# Chartered Governance Institute UK & Ireland

The Chartered Governance Qualifying Programme

# Risk Management

Syllabus

# Risk Management

Level 7, Part Two Programme

Total hours study time: 200

**Introduction**
The aim of this module is for students to develop and extend their understanding of the discipline of risk management, including how risk management links to compliance management and complements effective corporate governance in organisations.

All organisations manage risk, but in the last few decades risk management has become increasingly formalised and organised. A key driver for this has been corporate governance regulation which has emphasised the central role that risk management plays, both in terms of ensuring effective internal control within organisations and in helping to manage risks which may threaten an organisation's strategic objectives. Hence risk management has become a board level concern, with increased risk reporting and board level discussions on subjects such as risk appetite and risk culture.

In this module students will explore the role of the board in terms of risk management, as well as the people, processes and techniques that can be used to support the board and ensure the effective assessment, monitoring and control of risk at all levels of an organisation.

**Learning outcomes**
After successful completion of this module you should:

1   Understand how to advise the board on the use of risk frameworks as a basis for appraising, evaluating, and supporting risk management
2   Be able to critically evaluate approaches to risk management
3   Be able to critically evaluate the management of risk and provide professionally appropriate advice to those responsible for governance
4   Understand how to critically examine the impact of the business environment on risk with regard to legislation, policy and industry changes
5   Be able to critically evaluate the impact of organisational conduct, behaviours and culture on risk management practices.

**Module content**

| Section A: Risk frameworks | |
|---|---|
| *50% – 100 Learning hours* | |
| *LO.1: Understand how to advise the board on the use of risk frameworks as a basis for appraising, evaluating, and supporting risk management* | |
| *LO.2: Be able to critically evaluate approaches to risk management* | |
| **Topic area** | **Exemplification** |
| The global risk environment | • The importance of risk management: a stakeholder approach<br>  • the organisation as a nexus of global stakeholders<br>  • a shareholder perspective on risk management<br>    − bankruptcy costs<br>    − cash flow fluctuations<br>  • managing conflicts of interest between stakeholders<br>• Reasons for risk management regulation:<br>  • the problem of self-regulation<br>  • market failures<br>  • weighing up the benefits and costs of risk management regulation<br>  • the role of compliance management<br>• The global regulatory environment for risk management:<br>  • the need for international regulation and standards<br>  • international regulation and standards in relation to risk management:<br>    − corporate governance<br>    − environmental regulation<br>    − financial stability<br>    − health and safety<br>  • global regulatory principles:<br>    − rules<br>    − guidance<br>    − principles and outcomes-based regulation<br>    − risk-based regulation<br>• International risk management standards:<br>  • ISO 31000:2018, Risk management – Principles and Guidelines<br>  • Committee of Sponsoring Organizations of the Treadway Commission (COSO)<br>  • ISO 19600:2014, Compliance Management Systems |

| Topic area | Exemplification |
|---|---|
| Regulatory frameworks | • The link between risk management practices and corporate government regulation<br>• UK regulations: the Corporate Governance Code:<br>  ○ brief history of UK corporate governance regulation<br>  ○ the 'comply or explain' approach<br>  ○ the 'comply and sign' approach<br>  ○ key risk management regulations from UK Corporate Governance Code<br>  ○ Corporate governance in organisations without a premium listing<br>• Irish Regulations:<br>  ○ Irish Companies Act 2014<br>  ○ Irish system of corporate governance<br>• European Union regulations<br>• G20/OECD Principles of Corporate Governance<br>• World Bank corporate governance and financial reporting initiatives<br>• Corporate Governance regulations in other nations:<br>  ○ Channel Islands<br>  ○ United Arab Emirates<br>  ○ Kenya<br>  ○ Nigeria<br>  ○ Russian Federation<br>  ○ United States of America |
| Sector regulators | • Sector regulation on risk management for EU member states:<br>  ○ relationship between EU and member state regulation<br>  ○ European Central Bank<br>  ○ other EU-wide risk management regulators:<br>• Financial services risk management regulation:<br>  ○ British financial regulators:<br>    − Prudential Regulatory Authority (PRA)<br>    − Financial Conduct Authority (FCA)<br>    − Financial Ombudsman<br>    − Guernsey and Jersey financial services commissions<br>  ○ Irish regulators<br>  ○ financial services sector regulators in other countries<br>• Health and safety regulation:<br>  ○ health and safety agencies in the British Isles:<br>    − UK Health and Safety Executive<br>    − Guernsey Health and Safety Executive<br>    − Jersey Health and Safety Inspectorate<br>  ○ Irish Health and Safety Authority |

| Topic area | Exemplification |
|---|---|
| Sector regulators (*cont.*) | • health and safety regulators in other countries<br>• Environmental regulation:<br>  • environmental agencies in the British Isles<br>  • Irish Environmental Protection Agency<br>  • environmental regulators in other countries |
| Risk management frameworks and standards | • Contents of a risk management framework:<br>  • risk management procedures<br>  • technology systems that support risk management:<br>    − risk reports<br>  • risk appetite statement<br>  • training and awareness<br>  • risk governance and compliance arrangements<br>  • specialist staff<br>  • risk committees<br>• A detailed look at ISO31000:2018:<br>  • establishing the context<br>  • risk assessment<br>  • risk treatment<br>  • communication and consultation<br>  • recording and reporting<br>  • monitoring and review<br>• National standards and guidelines:<br>  • National Guidance on Implementing ISO 31000:<br>    − British Standard BS 31100<br>    − National Standards Agency of Ireland<br>  • The Orange Book<br>  • The Institute of Risk Management Standard<br>  • COSO Enterprise Risk Management Framework:<br>    − governance and culture<br>    − strategy and objective setting<br>    − performance<br>    − review and revision<br>    − information, communication and reporting<br>  • Control Objectives for Information and Related Technologies (COBIT):<br>    − core governance principles<br>    − generic process descriptions<br>    − control objectives<br>    − management guidelines<br>    − process maturity models |

| Topic area | Exemplification |
|---|---|
| Key risk management concepts | • Defining risk:<br>    • distinguishing between risk and uncertainty<br>    • risk events<br>    • probability, impact and exposure<br>    • pure and speculative risks<br>    • inherent, residual and target risks<br>    • principal and emerging risks<br>    • other useful concepts and definitions<br>• Categorising risk:<br>    • common approach to risk categorisation:<br>        − business risk<br>        − credit risk<br>        − market risk<br>        − liquidity risk<br>        − operational risk<br>        − reputation risk<br>    • alternative approaches to risk categorisation:<br>        − Kaplan and Mikes three risk categorisation<br>        − UK Treasury Orange Book Classification<br>    • risk of internal control failure<br>    • deciding on appropriate risk categorisation<br>    • role of the board<br>• Risk interconnectivity<br>• Risk perception:<br>    • subjective judgements and actions<br>    • unquantifiable risk<br>    • subjectivity of risk perception<br>• Other practical challenges and trends surrounding risk models<br>    • remediation techniques |
| Risk management as a foundation of organisational success | • The evolution of risk management<br>• The role of risk management in organisations:<br>    • reducing uncertainty<br>    • anticipation and resilience<br>    • supporting the internal control environment:<br>        − risk based compliance reviews<br>        − internal audit<br>        − external audit<br>• Linking risk to strategy:<br>    • role of the board |

| Topic area | Exemplification |
|---|---|
| Risk management as a foundation of organisational success (*cont.*) | • Creating value through risk:<br>　• exploiting risk as a part of day-to-day operations<br>　• strategic risk taking<br>　• adverse risk taking<br>　• role of the board<br>• Regulatory view of risk |
| Risk management processes, perspectives and responsibilities | • The standard risk management process:<br>　• process overview<br>　• risk identification<br>　• risk assessment<br>　• risk monitoring<br>　• risk control<br>• Enterprise risk management (ERM):<br>　• essential characteristics of ERM:<br>　　− holistic<br>　　− value added<br>　• formal and informal factors<br>　• benefits of ERM<br>　• elements of an effective ERM process:<br>　　− ERM policy and procedures<br>　　− risk appetite<br>　　− risk reporting<br>　　− risk and audit committees<br>　　− escalation and whistleblowing procedures<br>　　− business continuity management<br>• Roles/functions and responsibilities for risk management:<br>　• the board of directors and executive management<br>　• risk committees<br>　• chief risk officer<br>　• risk manager and risk function<br>　• compliance manager and compliance function<br>　• internal audit and risk management<br>　• company secretary or governance professional<br>　• other key functions:<br>　　− finance<br>　　− health and safety<br>　　− human resource management<br>　　− information security<br>　　− marketing and public relations<br>　　− operations |

| Topic area | Exemplification |
|---|---|
| Frameworks for governance, risk and compliance | • The role of governance and compliance within a risk management context:<br>  • implementing effective risk management policies and procedures<br>  • determining and implementing an effective risk appetite framework<br>• Components of an effective compliance management framework:<br>  • establishing compliance standards<br>  • developing compliance processes and controls:<br>    − compliance management policies and procedures<br>    − compliance reporting and escalation processes<br>    − compliance training and communication<br>  • linking compliance management with internal control<br>  • risk-based compliance<br>  • roles and responsibilities:<br>    − compliance function<br>    − boards and risk and audit committees<br>    − company secretary and governance professionals<br>    − other business areas<br>• Governance structures for risk management:<br>  • the three lines of defence and the three lines model<br>  • the five lines of assurance<br>  • the role of the board<br>  • governing risk management within a group structure:<br>• ISO 19600:2014 – compliance management systems<br>• Combining governance risk and compliance (GRC):<br>  • the rationale for GRC<br>  • the scope of GRC:<br>    − financial GRC<br>    − information technology GRC<br>    − legal GRC<br>  • GRC information systems |

| Section B: Managing risk and compliance |
|---|
| *25% – 50 Learning hours* |
| *LO.3: Be able to critically evaluate the management of risk and provide professionally appropriate advice to those responsible for governance* |

| Topic area | Exemplification |
|---|---|
| Evaluating and reporting risk | • Techniques for identifying risk events:<br>  • expert judgement<br>  • focus groups and surveys<br>  • checklists<br>  • physical inspections<br>  • analytical approaches<br>    − structured what-if technique (SWIFT)<br>    − Delphi technique<br>    − root cause analysis<br>    − system and process mapping<br>  • loss events and near miss investigations<br>• Identifying emerging risk:<br>  • Political, Economic, Social and Technical (PEST) analysis<br>  • Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis<br>  • World Economic Forum Global Risk Report<br>• Risk assessment techniques:<br>  • qualitative risk assessment<br>  • quantitative risk assessment<br>  • hybrid approaches:<br>    − stress testing<br>    − scenario analysis<br>• Risk registers and risk and control self-assessments:<br>  • the risk register<br>  • risk and control self-assessments<br>• Risk reporting:<br>  • Red, Amber, Green (RAG) reporting<br>  • risk reporting tools:<br>    − heat maps<br>    − risk event and near miss databases<br>    − risk, control and performance indicators<br>    − risk dashboards and balanced scorecards<br>    − narrative reporting<br>  • designing and implementing risk reports:<br>    − audience<br>    − size and level of detail<br>    − level of statistical complexity<br>    − frequency |

| Topic area | Exemplification |
|---|---|
| Risk culture, appetite and tolerance | • Risk appetite as a mechanism for balancing risk and return:<br>  ○ defining risk appetite<br>  ○ the role of risk appetite:<br>• Risk tolerance and risk capacity<br>• Expressing risk appetite:<br>  ○ metric-based expressions of risk appetite:<br>    − probability and impact boundaries<br>    − targets, limits and thresholds<br>  ○ non-metric expressions of risk appetite:<br>    − values<br>    − risk management principles<br>    − risk appetite statement<br>• Determining risk appetite:<br>  ○ factors to consider when determining appetite<br>  ○ the role of the board<br>  ○ the role of the chief risk officer and risk function<br>• Good practice guidance on implementing risk appetite:<br>  ○ Chief Risk Officers Forum<br>  ○ Institute of Risk Management<br>  ○ COSO risk appetite thought leadership paper<br>• Defining culture and risk culture:<br>  ○ defining organisational culture<br>  ○ defining risk culture<br>  ○ risk sub-cultures<br>  ○ the consequences of risk culture 'failures'<br>• Assessing, monitoring and controlling risk culture:<br>  ○ risk culture surveys and metrics<br>  ○ controlling risk culture<br>  ○ practical guidance on assessing, monitoring and controlling risk culture |
| Compliance management | • Linking compliance and risk management:<br>  ○ risk management rules and regulations<br>  ○ managing compliance risk<br>• Roles and responsibilities for compliance management:<br>  ○ board of directors<br>  ○ audit committee<br>  ○ company secretary/governance professional<br>  ○ compliance function<br>  ○ risk management function<br>  ○ internal audit function<br>  ○ other specialist functions<br>  ○ line managers across the organisation<br>  ○ staff members |

| Topic area | Exemplification |
|---|---|
| Compliance management (*cont.*) | • Risk based compliance monitoring<br>• Compliance management tools:<br>   ○ compliance policies and procedures<br>   ○ compliance codes of conduct<br>   ○ compliance reviews and audits<br>   ○ compliance impact analysis<br>   ○ gap analysis and action planning<br>   ○ compliance reporting<br>   ○ HR related controls<br>   ○ whistleblowing policies and procedures<br>   ○ establishing an appropriate culture |

## Section C: Risk and the business environment

**25% – 50 Learning hours**

*LO.4: Understand how to critically examine the impact of the business environment on risk with regard to legislation, policy and industry changes*

*LO.5: Be able to critically evaluate the impact of organisational conduct, behaviours and culture on risk management practices*

| Topic area | Exemplification |
|---|---|
| Risk control strategies | <ul><li>Reasons for risk control:<ul><li>managing probability and impact</li><li>using controls for loss events to help seize opportunities</li></ul></li><li>The five Ts of risk control:<ul><li>tolerate</li><li>treat</li><li>transfer</li><li>terminate</li><li>take the opportunity</li></ul></li><li>Risk treatment techniques:<ul><li>PCDD hazard risk typology – preventive, corrective, directive, detective</li><li>other categories of risk treatment techniques:<ul><li>formal controls</li><li>informal controls</li></ul></li></ul></li><li>Common risk treatment controls</li><li>Risk financing:<ul><li>retained risk financing</li><li>insurance risk transfer</li><li>non-conventional risk transfer for the financial effects of risk</li></ul></li><li>Controlling major loss events:<ul><li>crisis management</li><li>business continuity planning</li></ul></li><li>Controlling third party risks</li></ul> |
| Risk management in practice | <ul><li>Common applications of risk management practice:<ul><li>an overview of applications</li><li>operations or operational risk management</li><li>cyber risk management</li><li>project risk management</li><li>supply chain risk management</li></ul></li><li>Risk management, corporate social responsibility and sustainability</li></ul> |

| Topic area | Exemplification |
|---|---|
| Risk management in practice (*cont.*) | <ul><li>Regulatory reporting:<ul><li>regulatory reporting processes</li><li>roles and responsibilities for regulatory reporting:<ul><li>company secretary and other governance professionals</li><li>compliance function</li><li>finance function</li><li>health and safety function</li><li>information technology function</li><li>risk function</li><li>other business functions</li></ul></li></ul></li></ul> |
| Trends and future developments for risk management | <ul><li>Crime:<ul><li>offences against an individual</li><li>offences against property or services</li><li>violation of laws</li><li>other offences</li><li>countering the workplace crime</li><li>cybercrime prevention</li></ul></li><li>Financial crime:<ul><li>the impact of financial crime on organisations</li><li>anti-money laundering</li><li>countering the financing of terrorism</li><li>common AML and CFT controls</li><li>reporting a suspicious transaction or activity</li></ul></li><li>Bribery and corruption:<ul><li>importance of complying with principles of the UK Bribery Act 2010</li><li>key principles of internal control mechanisms</li></ul></li><li>Political risk, including sanctions</li><li>Corporate gifts</li><li>People risk:<ul><li>behavioural risk</li><li>common sources of behavioural risks:<ul><li>bullying</li><li>negligence</li><li>information leaks</li><li>criminal activity</li><li>effects of behavioural risk</li></ul></li></ul></li></ul> |

| Topic area | Exemplification |
|---|---|
| Trends and future developments for risk management (*cont.*) | <ul><li>managing behavioural risk:<ul><li>recruitment controls</li><li>codes of conduct</li><li>risk culture</li></ul></li></ul><ul><li>Climate change risk</li><li>Asymmetric risk</li><li>Reputation and resilience</li><li>The changing balance between tangible and intangible risks</li><li>Shareholder activism:<ul><li>role of the board</li></ul></li></ul> |
| More trends and future developments for risk management | <ul><li>Complex and connected risks:<ul><li>the modern world and the growth in emerging risks:<ul><li>complexity</li><li>interconnectedness</li><li>globalisation</li></ul></li></ul></li><li>Managing emerging risks:<ul><li>board level strategic environment emerging risk assessments</li><li>scenario planning and reverse stress testing</li><li>current examples of emerging risk:<ul><li>the networked economy</li><li>social media and digital natives</li><li>disruptive technologies</li><li>global pandemics (COVID-19)</li></ul></li></ul></li><li>Changing knowledge and skills:<ul><li>in-demand skills</li><li>talent sourcing</li><li>talent management</li><li>talent training</li><li>talent risk management framework</li><li>the workforce of the future</li><li>the role of the board</li></ul></li><li>Digital transformation:<ul><li>big data</li><li>automated decision making:<ul><li>algorithmic decision making</li><li>artificial intelligence</li><li>advantages and disadvantages</li><li>governance and compliance implications</li></ul></li><li>other new technologies</li><li>managing risks in a digital world</li><li>digital risks</li><li>the role of the board</li></ul></li></ul> |