GRC TRAINING SYLLABUS

Governance, Risk & Compliance Complete Syllabus

Build practical knowledge of cybersecurity governance, risk management, regulatory compliance, security policies, audits, and control frameworks. This syllabus introduces the core concepts and workflows used by GRC teams to assess risk, maintain compliance, and improve an organisation's security posture.

10 Modules
Structured learning path

Practical
Case studies and exercises

GRC
Governance, risk and compliance

SYLLABUS OVERVIEW

01	GRC fundamentals	Core concepts
02	Governance and security policies	Governance
03	Risk management	Risk assessment
04	Compliance and regulations	Compliance
05	Security frameworks and controls	Frameworks
06	Audit and assessment	Audit
07	Third-party risk management	Vendors
08	Incident, privacy and continuity	Resilience
09	GRC tools and reporting	Operations
10	Capstone project	Applied learning

COURSE OVERVIEW

What is GRC?

Governance, Risk, and Compliance (GRC) brings together the policies, processes, and controls an organisation uses to meet business objectives, manage uncertainty, and fulfil legal or regulatory obligations. Cybersecurity GRC connects security practices with organisational risk and accountability.

- **Governance** establish accountability, policies, roles, and decision-making processes
- **Risk management** identify, analyse, prioritise, treat, and monitor information-security risks
- **Compliance** map applicable obligations to controls and maintain evidence that requirements are being met
- **Learning outcome** understand how GRC activities support a measurable and continually improving security programme

LEARNING APPROACH

The syllabus combines foundational concepts with practical examples, documentation exercises, risk registers, control mapping, and audit evidence. Specific legal obligations depend on the organisation, industry, and jurisdiction.

Module 01

FOUNDATIONS

GRC fundamentals

Understand the purpose of GRC and how security, business objectives, and accountability fit together.

- **Introduction to GRC** terminology, objectives, operating models, and common responsibilities
- **GRC roles** security leadership, risk owners, control owners, auditors, compliance teams, and business stakeholders
- **Risk appetite and tolerance** how organisations define acceptable risk and escalation thresholds
- **Three lines model** management ownership, risk oversight, and independent assurance
- **GRC lifecycle** define, assess, implement, measure, report, and improve

PRACTICAL EXERCISE

Map GRC responsibilities and escalation paths for a sample organisation.

Module 02 GOVERNANCE

Governance, policies and procedures

Learn how organisations translate security objectives into approved policies, standards, procedures, and measurable responsibilities.

- **Policy hierarchy** policies, standards, baselines, procedures, and guidelines
- **Security policy lifecycle** drafting, review, approval, communication, exceptions, and periodic review
- **Roles and accountability** RACI matrices, control ownership, and management sign-off
- **Asset and data classification** ownership, handling requirements, and protection expectations
- **Metrics and oversight** KPIs, KRIs, governance committees, and management reporting

PRACTICAL EXERCISE

Create a concise information-security policy outline and a RACI matrix.

Module 03 RISK MANAGEMENT

Information security risk management

Build a repeatable process for identifying and treating risks to systems, data, services, and business operations.

- **Risk identification** assets, threats, vulnerabilities, existing controls, and business impact
- **Risk analysis** likelihood, impact, inherent risk, residual risk, and qualitative scoring
- **Risk assessment methods** risk matrices, scenarios, assumptions, and evidence quality
- **Risk treatment** avoid, mitigate, transfer, or accept with documented approval
- **Risk register** owners, treatment plans, due dates, status, and review cadence
- **Risk monitoring** exceptions, emerging threats, KRIs, and reassessment

PRACTICAL EXERCISE

Build a risk register for a sample business application and recommend treatments.

Module 04 COMPLIANCE

Compliance, laws and regulatory obligations

Learn how to identify applicable requirements and convert them into traceable organisational actions.

- **Compliance fundamentals** legal, regulatory, contractual, and internal requirements
- **Applicability assessment** business sector, geography, data types, customers, and service commitments
- **Requirement mapping** obligation statements, control mapping, evidence, owners, and review dates
- **India context** overview of relevant privacy, cybersecurity, and sector-specific obligations where applicable
- **Compliance gaps** gap analysis, remediation plans, exceptions, and escalation

IMPORTANT

This is educational content, not legal advice. Requirements change and must be validated against current official sources and qualified counsel where needed.

PRACTICAL EXERCISE

Create a compliance obligations tracker for a fictional organisation.

Module 05 FRAMEWORKS

Security frameworks, standards and controls

Explore widely used frameworks and understand how to select and map controls to an organisation's risk and compliance needs.

- **ISO/IEC 27001** information security management system concepts, scope, risk treatment, and continual improvement
- **NIST Cybersecurity Framework** Govern, Identify, Protect, Detect, Respond, and Recover outcomes
- **NIST SP 800-53 and 800-30** control catalogues and risk assessment concepts
- **CIS Controls** prioritised safeguards and practical security improvement
- **Control mapping** common controls, control owners, implementation status, and evidence
- **Statement of Applicability** understanding inclusion, exclusion, and justification in an ISMS context

PRACTICAL EXERCISE

Map a small set of security controls across two frameworks and identify shared evidence.

Module 06

ASSURANCE

Audit readiness and control assessment

Understand how to prepare for internal reviews, external audits, and control effectiveness assessments.

- **Audit fundamentals** scope, criteria, objectives, sampling, independence, and audit trails
- **Evidence collection** policies, records, screenshots, tickets, logs, approvals, and interviews
- **Control testing** design effectiveness, operating effectiveness, and documented test procedures
- **Findings and nonconformities** root cause, severity, corrective action, and closure evidence
- **Audit preparation** evidence owners, evidence repository, readiness reviews, and timelines

PRACTICAL EXERCISE

Draft an evidence request list and write a sample control-testing result.

Module 07

THIRD-PARTY RISK

Vendor and third-party risk management

Assess the security risks introduced by suppliers, cloud providers, contractors, and other external partners.

- **Vendor inventory** criticality, service dependencies, data access, and business impact
- **Due diligence** questionnaires, certifications, independent reports, and security documentation
- **Risk tiering** inherent vendor risk, residual risk, and assessment depth
- **Contractual safeguards** security clauses, breach notification, data handling, and right-to-audit provisions
- **Ongoing monitoring** renewals, material changes, findings, and offboarding

PRACTICAL EXERCISE

Assess a fictional SaaS provider using a vendor risk questionnaire and scorecard.

Module 08

RESILIENCE

Incident management, privacy and business continuity

Connect GRC processes with incident response, personal-data handling, operational resilience, and recovery planning.

- **Incident governance** roles, escalation, severity, communications, and post-incident review
- **Privacy principles** data minimisation, purpose limitation, retention, access, and accountability
- **Business impact analysis** critical processes, dependencies, recovery time, and recovery point objectives
- **Business continuity and disaster recovery** plans, testing, lessons learned, and improvement
- **Exceptions and lessons learned** tracking corrective actions through to closure

PRACTICAL EXERCISE

Prepare an incident escalation matrix and a basic business continuity checklist.

Module 09

GRC OPERATIONS

GRC tools, documentation and reporting

Learn how GRC teams organise records, maintain traceability, and communicate risk status to decision-makers.

- **GRC platforms** use cases for risk registers, control libraries, audits, issues, and compliance mapping
- **Documentation management** version control, approvals, access control, retention, and evidence integrity
- **Dashboards** risk exposure, control coverage, overdue actions, audit findings, and exceptions
- **Reporting to leadership** concise risk narratives, trends, decisions required, and remediation status
- **Continuous improvement** lessons learned, maturity reviews, and programme metrics

PRACTICAL EXERCISE

Design a simple GRC dashboard using sample risk and control data.

Module 10 CAPSTONE

End-to-end GRC implementation project

Apply the course concepts to a fictional organisation and produce a compact set of GRC deliverables.

- **Define scope** describe the organisation, critical assets, business context, and GRC objectives
- **Assess risk** create a risk register with owners, ratings, and treatment plans
- **Map controls** select a suitable framework and map key controls to evidence
- **Review compliance** document applicable requirements and identify gaps
- **Prepare for audit** produce an evidence checklist and sample finding with corrective action
- **Present results** summarise residual risks, priorities, owners, deadlines, and management decisions

FINAL DELIVERABLES

GRC scope statement, risk register, control mapping sheet, compliance tracker, audit evidence checklist, and management summary.

REFERENCE TABLE

Core GRC deliverables at a glance

Deliverable	Purpose
Risk register	Track risks, owners, ratings, treatments, and review dates
Policy set	Document security expectations, responsibilities, and approved processes
Control matrix	Map requirements to controls, owners, implementation status, and evidence
Compliance tracker	Record obligations, applicability, evidence, and remediation actions
Audit evidence pack	Organise records and test results to support assurance activities
GRC dashboard	Communicate risk trends, control coverage, and overdue actions

WHO SHOULD LEARN

Who is this syllabus for?

This learning path is suitable for beginners exploring GRC and for IT or security professionals who want to understand risk and compliance workflows.

- **Beginners** who want to learn GRC terminology and foundational processes
- **Cybersecurity professionals** moving towards governance, risk, audit, or compliance roles
- **IT and cloud teams** working with controls, evidence, policies, or customer security reviews
- **Auditors and risk teams** who need a structured overview of cybersecurity control programmes

Ready to build your GRC skills?

Explore Techonquer training options or contact the team to discuss the learning path that fits your goals.

Contact Us: +916367098233

Enroll Now: https://techonquer.org/grc-training

Common questions

Do I need prior GRC experience?

No. The syllabus starts with core GRC concepts and builds towards risk assessment, control mapping, audit readiness, and a capstone project.

Will I learn about frameworks?

Yes. The syllabus introduces ISO/IEC 27001, the NIST Cybersecurity Framework, selected NIST publications, and CIS Controls.

Are practical exercises included?

Yes. Exercises include creating a risk register, drafting policy outlines, mapping controls, preparing evidence requests, and building a GRC dashboard.

Does this guarantee a certification or job?

No certification or employment outcome is implied by this syllabus. Check the course page for the current programme format and any certification details.