

GRC for Security Professionals

GRC201

Turn security from a cost center into a strategic business enabler. Build effective Governance, Risk, and Compliance programs that align security with business objectives, manage real risk, and demonstrate clear value to executives and auditors.

Modules	25
Lessons	157
Phases	4
Free preview	Course Orientation (6 lessons)

The method

Most GRC fails by producing documents rather than changing anything. This course is built around the opposite loop, and runs it through every framework it implements.

1. Write the policy somebody can comply with. A policy nobody can follow is a finding waiting to be written against you. The test is whether an ordinary employee could act on it.
2. Assess risk against something real. A register scored from opinion produces an order nobody defends. Method first, then the scoring, then the register.
3. Treat the risk with a control that exists. A treatment decision with no owner, no date and no evidence is a treatment decision that has not been made.
4. Monitor the control, not the document. Controls decay silently. What proves a control still works, and who checks, is the difference between a program and a binder.
5. Report so somebody decides. A board paper that produces no decision is a status update. The reporting module is about the decision it is meant to cause.

The frameworks, ISO 27001, NIST CSF 2.0, SOC 2 and CMMC, are then implemented through that same loop rather than as separate checklists.

What this course assumes

No minimum experience and no prerequisite course. Every framework is introduced from what it asks for and why, and the course assumes you are a practitioner rather than an auditor.

What makes it go faster: an organization you are actually responsible for, because every exercise produces an artifact you can use. Not required.

What this course does not cover: legal advice, audit as a profession, and technical security controls in depth. This is building and running the governance function.

Full syllabus

Phase 1: Foundations

Course Orientation FREE PREVIEW

What GRC for Security Professionals teaches: build a working governance, risk, and compliance program, a risk register you actually work, policies people follow, controls mapped to ISO 27001, NIST CSF, SOC 2, GDPR, and CMMC, and audit evidence produced as a byproduct.

1. 0.1 The Problem with GRC Training
2. 0.2 Who This Course Is For
3. 0.3 Course Structure and Module Map
4. 0.4 Prerequisites and What You Need
5. 0.5 How to Learn from This Course
6. Module Summary

What GRC Actually Is, and Why It Fails

The governance-risk-compliance triad as an operating system.

1. 1.1 The GRC Triad as an Operating System
2. 1.2 Why GRC Programs Fail: Case Studies
3. 1.3 Organizational Positioning of GRC
4. 1.4 Regulatory Drivers: Why Organizations Do GRC
5. Module Summary
6. Check My Knowledge

Building the Policy Framework

Policy as executable governance. The policy hierarchy and the enforcement test that separates its levels. Why policies become shelf-ware and how to write ones that hold. The minimum viable policy set. The policy lifecycle. Mapping policies to the controls that enforce them and the requirements...

1. 2.1 The Policy Hierarchy
2. 2.2 Why Policies Fail, and How to Write Ones That Work
3. 2.3 The Minimum Viable Policy Set
4. 2.4 The Policy Lifecycle
5. 2.5 Mapping Policies to Controls and Regulations
6. Module Summary
7. Check My Knowledge

Phase 2: Risk Management

Risk Assessment Methodology

The risk engine the policy framework has been referencing.

1. 3.1 Risk Assessment Fundamentals
2. 3.2 Risk Identification
3. 3.3 Risk Analysis: Scoring and Calibration
4. 3.4 Risk Appetite and Tolerance
5. 3.5 Building the Risk Register
6. 3.6 Evidence: Turning Telemetry into Register Entries
7. Module Summary
8. Check My Knowledge

Risk Treatment and Controls

Turning scored risks into decisions and controls.

1. 4.1 The Four Treatment Options
2. 4.2 Control Selection
3. 4.3 The Statement of Applicability
4. 4.4 Treatment Plans and Residual Risk
5. 4.5 Verifying That Controls Operate
6. Module Summary
7. Check My Knowledge

Risk Monitoring and Reporting

Keeping the register true between reviews.

1. 5.1 Risk Indicators and Control Metrics
2. 5.2 Dashboards for Two Audiences
3. 5.3 Board Reporting
4. 5.4 Escalation
5. 5.5 The Quarterly Review
6. 5.6 Queries That Produce Trends
7. Module Summary
8. Check My Knowledge

Phase 3: Framework Implementation

ISO 27001 Implementation

Mapping the risk programme onto ISO 27001.

1. 6.1 How the Standard Is Built
2. 6.2 Context, Scope, and Leadership
3. 6.3 Planning: Clause 6
4. 6.4 Support and Operation
5. 6.5 Performance and Improvement
6. 6.6 Annex A and the Full SoA
7. 6.7 Certification
8. Module Summary
9. Check My Knowledge

NIST CSF 2.0 Implementation

A framework you cannot be certified against, and why it earns its place next to one you can.

1. 7.1 What CSF Is For
2. 7.2 The Govern Function
3. 7.3 The Five Operational Functions
4. 7.4 Current and Target Profiles
5. 7.5 Implementation Tiers
6. 7.6 Running CSF Alongside ISO 27001
7. Module Summary
8. Check My Knowledge

SOC 2 Implementation

An attestation rather than a certification, tested against controls you write yourself.

1. 8.1 What a SOC 2 Report Is
2. 8.2 The System Description
3. 8.3 The Criteria and What They Test
4. 8.4 Evidence Across the Window
5. 8.5 Working with the Examining Firm
6. 8.6 Using the Report
7. Module Summary
8. Check My Knowledge

Data Protection and Privacy

UK GDPR, the DPA 2018 and the Data (Use and Access) Act 2025 read together.

1. 9.1 The UK Regime as It Stands
2. 9.2 Lawful Bases
3. 9.3 Records of Processing
4. 9.4 Impact Assessments
5. 9.5 Individual Rights and Complaints
6. 9.6 Breach Notification
7. 9.7 Transfers and Accountability Roles
8. Module Summary
9. Check My Knowledge

CMMC Implementation

A certification regime attached to one customer, currently mid-reform.

1. 10.1 The Programme and Where It Stands
2. 10.2 Identifying What You Hold
3. 10.3 The 110 Requirements
4. 10.4 The Plan, the Score, and What You Can Defer
5. 10.5 Assessment and Affirmation
6. 10.6 Scoping and the Enclave
7. Module Summary
8. Check My Knowledge

Phase 4: Governance Operations

Security Awareness

Every framework in this course requires awareness training and none tells you how to make it work.

1. 11.1 Why Awareness Programmes Fail
2. 11.2 Designing Interventions That Work
3. 11.3 Running Simulations
4. 11.4 Role-Specific Training
5. 11.5 The Champion Network
6. 11.6 Measuring the Programme
7. Module Summary
8. Check My Knowledge

Audit Management

Running audits as a programme rather than a series of events.

1. 12.1 The Audit Landscape
2. 12.2 Building the Internal Programme
3. 12.3 Conducting the Audit
4. 12.4 Managing the External Audit
5. 12.5 The Finding Lifecycle
6. 12.6 Running Several Audits at Once
7. Module Summary
8. Check My Knowledge

GRC Leadership

Running a function rather than a process.

1. 13.1 Translating Risk for the Board
2. 13.2 The Board Report
3. 13.3 Committees and Where Decisions Get Taken
4. 13.4 Budgeting and the Cost of Inaction
5. 13.5 Delivering Bad News
6. Module Summary
7. Check My Knowledge

Regulatory Change Management

The discipline that keeps everything else from going quietly out of date.

1. 14.1 Watching for Change
2. 14.2 Assessing What It Requires
3. 14.3 Turning It Into Work
4. 14.4 Keeping the Scan Working
5. Module Summary
6. Check My Knowledge

Building and Operating the GRC Function

Whether anybody actually has the capacity.

1. 15.1 Where the Function Sits
2. 15.2 Who Does the Work
3. 15.3 Tooling
4. 15.4 The Operating Model
5. 15.5 Assessing the Function
6. Module Summary
7. Check My Knowledge

Sector Governance and Emerging Requirements

What changes when obligations come from a sector regulator, company law, or an insurer rather than a general framework.

1. 16.1 When the Regulator Has a Sector View
2. 16.2 When a Regulator Stops Asking About Policies
3. 16.3 Obligations That Arrive Through Company Law
4. 16.4 Underwriters, Emerging Requirements, and What You Do Next
5. Module Summary
6. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

The scales, matrices, mappings and report skeletons, with what each instrument decides and where it misleads.

1. Scoring Risk Defensibly
2. Frameworks and Cross-Mapping
3. Privacy and Breach Notification
4. Policies, Audits and Findings
5. Metrics and the Board
6. Running the Function

Cookbooks

Ordered procedures for the work a GRC function actually does: assessments, certifications, audits, breaches and board cycles.

1. Running a Risk Assessment
2. Getting to a Certification
3. Handling a Notifiable Breach
4. Surviving an Audit
5. Building a Policy Set
6. Preparing the Board Report
7. Absorbing a New Regulation

Lab Setup

A working register, policy set, control map and evidence pack, built from nothing and then tested against the failures that make them useless.

1. Building the Register
2. Controls, Evidence and the Gaps
3. Verify, and What the Lab Cannot Teach

Walkthroughs

Six cases reasoned end to end, including the ones where every artifact was current and the function was achieving nothing.

1. The Dashboard That Was Ninety-Four Percent
2. The Date That Was Already Impossible
3. The Register Nobody Argued With
4. The Notification Nobody Wanted to Make
5. The Finding That Was Not One
6. The Risk With No Owner

Playbooks

What to do when a regulator writes, an auditor raises a finding, a customer sends a questionnaire, or somebody asks for an exception.

1. A Regulator Has Written
2. A Customer Questionnaire Arrives
3. An Auditor Raises a Finding
4. Somebody Wants an Exception
5. A Data Subject Request Arrives
6. A Supplier Has Been Breached
7. Somebody Asks If We Are Compliant

Playground

The exam, the lab pack, the artifacts you built, and the two products this course bridges into.

References & Further Reading

External sources this course draws on: frameworks, standards, regulator guidance and vendor documentation.

1. References & Further Reading

Course Completion

Course Exam

GRC for Security Professionals end-of-course exam: a simulation-based assessment testing whether you can establish what binds an organization, grade gaps against evidence that already exists, sequence work against a date you do not control, and take a board a decision it can act on.

1. Course Completion. GRC for Security Professionals

Generated 2026-09-01 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/practical-grc/