Governance, Risk and Compliance (GRC) Fundamentals

2027 □□□□□□□ 1 – □□□□□□□ 27
Edinburgh (UK)



Governance, Risk and Compliance (GRC) Fundamentals

Ref: 2022[illegible] **Date:** 27 **Location:** Edinburgh (UK) **Fees:** 5200 GBP

Governance, Risk and Compliance GRC is the joined-up way an organisation sets direction and accountability, handles uncertainty that could affect its objectives, and meets the obligations it must or chooses to follow. This GRC Fundamentals course runs for one week, is meant for professionals new to the field, and ends with each delegate drafting a GRC starter plan for one area of their organisation. Blackbird Training Centre delivers this introduction to GRC.

Introduction

The course rests on three reference points. ISO 31000:2018 is the international guideline on risk management principles and process. ISO 37301:2021 sets out the requirements of a compliance management system. The OCEG GRC Capability Model describes how governance, risk and compliance activities can work as one system. The level is foundational: each term is defined before it is applied, and no earlier GRC experience is assumed. Teaching is case-study based, using short scenarios from banking, healthcare and manufacturing to show how each idea looks inside a real organisation.

Course Objectives

- Define governance, risk and compliance in plain terms and explain how the three depend on one another in daily decisions.
- Distinguish governance from management, so that oversight duties and operational duties are assigned to the right people.
- Compare ISO 31000 and COSO Enterprise Risk Management and select the one that suits the organisation's size and needs.
- Apply a likelihood and impact scale to rate a set of risks and record them in a basic risk register.
- Distinguish mandatory compliance requirements from voluntary commitments when building an obligations register.
- Interpret simple maturity and effectiveness measures to judge where a first GRC effort should begin.

Target Audience

- Early-career staff moving into risk or compliance duties, who must decide which risks and obligations to record first.
- Team leaders who own operational processes, who must judge which controls their area needs and who checks them.
- Policy and administration staff who maintain organisational documents, who must choose how policies link to obligations.
- Junior internal audit and quality staff, who must judge whether a control is designed well before testing it.
- Project and finance staff joining a new GRC function, who must decide how their reporting feeds risk oversight.



Course Outline

Day 1: GRC Terms and How They Connect

- Governance vs Management: Who Sets Direction and Who Executes Within Limits
- Integrated GRC: Linking Oversight, Risk and Obligations Instead of Separate Silos
- OCEG GRC Capability Model: Principled Performance as a Reference Definition of GRC
- Frameworks and Standards Landscape: Where COSO, ISO 31000 and ISO 37301 Fit
- GRC Maturity Models: Gauging Organisational Readiness Before Building New Processes

Day 2: Governance Structures and Accountability

- Corporate Governance Principles: Accountability, Fairness, Transparency and Responsibility in Practice
- Board vs Executive Leadership: Separating Oversight Duties From Day-to-Day Management
- Three Lines Model: Roles of Management, Risk and Compliance Functions, Internal Audit
- Governance Structures: Committees, Delegations of Authority and Policy Hierarchies Explained
- Ethics and Corporate Culture: Codes of Conduct, Transparency and Speak-Up Channels

Day 3: Identifying and Assessing Risk

- Risk vs Issue: Telling an Uncertain Future Event From a Present Problem
- ISO 31000 vs COSO ERM: Two Reference Frameworks for Enterprise Risk Management
- Risk Identification and Assessment: Likelihood, Impact and Simple Rating Scales
- Risk Response Options: Avoid, Reduce, Transfer or Accept Within Risk Appetite
- Risk Monitoring and Reporting: Key Risk Indicators and Escalation to Leadership

Day 4: Setting Up Compliance Management

- Mandatory Requirements vs Voluntary Commitments: Two Sources of Compliance Obligations
- ISO 37301: Building Blocks of a Compliance Management System in Any Sector
- Compliance Arrangements: Policies, Training, Monitoring and the Handling of Breaches
- Internal Controls and Audit: How Preventive and Detective Controls Support Assurance
- Third-Party Compliance: Due Diligence and Ongoing Monitoring of Vendors and Suppliers

Day 5: Drafting a GRC Starter Plan

- GRC Technology vs Spreadsheets: Choosing Tools That Match Current Maturity
- Data Governance: Ownership, Quality and Information Management Behind GRC Reporting
- Change Management: Introducing GRC Roles and Processes Without Disrupting Operations
- GRC Effectiveness Measures: Indicators and Return on Investment for the Plan
- GRC Starter Plan: Completing the Roles Matrix, Risk Register and Obligations Register



Skills You Will Gain

- GRC vocabulary
- Governance roles mapping
- Delegation of authority design
- Risk rating and prioritisation
- Risk register maintenance
- Compliance obligations mapping
- Control design review
- Key risk indicator selection

Why Attend This Course

- From treating governance, risk and compliance as three unrelated departments to seeing how one decision touches all three.
- From listing risks informally in meetings to rating them on an agreed scale and recording owners and responses.
- From reacting to rules as they surface to keeping a single register of what the organisation must and has chosen to meet.
- From having no starting point to leaving with a GRC starter plan: a roles matrix, a risk register and an obligations register.

Conclusion

GRC, put simply, is the discipline of steering an organisation, anticipating what could go wrong and staying within its rules as one coordinated effort rather than three separate tasks. The course makes clear the line between governance and management, between a risk and an issue, and between a mandatory requirement and a voluntary commitment. It suits delegates who are new to GRC and need a sound grounding before moving on to advanced study of enterprise frameworks and board-level oversight.

Course FAQs

What is Governance, Risk and Compliance GRC?

GRC is an integrated approach in which an organisation directs and controls its activities, manages uncertainty affecting its objectives, and meets its legal and voluntary obligations through shared roles, data and processes rather than isolated functions.

What is the difference between governance and management in GRC?

Governance sets direction, risk appetite and accountability and oversees results; management runs operations within those limits. In GRC terms, a board approves the risk appetite, while managers own individual risks and controls and report on them.



Which standards does a GRC Fundamentals course follow?

The course draws on ISO 31000:2018 for risk management, ISO 37301:2021 for compliance management systems, the OCEG GRC Capability Model for integration, and the Three Lines Model and COSO ERM for roles and enterprise risk.

Is GRC Fundamentals training right for a newly appointed compliance officer?

Yes. A newly appointed compliance officer gains the shared vocabulary and the basic registers needed to work with risk, audit and management colleagues. Someone already running an established GRC framework may find the advanced level a closer fit.

What do delegates produce during GRC Fundamentals training?

Each delegate builds a GRC starter plan for one area of their organisation, made up of a governance roles matrix, a rated risk register with owners and responses, and a register of compliance obligations.

