CHARTERED GOVERNANCE Hong Kong

Risk Management

Chartered Governance Qualifying Programme

Syllabus

Chartered Governance Institute UK & Ireland

The Hong Kong Chartered Governance Institute

Chartered Governance Qualifying Programme

Risk Management

Part Two Programme

Total study time: 200 hours

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. This has made risk management 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 board's role 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 be able to:

1. Demonstrate an understanding of the global and regional regulatory framework for risk management and the relationships between risk management and corporate governance, compliance and ethics.
2. Critically evaluate approaches to risk management and advise the board on the use of risk frameworks as a basis for appraising, evaluating and supporting risk management.
3. Critically evaluate the management of risk and provide professionally appropriate advice to those responsible for governance.
4. Critically examine the impact of the business environment on risk with regard to legislation, policy and industry changes.
5. 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: Demonstrate an understanding of the global and regional regulatory framework for risk management and the relationships between risk management and corporate governance, compliance and ethics LO.2: Critically evaluate approaches to risk management and advise the board on the use of risk frameworks as a basis for appraising, evaluating, and supporting risk management	
Topic area	**Learning areas**

The global risk environment	• The importance of risk management: a stakeholder approach:
	  • the organisation as a nexus of global stakeholders
	  • a shareholder perspective on risk management:
	  - bankruptcy costs
	  - cash flow fluctuations
	  • managing conflicts of interest between stakeholders
	• Reasons for risk management regulation:
	  • the problem of self-regulation
	  • market failures
	  • weighing up the benefits and costs of risk management
	  • the role of compliance management
	• The relationship of risk management with:
	  • corporate governance
	  • compliance
	  • internal control
	  • whistle-blowing
	  • sustainability
	  • financial report reliability
	  • environmental protection
	  • anti-money laundering
	  • anti-bribery and corruption
	  • community and social development
	• The global regulatory environment for risk management:
	  • the need for international regulation and standards
	  • international regulation and standards in relation to risk management:
	  - corporate governance
	  - environmental regulation
	  - financial stability
	  - health and safety
	  • global regulatory principles:
	  - rules
	  - guidance

Topic area	Learning areas
The global risk environment (*cont.*)	- principles and outcomes-based regulation - risk-based regulation • International risk management standards: • ISO 31000:2018, Risk Management – Principles and Guidelines • Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Framework • ISO 19600:2014, Compliance Management Systems
Regulatory frameworks	• The link between risk management practices and corporate governance regulation • UK regulations: Corporate Governance Code: • brief history of UK corporate governance regulation • the 'comply or explain' approach • the 'comply and sign' approach • key risk management regulations • corporate governance in public sector and non-governmental organisations (NGOs) • Appendix 14 Corporate Governance Code and Corporate Governance Report of SEHK Listing Rules • G20/OECD Principles of Corporate Governance • World Bank corporate governance and financial reporting initiatives • Corporate governance codes and other relevant rules and regulations for risk management in Hong Kong: • cyber security • corporate governance (listed companies, public sector and non-governmental organisations (NGOs)) • anti-money laundering • monetary and banking • prevention of bribery and corruption • intellectual property rights • environmental protection • Corporate governance codes and other relevant compliance requirements: • Sarbanes-Oxley Act in the US • Other guidelines in Hong Kong and the Mainland: - 'Internal Control and Risk Management - A Basic framework' – issued by the Hong Kong Institute of Certified Public Accountants - Mainland China's Internal Control and Risk Management Standards

Topic area	Learning areas

Sector regulation	• Risk management regulation within Hong Kong financial services:
	  • Hong Kong Monetary Authority
	  • Securities and Futures Commission
	  • Hong Kong Insurance Authority
	• Financial services and risk management regulations in the US, including the Foreign Account Tax Compliance Act (FATCA)
	• Financial services and risk management regulations in Mainland China
	• OECD compliance, including the Common Reporting Standard (CRS)
	• Environmental risk management regulation in Hong Kong
	• Regulators of listed corporations in Hong Kong:
	  • Stock Exchange of Hong Kong
	  • Securities and Futures Commission
	  • Financial Reporting Council

Risk management frameworks and standards	• Contents of a risk management framework:
	  • risk management procedures
	  • technology systems that support risk management
	  - risk reports
	  • risk appetite statement
	  • training and awareness
	  • risk governance and compliance arrangements
	  • specialist staff
	  • risk committees
	• ISO 31000:2018, Risk Management Guidelines:
	  • establishing the context
	  • risk assessment
	  • risk treatment
	  • communication and consultation
	  • recording and reporting
	  • monitoring and review
	• National standards and guidelines:
	  • National guidance on Implementing ISO 31000:
	  - British Standard BS 31100
	  • The Orange Book
	  • The IRM's Risk Management Standard
	  • COSO Enterprise Risk Management Framework:
	  - governance and culture
	  - strategy and objective setting
	  - performance

Topic area	Learning areas
Risk management frameworks and standards (*cont.*)	- review and revision - information, communication and reporting • Control Objectives for Information and Related Technologies (COBIT): - core governance principles - generic process descriptions - control objectives - management guidelines - process maturity models
Key risk management concepts	• Defining risk: • distinguishing between risk and uncertainty • risk events • probability, impact and exposure • pure and speculative risks • inherent, residual and target risks • principal and emerging risks • other useful concepts and definitions • Categorising risk: • common approach to risk categorisation: - business risk - credit risk - market risk - liquidity risk - operational risk - reputation risk • alternative approaches to risk categorisation - Kaplan and Mikes three risk categorisation - UK Treasury Orange Book Classification • risk of internal control failure • deciding on appropriate risk categorisation • role of the board • Risk interconnectivity • Risk perception: • subjective judgements and actions • unquantifiable risk • subjectivity of risk perception • Other practical challenges and trends surrounding risk models • remediation techniques
Risk management as a foundation of organizational success	• The evolution of risk management • The role of risk management in organisations: • reducing uncertainty • anticipation and resilience

Topic area	Learning areas

Risk management as a foundation of organizational success (*cont.*)	• supporting the internal control environment:
	  - risk based compliance reviews
	  - internal audit
	  - external audit
	• Linking risk to strategy:
	  • role of the board
	• Creating value through risk:
	  • exploiting risk as a part of day-to-day operations
	  • strategic risk taking
	  • adverse risk taking
	  • role of the board
	• Regulatory view of risk

Risk management processes, perspectives and responsibilities	• The standard risk management process:
	  • process overview
	  • risk identification
	  • risk assessment
	  • risk monitoring
	  • risk control
	• Enterprise risk management (ERM):
	  • essential characteristics of ERM:
	  - holistic
	  - value added
	  • formal and informal factors
	  • benefits of ERM
	  • elements of an effective ERM process:
	  - ERM policy and procedures
	  - risk appetite
	  - risk reporting
	  - risk and audit committees
	  - escalation and whistleblowing procedures
	  - business continuity management
	• Roles/functions and responsibilities for risk management:
	  • the board of directors and executive management
	  • risk committees
	  • chief risk officer
	  • risk manager and risk function
	  • compliance manager and compliance function
	  • internal audit and risk management
	  • company secretary or governance professional
	  • other key functions:
	  - finance

Topic area	Learning areas
Risk management processes, perspectives and responsibilities (*cont.*)	- health and safety - human resource management - information security - marketing and public relations - operations

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

Section B: Managing risk and compliance ***25% – 50 learning hours*** LO.3: Critically evaluate the management of risk and provide professionally appropriate advice to those responsible for governance	
Topic area	**Learning areas**

Evaluating and reporting risk	• Techniques for identifying risk events:
	  • expert judgement
	  • focus groups and surveys
	  • checklists
	  • physical inspections
	  • analytical approaches:
	  - structured what-if technique (SWIFT)
	  - Delphi technique
	  - root cause analysis
	  - system and process mapping
	  • loss events and near miss investigations
	• Identifying emerging risk:
	  • political, economic, social and technical (PEST) analysis
	  • strengths, weaknesses, opportunities and threats (SWOT) analysis
	  • World Economic Forum 'The Global Risks Report'
	• Risk assessment techniques:
	  • qualitative risk assessment
	  • quantitative risk assessment
	  • hybrid approaches:
	  - stress testing
	  - scenario analysis
	• Risk registers and risk and control self-assessments:
	  • the risk register
	  • risk and control self-assessments
	• Risk reporting:
	  • red, amber, green (RAG) reporting
	  • risk reporting tools:
	  - heat maps
	  - risk event and near miss databases
	  - risk, control and performance indicators
	  - risk dashboards and balanced scorecards
	  - narrative reporting
	  • designing and implementing risk reports:
	  - audience
	  - size and level of detail
	  - level of statistical complexity
	  - frequency

Topic area	Learning areas

Risk culture, appetite and tolerance	• Risk appetite as a mechanism for balancing risk and return:
	  • defining risk appetite
	  • the role of risk appetite
	• Risk tolerance and risk capacity
	• Expressing risk appetite:
	  • metric-based expressions of risk appetite:
	  - probability and impact boundaries
	  - targets, limits and thresholds
	  • non-metric expressions of risk appetite:
	  - values
	  - risk management principles
	  - risk appetite statement
	• Determining risk appetite:
	  • factors to consider when determining appetite
	  • the role of the board
	  • the role of the chief risk officer and risk function
	• Good practice guidance on implementing risk appetite:
	  • Chief Risk Officers Forum
	  • Institute of Risk Management
	  • COSO risk appetite thought leadership paper
	• Defining culture and risk culture:
	  • defining organisational culture
	  • defining risk culture
	  • risk sub-cultures
	  • the consequences of risk culture 'failures'
	• Assessing, monitoring and controlling risk culture:
	  • risk culture surveys and metrics
	  • controlling risk culture
	  • practical guidance on assessing, monitoring and controlling risk culture

Compliance management	• Linking compliance and risk management:
	  • risk management rules and regulations
	  • managing compliance risk
	• Roles and responsibilities for compliance management:
	  • board of directors
	  • audit committee
	  • company secretary/governance professional
	  • compliance function
	  • risk management function
	  • internal audit function

Topic area	Learning areas
Compliance management (*cont.*)	• other specialist functions • line managers across the organisation • staff members • Risk-based compliance monitoring • Compliance management tools: • compliance policies and procedures • compliance codes of conduct • compliance reviews and audits • compliance impact analysis • gap analysis and action planning • compliance reporting • HR related controls • whistleblowing policies and procedures • establishing an appropriate culture

Section C: Risk and the business environment ***25% – 50 learning hours*** LO.4: Critically examine the impact of the business environment on risk with regard to legislation, policy and industry changes LO.5: Critically evaluate the impact of organisational conduct, behaviours and culture on risk management practices	
Topic area	**Learning areas**

Risk control strategies	• Reasons for risk control:
	  • managing probability and impact
	  • using controls for loss events to help seize opportunities
	• The five Ts of risk control:
	  • tolerate
	  • treat
	  • transfer
	  • terminate
	  • take the opportunity
	• Risk treatment techniques:
	  • PCDD hazard risk typology: preventive, corrective, directive, detective
	  • other categories of risk treatment techniques:
	  - formal controls
	  - informal controls
	• Common risk treatment controls
	• Risk financing:
	  • retained risk financing
	  • insurance risk transfer
	  • non-conventional risk transfer for the financial effects of risk
	• Controlling major loss events:
	  • crisis management
	  • business continuity planning
	• Controlling third party risks

Risk management in practice	• Common applications of risk management practice:
	  • an overview of applications
	  • operations or operational risk management
	  • cyber risk management
	  • project risk management
	  • supply chain risk management
	• Risk management, corporate social responsibility and sustainability
	• Regulatory reporting:
	  • regulatory reporting processes
	  • roles and responsibilities for regulatory reporting:

Topic area	Learning areas
Risk management in practice (*cont.*)	- company secretary and other governance professionals - compliance function - finance function - health and safety function - information technology function - risk function - other business functions • CG reporting and ESG reporting in Hong Kong
Trends and future developments for risk management	• Crime: • offences against an individual • offences against property or services • violation of laws • other offences • countering the workplace crime • cybercrime prevention • Financial crime: • the impact of financial crime on organisations • anti-money laundering • countering the financing of terrorism • common AML and CFT controls • reporting a suspicious transaction or activity • Bribery and corruption: • Prevention of Bribery Ordinance Cap 201 • key principles of internal control mechanisms • Political risk, including sanctions • Corporate gifts • People risk: • behavioural risk • common sources of behavioural risks: - bullying - negligence - information leaks - criminal activity - effects of behavioural risk • managing behavioural risk: - recruitment controls - codes of conduct - risk culture • Climate change risk • Asymmetric risk • Reputation and resilience

Topic area	Learning areas
Trends and future developments for risk management (*cont.*)	• The changing balance between tangible and intangible risks • Shareholder activism: • role of the board

More trends and future developments for risk management	• Complex and connected risks:
	  • the modern world and the growth in emerging risks
	  - complexity
	  - interconnectedness
	  - globalisation
	• Managing emerging risks:
	  • board level strategic environment emerging risk assessments
	  • scenario planning and reverse stress testing
	  • current examples of emerging risk:
	  - the networked economy
	  - social media and digital natives
	  - disruptive technologies
	  - global pandemics (COVID-19)
	• Changing knowledge and skills:
	  • in-demand skills
	  • talent sourcing
	  • talent management
	  • talent training
	  • talent risk management framework
	  • the workforce of the future
	  • the role of the board
	• Digital transformation:
	  • big data
	  • automated decision making:
	  - algorithmic decision making
	  - artificial intelligence
	  - advantages and disadvantages
	  - governance and compliance implications
	  • other new technologies
	  • managing risks in a digital world
	  • digital risks
	  • the role of the board

- End -

The Hong Kong Chartered Governance Institute 香港公司治理公會
(Incorporated in Hong Kong with limited liability by guarantee)

Hong Kong Office
3/F, Hong Kong Diamond Exchange Building,
8 Duddell Street, Central, Hong Kong
T: (852) 2881 6177 F: (852) 2881 5050
W: hkcgi.org.hk E: student@hkcgi.org.hk

Better Governance. Better Future.
卓越治理 更佳未來