds of Control
7. 3.7 Building the Control Test Matrix
8. 3.8 Exercise: The Vulnerability Management Test Matrix

Evidence Quality and Traceability

Judging the evidence that arrives: sufficiency and appropriateness, relevance, reliability and provenance, completeness, timestamps, the weaker forms, and contradictions, assembled in an evidence register.

1. 4.1 Sufficient and Appropriate Evidence
2. 4.2 Relevance
3. 4.3 Reliability and Provenance
4. 4.4 Completeness and Population
5. 4.5 Timestamps and Periods
6. 4.6 Screenshots, Documents and Statements
7. 4.7 Contradictions and the Register
8. 4.8 Exercise: Register the Vulnerability Management Submission

Assessment Methods and Sampling

Choosing a method, interviews and walkthroughs, then populations, selection, sample size and failures, after PCAOB AS 2201 and AS 2315.

1. 5.1 Choosing a Method
2. 5.2 Interviews
3. 5.3 Walkthroughs
4. 5.4 Populations
5. 5.5 Selecting the Sample
6. 5.6 Sample Size
7. 5.7 Failures, and What a Sample Cannot Support
8. 5.8 Exercise: The Operational Sampling Plan

Phase 3: Assessing Controls

Assessing Identity and Access Controls

Testing the six clauses of an access standard on their whole populations: leavers, privileged and emergency access, service accounts, an access review, exceptions and compensating controls, and the identity ledger.

1. 6.1 The Identity Workpapers
2. 6.2 Leavers, Movers and Joiners
3. 6.3 Privileged and Emergency Access
4. 6.4 Service Accounts
5. 6.5 Access Reviews
6. 6.6 Exceptions and Compensating Controls
7. 6.7 Writing the Identity Determinations
8. 6.8 Exercise: MFA Coverage and Enforcement

Assessing Operational Controls

Testing operational controls on their whole populations: scanning coverage, logging, endpoint protection, change, backup and recovery, and incident response exercises.

1. 7.1 Vulnerability Scanning Coverage
2. 7.2 Logging and Monitoring
3. 7.3 Endpoint Coverage
4. 7.4 Change Control
5. 7.5 Backup and Restore
6. 7.6 Incident Response Exercises
7. 7.7 Writing the Operational Determinations
8. 7.8 Exercise: Vulnerability Remediation and Severity

Cloud and Supplier Evidence

Assessing the evidence for outside dependencies: SOC 2 reports, their periods and carve-outs, complementary user entity controls, cloud tenant configuration and the evidence-gap analysis.

1. 8.1 Who Operates What
2. 8.2 Reading a SOC 2 Report
3. 8.3 Period, Carve-Outs and Bridge Letters
4. 8.4 Complementary User Entity Controls
5. 8.5 The Customer's Configuration in Cloud Services
6. 8.6 The Evidence-Gap Analysis
7. 8.7 Exercise: The Payroll Portal CUECs

Phase 4: Conclusions

Findings and Significance

Turning determinations into findings another assessor can reproduce: condition, criteria and scope, consequence and compensating controls, cause where supported, severity with its rationale, and validation with owners.

1. 9.1 From Determinations to Findings
2. 9.2 Condition, Criteria and Scope
3. 9.3 Consequence and Compensating Controls
4. 9.4 Cause, Where the Evidence Supports It
5. 9.5 Severity and Its Rationale
6. 9.6 Factual Validation with Owners
7. 9.7 Exercise: Review the Draft Findings

Remediation and Retesting

Following findings to their close: corrective actions, interim measures and compensating controls, risk acceptance, closure evidence, and retesting on a later period.

1. 10.1 From Finding to Corrective Action
2. 10.2 Interim Measures and Compensating Controls
3. 10.3 Risk Acceptance
4. 10.4 Closure Evidence
5. 10.5 Retesting and Recurrence
6. 10.6 Exercise: Retest the Leaver Control

Assurance Reporting

Turning findings into the assurance report: conclusions the evidence supports, limitations, management disagreement and escalation, reports for different readers, and assembling the report.

1. 11.1 Conclusions the Evidence Supports
2. 11.2 Limitations and What Was Not Tested
3. 11.3 Management Disagreement and Escalation
4. 11.4 Reports for Different Readers
5. 11.5 Assembling the Report
6. 11.6 Exercise: Review the Draft Board Summary

Phase 0: Course Resources

Assessment Cheatsheets

One sheet per area of assessment work: the question, the record to request, the test, what to read in the result and what it does not prove.

1. Criteria, Statements and Procedures
2. Evidence Quality
3. Populations and Sampling
4. Identity and Access Tests
5. Operational Control Tests
6. Cloud and Supplier Evidence
7. Findings, Remediation and Reporting
8. Lookup Values

Cookbooks

Nine runbooks, one per stage of an assessment, each with the template it fills, what every column takes, and a completed example.

1. Planning the Assessment
2. Building the Test Matrix
3. Requesting and Registering Evidence
4. Planning and Running a Sample
5. Testing a Control Area to Its Determinations
6. Assessing a Supplier Through Its Report
7. Writing and Validating Findings
8. Tracking Remediation and Retesting
9. Writing the Assurance Report

Lab Setup

The workspace for the course: the evidence packs and their index, a spreadsheet set up for dates and business days, checking what each file covers, and a verification that fails loudly.

1. The Evidence Packs
2. The Spreadsheet Workspace
3. What a File Covers
4. Verify the Workspace

Walkthroughs

Four assessment cases worked end to end on the evidence pack, including the wrong turns, each ending in a determination, a finding and the point that transfers.

1. The Leaver Control, From Clause to Retest
2. The Restore Test That Said Pass
3. The Review That Was Complete
4. The Figure on the Dashboard

Playbooks

Eight situations that arise during fieldwork and need handling the same day, each with prerequisites, a pre-flight, a time budget, the sequence and three outcomes.

1. Evidence Arrives Late, Partial or as a Screenshot
2. An Exception Turns Up in a Sample
3. An Owner Offers a Compensating Control
4. Scope Changes During Fieldwork
5. A Supplier Report Is Out of Period or Qualified
6. Management Disputes a Finding
7. Someone Asks You to Soften a Finding
8. You Find What Looks Like an Incident

Practice Playground

Every exercise and practice-tool scenario in the course, by module, with the lesson each one sits in, and the course exam.

1. Exercises, Tools and the Exam

References

The sources the course cites, grouped by part of the course, each with the lessons that cite it.

1. Assessment method, evidence and sampling
2. Identity, operational and supplier controls
3. Findings, remediation and reporting

Course Completion

Course Exam

Security Control Assessment and Assurance end-of-course exam: 40 questions in four parts, from planning an assessment to reporting it, checked on the server.

1. Course Completion. Security Control Assessment and Assurance

Generated 2026-11-04 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/security-control-assessment/