MAICSA Syllabus Document – Module 5

Risk Management

January 2020

Introduction

The content for this module is an expanded version of the content specified in the *International Qualifying Scheme (IQS)* module entitled *Risk and Compliance.* **All** (100%) of the content specified in the IQS syllabus is covered in this module. The name of the module has been changed to *Risk Management* to more accurately describe the content within the module.

Module 5

Risk Management

Level: **7**

Module type: **Mandatory – Part Two (Level 7) 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.

Before studying this module
Students must have completed all Level 6 modules in the programme before attempting this module.

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 ***35% – 70 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*	
Topic area	**Potential content**
An overview of the global risk management and associated regulatory environment	The importance of risk management and associated compliance frameworks: adding value to organisations: − a shareholder perspective − a wider stakeholder perspective − managing conflicts of interest between stakeholders regarding their risk exposures self-regulation – reasons why organisations cannot achieve effective risk management arrangements on their own reasons for risk management regulation: − market failures − using regulation to address market failures − weighing up the benefits and costs of risk management regulation − the role of compliance management in relation to risk management regulation The development and philosophy of the national and international regulatory environment for risk management: the importance of both a national and a global perspective types of regulation that make up the regulatory environment for risk management (e.g. health and safety, governance, environmental) components of the risk management regulatory environment: − types of regulation, including health and safety, governance, environmental − rules and guidance (including standards) − principles-based versus outcomes-based regulation – differences, advantages and disadvantages − risk-based regulation –the level of regulation and the intensity of supervision is related to the types and levels of risk to which an organisation is exposed, e.g. the prudential regulation of banks and insurance companies

Topic area	Potential content
	International risk management regulations and standards, including: ISO 31000:2009, Risk management – Principles and Guidelines COSO Enterprise Risk Management Framework (2004) ISO 19600:2014, Compliance Management Systems – Guidelines how G20/OECD Principles of Corporate Governance relate to risk and compliance management risk management in banks – The Basel III Accord
Regulatory frameworks	Risk management requirements within corporate governance regulations, including: the UK Corporate Governance Code Irish Companies Act 2014 and the Irish system of corporate governance European Union corporate governance rules OECD Principles of Corporate Governance the work of the World Bank Corporate Governance Group corporate governance codes in other countries, e.g. Russia, Nigeria, Kenya, Dubai
The mandate, authority and scope of different regulators in different industries	UK and Ireland – the role of the European Union Risk management regulation within financial services: UK regulatory agencies, including: − Prudential Conduct Authority − Financial Conduct Authority Irish regulatory agencies, including: − Irish Central Bank − European Central Bank other agencies, e.g. Financial Services Commissions in Jersey, Guernsey and Jamaica, Dubai Financial Services Authority, Central Banks in Africa and Russia Health and safety regulation: UK regulatory agencies, including: − UK Health and Safety Executive − Guernsey Health and Safety Executive − Jersey Health and Safety Inspectorate Irish regulatory agencies, including the Health and Safety Authority other government agencies, for example: Ministry of Labour and Social Security of the Russian Federation

Topic area	Potential content
	Kenyan Directorate of Occupational Safety and Health Services Nigerian National Council of Occupational Safety Environment, Health and Safety (EHS) in Dubai Environmental risk management regulation: UK regulatory agencies, including: − UK Environment Agency − Jersey and Guernsey Departments of the Environment Irish regulatory agencies, including the Irish Environment Protection Agency other policies and agencies, for example: − Russian environmental policy − Nigerian National Environmental Standards and Regulations Enforcement agency − Kenyan National Environmental Management Authority − Dubai Environment Department
Risk management frameworks and introduction to risk management standards	Reasons why risk management standards are needed Key aspects of ISO3100 (2009): International Standard for Risk Management National standards and good practice guides for risk management, including: The Orange Book: Management of Risk – Principles and Concepts A Risk Management Standard – Institute of Risk Management Enterprise Risk Management – Integrated Framework – The Committee of Sponsoring Organizations' of the Treadway Commission (COSO) BS 31100 (BS31100) – The British Code of Practice for Risk Management & Guidance for ISO31000 COBIT Framework for IT Governance and Control –IT Governance Institute and the Information Systems Audit and Control Association (ISACA) National Guidance on Implementing I.S. ISO 31000:2009 Risk Management Principles and Guidelines – National Standards Agency of Ireland

Topic area	Potential content
Key risk management concepts	Defining risk: distinguishing between risk and uncertainty risk events, probability, impact and exposure inherent and residual risk exposure – reasons why both are needed perceptions of risk: − reasons why risk isn't always bad − pure versus speculative risk Categorising risk: common typology, including: − business risk − credit risk − liquidity risk − market risk − operational risk, including conduct and compliance risks alternative typology: − strategic risks − external risks − internal control risks benefits and limitations of organisations using the same typology A brief history of risk management during the 20th and 21st centuries The role of risk management in organisations: to reduce uncertainty to anticipate and hopefully prevent future risk events using risk management to support internal control: − risk and compliance management − risk and internal audit: a spotlight on risk based internal auditing − the consequences of weak internal control risk management, e.g. the Volkswagen emissions scandal − the role of the external auditor risk and strategy setting and implementation – using risk management to support effective strategic risk taking perspectives on risk management: − using risk management to help anticipate risk events − the link between risk management and ensuring resilience in the event of large scale loss and business disruption

Topic area	Potential content
	risk management as a tool for both value protection (e.g. protecting the value of shareholder equity and protecting reputation) and creating value in organisations
Risk management processes, perspectives and responsibilities	The standard risk management process: risk identification risk assessment risk monitoring risk control Extending the standard process – the characteristics of enterprise risk management: holistic – managing all risk types from across the enterprise value added – a strategic-level focus blending the formal (e.g. procedural) and informal (e.g. cultural) aspects of risk management techniques for identifying, assessing, monitoring and controlling risk within an ERM framework the benefits of ERM The elements of an effective risk management framework: designing and implementing an effective risk management policy risk reports to support management decision making drafting a risk appetite statement the role of the risk (or risk and audit) committee escalation and whistleblowing procedures business continuity management processes and plans The roles/functions and responsibilities that are involved in risk management: the board of directors and executive management risk committees the rise of the Chief Risk Officer the role of the risk function and the risk manager the role of the compliance function and compliance manager internal audit and risk management other important functions, including information security, human resources, health and safety, operations, finance and marketing and public relations (PR) the role of the company secretary/governance professional in risk management

Topic area	Potential content
Risk management-related compliance frameworks and governance structures – leading international practice with regard to governance, risk and compliance	The role of governance and compliance from a risk management perspective The components of an effective risk management compliance framework: establishing compliance standards developing compliance processes and controls to include: − escalation processes − documented policies and procedures − training and communication the link between internal control and compliance risk-based compliance key roles and responsibilities, including the role of the audit or audit and risk committee and the company secretary/governance professional Governance structures from a risk management perspective: managing risk within a group structure: − multiple legal entity versus an integrated (single legal entity) structure − advantages and disadvantages the three lines of defence approach to the governance of risk and compliance: − the appropriateness of the three lines of defence approach − the potential advantages and disadvantages of the three lines approach − how disadvantages can be mitigated the five lines of assurance as an alternative to the three lines approach the role of the board in relation to risk management ISO 19600:2014 Compliance management systems – Guidelines The emergence of governance risk and compliance (GRC) frameworks the benefits of integrating governance, risk management and compliance activities into a single management framework the core scope of a GRC framework: − financial GRC − information technology GRC − legal GRC integrated GRC information management and reporting systems – the advantages and disadvantages of implementing a comprehensive GRC solution from a third party vendor

Section B: Managing risk and compliance ***40% – 80 Learning hours*** *LO.2: Be able to critically evaluate approaches to risk management* *LO.3: Be able to critically evaluate the management of risk and provide professionally appropriate advice to those responsible for governance*	
Topic area	**Potential content**
Risk identification, assessment, analysis and evaluation and risk reporting	Techniques for identifying risk events, including: checklists, surveys and interviews expert judgement focus groups the Structured What-if Technique (SWIFT) the Delphi technique root cause analysis systems and process mapping and analysis incident analysis (of loss events and near misses) Identifying emerging risks: Political, Economic, Social and Technical (PEST) analysis Strengths, Weaknesses, Opportunities and Threat (SWOT) analysis the annual World Economic Forum Global Risks Report Techniques for assessing risk events: qualitative risk assessment using risk matrices quantitative risk assessment tools: focus on Value at Risk analysis hybrid approaches: − stress testing − scenario analysis, including using bow tie analysis to assess the causes and effects of risk events Recording risk event information on risk registers: the typical components of a risk register using risk registers to support risk monitoring and risk control key pitfalls to avoid when using risk registers Risk and control self-assessment Risk reporting: the concept of Red, Amber, Green (RAG) reporting risk reporting tools: − heat maps and reporting significant risks − loss and near miss databases − key risk indicators − key control indicators

Topic area	Potential content
	− key performance indicators − risk dashboards − narrative reporting designing and implementing risk reports: key decisions to make, including: − who to report to and why − appropriate report size and format − frequency of reporting the benefits of using risk reports to aid action planning and management decision making
Risk culture, appetite and tolerance	Balancing risk and return – understanding the concept of risk appetite: defining risk appetite the role of risk appetite Other key terms – risk tolerance and risk capacity Expressing risk appetite: probability and impact boundaries targets, limits and thresholds qualitative statements Factors to consider when determining an organisation's appetite for risk: strategic aims and objectives balance sheet strength stakeholder risk aversion the external economic environment The role of the board in setting and governing an organisation's risk appetite Risk appetite information in annual reports – what should be considered for inclusion Good practice guidance on implementing an effective risk appetite framework, for example: The Chief Risk Officers Forum – Establishing and Embedding Risk Appetite: A Practitioners View Risk Appetite Research Report – Association of Insurers and Risk Managers in Industry and Commerce (AIRMIC) Risk Appetite and Tolerance – Institute of Risk Management Defining culture and risk culture, including: the concept of risk culture as a subset of an organisation's broader culture risk culture as an indicator of how an organisation takes risk in addition to how it controls it

Topic area	Potential content
	Risk sub-cultures: why they exist determining if risk sub-cultures are a help or a hindrance The consequences of risk culture failure, e.g. the Barclays LIBOR scandal Using risk culture surveys and risk culture metrics to assess and monitor organisational risk culture Changing an organisation's risk culture – the levers of risk culture control: belief systems boundary systems diagnostic control systems interactive control systems Guidance on monitoring and managing risk culture in organisations, for example: Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture – the Financial Stability Board (2014) Guidance on Risk Management, Internal Control and Related Financial and Business Reporting –the Financial Reporting Council (2014) Safety Culture Maturity Model – the UK Health and Safety Executive (2000) Risk Culture: Under the Microscope Guidance for Boards – Institute of Risk Management (2012)
Compliance management methodologies, tools and techniques	Integrating compliance management within risk management and enterprise risk management in particular Roles and responsibilities of compliance stakeholders in organisations, including: the compliance function the risk function the audit function the company secretary/governance professional board of directors business management Risk based compliance – directing resources to the largest compliance risks Common techniques for managing compliance risk, including: compliance risk assessments, including: − impact analysis, e.g. financial, reputation, legal and business − compliance audits

Topic area	Potential content
	gap analysis and performance improvement plans compliance reporting codes of conduct establishing an appropriate compliance culture

Section C: The impact of the business environment on organisational risk management ***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	**Potential content**
Responding to risk – risk control strategies	Introduction to risk control: reasons why organisations need to control risk risk control as more than just reducing risk The '4Ts' of risk control – Tolerate, Treat, Transfer, Terminate Risk treatment techniques: the PCDD hazard risk typology – preventive, corrective, directive, detective other risk treatment techniques: − formal (technical/procedural) versus informal (human oriented) controls − the link to risk culture and risk culture controls Common controls for business, credit, market and operational risks, including: automation capital and collateral data backup diversification firewalls insurance and financial hedging mandates and other limits of responsibility policies and procedures recovery plans (financial and physical) recruitment redundancy segregation of duties securitisation staff training and development other activities to encourage appropriate behaviours, including: − sensitivity training − methods of preventing unconscious bias when recruiting

Topic area	Potential content
	The role of risk financing and some common risk financing techniques: retained risk financing via the holding of financial reserves, e.g. capital and provisions risk financing via insurance risk transfer non-conventional risk financing tools: − captive insurance companies − hedging with derivatives − contingent capital Controlling major risk events – crisis management and business continuity planning (BCP) Controlling third party risks from suppliers and outsource service providers
Risk management in practice	Common applications of risk management practice in organisations corporate governance and compliance management internal control health and safety management environmental risk management cyber risk management 'operations' risk management strategic risk management project risk management supply chain risk management Linking risk management, corporate social responsibility and sustainability Regulatory reporting – implications for risk and compliance management developing reporting processes that ensure accurate reporting and provide assurance to boards and senior managers key roles and responsibilities for regulatory reporting, including the role of the company secretary/governance professional
Emerging trends and future developments in risk management	Risk and opportunity management – designing a risk management framework that facilitates the reduction of pure risk and the taking of speculative risks where there are clear business benefits Anti-money laundering (AML) and countering the financing of terrorism (CFT) legislation/practices: reasons why AML and CFT legislation are needed the application of AML and CFT regulation in and outside of the financial services sector

Topic area	Potential content
	key AML and CFT controls, including: − identity checking – customer due diligence (CDD) and know your customer (KYC) − financial activity monitoring − retaining financial transaction documentation reporting suspicious activity and appointing a nominated officer Complexity, change and emerging risks: risk management challenges in a modern world, including: − high levels of complexity − interconnected markets − globalisation the key characteristics of emerging risk, e.g. high levels of uncertainty and unpredictability assessing and controlling emerging risks current sources of emerging risk, including: − the networked economy − social media − digital natives − disruptive technology − reputation risk the role of the board in managing emerging risk strategies for managing emerging risk, including: − organisational resilience − promoting mindfulness − fostering a culture of creativity Behavioural risk management: common behavioural risk factors, including: − bullying − negligence − leaking sensitive information − criminal activities the implications of behavioural risk, including: − reputation effects − staff morale − legal/compliance issues managing behavioural risk, including: − recruitment − clear rules on behaviour − managing risk culture

Topic area	Potential content
	Information technology advances: the implications of 'big data' for risk management, including: − real time reporting − different styles of risk report − identification of emerging risks via social media activity decision making automation via algorithmic decision making and artificial intelligence, e.g. automated trading in banks governance and compliance implications of automated and artificial intelligence (AI) supported decision making, including: − European Union regulations – General Data Protection Regulation (GDPR) advantages, disadvantages and implications of replacing human decision making by automation, including: − speed − reliability − cost − system failures − ability to deal with complex decisions