BLACKBIRD FOR TRAINING

GRC Strategic Integration and Implementation for Leaders

11 – 22 January 2027
Zurich (Switzerland)

UK Traininig
PARTNER



www.blackbird-training.com

GRC Strategic Integration and Implementation for Leaders

Ref: 3254908_189774 **Date:** 11 – 22 January 2027 **Location:** Zurich (Switzerland) **Fees:** 10600 GBP

Governance, risk and compliance GRC strategic integration is the design of one coordinated capability through which an organisation sets direction, manages uncertainty and meets its legal and ethical obligations. This two-week course is for board members, C-suite executives and senior risk, compliance and audit leaders, and its final deliverable is an integrated GRC implementation roadmap setting out structures, priorities, controls and milestones.

Introduction

Three frameworks anchor the course. COSO Enterprise Risk Management – Integrating with Strategy and Performance links risk to strategy-setting and performance. ISO 31000:2018 is the international standard giving principles and a process for managing risk. The G20/OECD Principles of Corporate Governance set out expectations for boards, shareholders and disclosure. The level is advanced, and the two weeks allow an integrated capability to be designed and implemented in depth rather than surveyed. Teaching combines case studies from banking, energy and public administration with a running design simulation.

Course Objectives

- Distinguish integrated from siloed GRC and define the structures, roles and reporting lines an integrated capability needs
- Compare corporate and public-sector governance models and apply the G20/OECD Principles of Corporate Governance to board practice
- Apply COSO ERM and ISO 31000 together to set risk appetite, assess risks and link them to strategic performance
- Select digital compliance and RegTech tools and justify the oversight each one requires
- Interpret risk culture through cultural audits and behavioural reviews and justify leadership actions that strengthen accountability
- Apply internal control and post-incident review methods to design an integrated GRC implementation roadmap



Target Audience

- Board members and C-suite executives accountable for governance, who must decide how far GRC functions should be integrated
- Chief risk, compliance and audit officers, who must judge how responsibilities are divided across the three lines
- Senior leaders of public-sector bodies, who must choose governance and accountability arrangements that withstand public scrutiny
- Heads of strategy and transformation sponsoring digital initiatives, who must assess which governance and cyber controls new technology needs
- Senior legal and ethics advisers working across jurisdictions, who must determine how overlapping legal obligations are met consistently

Course Outline

Day 1: GRC Integration Foundations and Governance Structures

- Integrated vs Siloed GRC: Shared Processes Compared with Separate Specialist Units
- Evolution of Governance Models: From Rule-Based Oversight to Value-Focused Regulatory Compliance
- Governance and Value Creation: Aligning Board Oversight with Strategic Objectives
- Governance Structures: Board, Audit Committee and Compliance Function Roles and Reporting Lines
- Three Lines Model: Dividing Management, Oversight and Independent Assurance Responsibilities

Day 2: Stakeholders, Internal Audit and Governance Reporting

- Shareholder Activism vs Public Scrutiny: Two Sources of Pressure on Governance Choices
- Stakeholder Ecosystem Mapping: Ranking Investors, Supervisors, Employees and Communities by Influence
- Internal Audit in GRC Integration: Moving from Compliance Checking to Assurance Over Risk
- Governance Performance Communication: Reporting Effectively to Boards, Investors and the Public
- Project Governance and Accountability: Decision Rights and Gateways in Public-Sector Projects

Day 3: Corporate and Public-Sector Governance Models

- Corporate vs Public-Sector Governance: Shareholder Accountability Compared with Public Accountability
- G20/OECD Principles of Corporate Governance: Core Provisions and Their Practical Use
- Cross-Border Governance: Group Structures and Subsidiary Oversight in Multinational Organisations
- ESG in Governance: Embedding Environmental, Social and Governance Factors in Board Decisions
- Local Governance and Public Accountability: Transparency Duties of Municipal and Agency Leaders



Day 4: Legal and Ethical Dimensions of Compliance

- Rules-Based vs Values-Based Compliance: Prescriptive Controls Compared with Integrity-Led Conduct
- Cross-Jurisdictional Compliance: Overlapping Data Protection, Financial Reporting and Anti-Bribery Laws
- Anti-Bribery and Anti-Corruption Strategies: Due Diligence, Gifts Policies and Third-Party Checks
- Ethical Leadership and Integrity: Setting the Tone at the Top Through Decisions
- Compliance Failure Case Studies: Causes, Recoveries and Reforms After Major Breaches

Day 5: Technology and Digital Compliance

- RegTech vs Traditional Compliance Monitoring: Automated Surveillance Compared with Periodic Manual Review
- AI-Based Monitoring and Digital Reporting Platforms: Uses, Limits and Oversight Needs
- Governance of Digital Transformation: Decision Rights and Risk Review for Technology Initiatives
- Cyber Governance and Information Security: Board Oversight of Cyber Risk and Controls
- Digital Compliance Maturity: Assessing and Raising the Maturity of Compliance Technology

Day 6: Enterprise Risk Management Fundamentals

- Risk Appetite vs Risk Tolerance vs Risk Capacity: Three Limits on Risk-Taking
- Aligning Risk Management with Business Objectives: Linking Risks to Strategy and Plans
- Risk Governance Across Units: Committees, Risk Owners and Escalation Routes
- Qualitative vs Quantitative Risk Assessment: Heat Maps Compared with Modelled Loss Estimates
- Risk Registers: Structuring Entries So Ratings and Owners Are Comparable Across Units

Day 7: Emerging Risks and Strategic Response

- Scenario Planning vs Risk Intelligence: Exploring Futures Compared with Tracking Live Signals
- Cyber, Reputation and Third-Party Risks: Sources, Indicators and Response Options
- Climate-Related Risks: Physical and Transition Risks to Finances and Operations
- Geopolitical Risk Tracking: Monitoring Sanctions, Instability and Trade Disruption Signals
- Emerging Risk Radar: Prioritising Signals for Board Attention and Response Planning

Day 8: COSO ERM and ISO 31000 in Advanced Application

- COSO ERM vs ISO 31000: Integrating Two Frameworks into One Risk Process
- Risk and Performance Linkage: Connecting Key Risk Indicators to Strategic Performance Metrics
- Embedding Risk Ownership: Assigning Accountability for Risks Within Daily Operations
- Risk Visualisation: Dashboards and Digital Compliance Tools for Board Reporting
- COSO ERM Components: Governance, Strategy, Performance, Review and Information Applied Together



Day 9: Risk Culture and Leadership

- Risk-Aware vs Risk-Averse Culture: Informed Risk-Taking Compared with Habitual Avoidance
- Leadership's Role in Risk Accountability: Behaviours That Make Ownership Visible to Staff
- Risk Awareness Communication: Messages, Channels and Training for Different Staff Groups
- Cultural Audits and Behavioural Reviews: Methods for Measuring an Organisation's Risk Culture
- Incentives and Consequences: Aligning Reward Structures with Desired Risk Behaviours

Day 10: Implementing an Integrated GRC Capability

- Manual vs Automated Controls: Internal Controls in Procurement and Finance Processes
- Control Automation and Audit Workflows: Applying Earlier Digital Tools to Assurance Work
- Control Effectiveness Analytics: Applying Key Risk Indicators to Test Whether Controls Work
- Post-Incident Reviews: Applying Root-Cause Findings to Continuous Improvement of GRC
- Integrated GRC Implementation Roadmap: Finalising Structures, Priorities, Controls and Milestones

Skills You Will Gain

- GRC Operating Model Design
- Board Governance Assessment
- Risk Appetite Setting
- Integrated Risk Assessment
- Compliance Technology Selection
- Risk Culture Diagnosis
- Internal Control Design
- Post-Incident Review

Why Attend This Course

- From governance, risk and compliance units working in parallel to one integrated capability with shared processes and data
- From risk registers kept for audit purposes to risk appetite and indicators tied to strategy and performance
- From reacting to compliance failures to anticipating emerging, cyber and third-party risks through scenarios and intelligence
- From a broad intention to integrate to an implementation roadmap with structures, priorities, controls and milestones



Conclusion

Integrated GRC treats direction-setting, risk-taking and rule-keeping as one system with shared owners, data and assurance rather than three separate departments. The course clarifies three distinctions: integrated versus siloed GRC, risk appetite versus tolerance and capacity, and rules-based versus values-based compliance. It is the right choice for board members and senior executives who must design and implement an integrated capability, and who need two weeks to work through governance, risk, compliance, technology and culture in depth.

Course FAQs

What is GRC strategic integration?

GRC strategic integration is the alignment of governance, risk management and compliance into one coordinated capability, with shared structures, risk appetite, data, controls and assurance, so that leadership decisions, risk-taking and legal obligations are managed together.

What is the difference between risk appetite and risk tolerance in GRC integration?

Risk appetite is the amount and type of risk an organisation is willing to pursue to meet its objectives. Risk tolerance is the acceptable variation around a specific objective or measure, usually expressed as a numeric limit that triggers escalation.

Which frameworks does GRC strategic integration and implementation training follow?

The course follows COSO Enterprise Risk Management – Integrating with Strategy and Performance and ISO 31000:2018 for risk, the G20/OECD Principles of Corporate Governance for boards, and the Three Lines Model for assurance roles.

Is GRC strategic integration and implementation training right for a chief risk officer?

Yes. A chief risk officer leads the second line and must connect risk appetite, indicators and culture with governance and compliance, which the sessions on COSO ERM, ISO 31000, risk culture and control analytics address directly.

What do delegates produce in GRC strategic integration and implementation training?

Delegates produce an integrated GRC implementation roadmap for their organisation, covering governance structures, the division of roles across the three lines, risk appetite statements, priority controls, technology choices and implementation milestones.

