JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Cybersecurity Governance, Risk and Compliance Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Cybersecurity Governance, Risk and Compliance Training Course

Cybersecurity Governance, Risk and Compliance is a 1-week training course for GRC analysts, information security officers and internal auditors, who leave with a Cyber Control Matrix and Evidence Pack linking policies, controls and audit proof. Customers, insurers and audit committees now ask for demonstrable cyber controls rather than assurances, so a coherent policy hierarchy and traceable evidence have become daily needs. Jupiter Prime Training delivers this course on cybersecurity governance, risk and compliance.

Why Cybersecurity Governance, Risk and Compliance Matters Now

Three pressures converge on cyber GRC teams: audit committees that want a clear posture rating each quarter, overlapping control requirements from contracts, insurers and sector rules, and cloud services that move control ownership to suppliers. A team with one control library, mapped once and tested continuously, answers each new questionnaire in days; a team without one rebuilds evidence for every request. The course rests on the NIST Cybersecurity Framework 2.0 NIST CSF 2.0, whose Govern function frames oversight, and on ISO/IEC 27001:2022 for information security management system requirements.

Who Gains Most from Cybersecurity Governance, Risk and Compliance

- GRC analysts who maintain control libraries, policy registers and compliance calendars
- Information security officers who draft policies and approve exceptions
- Internal auditors who test cyber controls and judge evidence sufficiency
- Second-line risk specialists who rate cyber exposure for the enterprise risk profile
- Vendor assurance staff who assess supplier security questionnaires and attestations

A second-line function that sends its GRC analyst and an internal auditor together gains most, because both leave agreeing what evidence proves a control works.

Cybersecurity Governance, Risk and Compliance Capabilities

Participants turn scattered policies and requirements into one traceable chain from obligation to tested control.

- Design a cyber governance structure with charters, roles and escalation lines — the security steering committee
- Build a policy hierarchy from policy to standard to procedure — policy owners and approvers
- Align overlapping requirements in one control matrix using NIST CSF 2.0 and ISO/IEC 27001:2022 — control owners
- Specify evidence criteria and sampling for control testing — internal and external auditors
- Weigh policy exception requests against residual risk — the risk acceptance authority
-

Communicate cyber posture through indicators and heat maps — the audit and risk committee

Key Cybersecurity Governance, Risk and Compliance Terms

- Control matrix — a table mapping each requirement to the internal control, its owner, test method and evidence.
- Policy hierarchy — the layered set of policies, standards, procedures and guidelines, each more detailed than the one above.
- Policy exception — a time-bound, approved departure from a policy, with compensating measures and a named risk owner.
- Control effectiveness testing — checking through inspection, observation or re-performance whether a control operates as designed.
- Statement of Applicability — the ISO/IEC 27001 document listing which controls apply, which are excluded and why.
- Cyber posture — the overall state of an organisation's cyber defences, expressed through indicators and maturity ratings.

Cybersecurity Governance, Risk and Compliance Day by Day

Day 1: Governance Structures and Accountability

- Three Lines Model for Cyber — Separating Ownership, Oversight and Assurance
- Security Steering Committee Charter — Setting Decision Rights and Escalation
- NIST CSF 2.0 Govern Function — Framing Organisational Context and Roles
- RACI for Control Ownership — Removing Orphaned Responsibilities
- Banking and Energy Governance Contrasts — Matching Structure to Exposure

Day 2: Policy Hierarchy and Exceptions

- Policy, Standard and Procedure Layers — Placing Each Requirement Correctly
- Policy Drafting Conventions — Writing Testable Statements
- Policy Approval and Review Cycle — Keeping Documents Current
- Exception Request Workflow — Recording Compensating Measures and Expiry
- Policy Awareness Attestation — Proving Staff Acknowledgement

Day 3: Control Frameworks and Mapping

- ISO/IEC 27001:2022 Annex A Themes — Structuring the Control Library
- Statement of Applicability Drafting — Justifying Inclusions and Exclusions
- Crosswalk to NIST CSF 2.0 Categories — Answering Multiple Requirements Once
- Contract and Insurer Requirement Intake — Adding Obligations Without Duplication
- Supplier Control Inheritance — Deciding What Cloud Providers Cover

Day 4: Compliance Monitoring and Audit Evidence

- Control Testing Methods — Choosing Inspection, Observation or Re-Performance
- Evidence Sufficiency Criteria — Judging Completeness and Reliability
- Continuous Control Monitoring Feeds — Reducing Manual Sample Collection
- Finding Rating and Remediation Tracking — Prioritising Corrective Actions
- Cyber Risk Register Linkage — Connecting Failed Controls to Exposure

Day 5: Practising the Cyber Control Matrix and Evidence Pack

- Governance Gap Review — Applying Charter and RACI Lessons to a Case
- Exception Decision Panel — Applying Residual Risk Judgement to Requests
- Mock Audit Walk-Through — Applying Evidence Criteria to Sample Controls
- Committee Posture Dashboard — Selecting Indicators for Directors
- Cyber Control Matrix and Evidence Pack — Completing Mappings, Owners and Proof

Applying Cybersecurity Governance, Risk and Compliance After the Course

- Map one incoming customer security questionnaire to the control matrix and record which evidence already answers it.
- Review all open policy exceptions and close or renew each with a named risk owner.

Cybersecurity Governance, Risk and Compliance Questions FAQ

What is cybersecurity governance, risk and compliance, and why does it matter now?

It is the discipline of directing cyber security through structures, policies, control frameworks and evidence. It matters now because committees, customers and insurers ask for proof that controls work, and overlapping requirements multiply effort without a single mapped control library.

Which roles gain most from cybersecurity governance, risk and compliance training?

GRC analysts, information security officers and internal auditors gain most. They own the policies, control mappings and evidence that every audit and questionnaire relies on.

How does cybersecurity governance, risk and compliance differ from an AI governance course?

It covers the whole cyber control environment rather than oversight of machine learning models. An AI governance course deals with model inventories and algorithmic risk; this subject builds policy hierarchies, control mappings and audit evidence across all information systems.

What do you bring back from cybersecurity governance, risk and compliance training?

You bring back a Cyber Control Matrix and Evidence Pack. It maps requirements to controls, names owners, sets test methods and lists the evidence each control needs.

Cybersecurity Governance, Risk and Compliance: The Way Forward

The Cyber Control Matrix and Evidence Pack first informs which controls are tested before the next audit cycle. GRC analysts, control owners and internal auditors use it to answer questionnaires, plan testing and track remediation. After the first external audit, the evidence criteria are worth revisiting, as auditor feedback shows where proof was thin or excessive.