Subject SP9

CMP Upgrade 2021/22

CMP Upgrade

This CMP Upgrade lists the changes to the Syllabus objectives, Core Reading and the ActEd material since last year that might realistically affect your chance of success in the exam. It is produced so that you can manually amend your 2021 CMP to make it suitable for study for the 2022 exams. It includes replacement pages and additional pages where appropriate.

Alternatively, you can buy a full set of up-to-date Course Notes / CMP at a significantly reduced price if you have previously bought the full-price Course Notes / CMP in this subject. Please see our 2022 *Student Brochure* for more details.

We only accept the current version of assignments for marking, *ie* those published for the sessions leading to the 2022 exams. If you wish to submit your script for marking but have only an old version, then you can order the current assignments free of charge if you have purchased the same assignments in the same subject in a previous year, and have purchased marking for the 2022 session.

This CMP Upgrade contains:

- all significant changes to the Syllabus objectives and Core Reading
- additional changes to the ActEd Course Notes and Assignments that will make them suitable for study for the 2022 exams.

0 Changes to the Syllabus

There are no changes to the syllabus objectives.

1 Changes to the Core Reading

This section contains all the ***non-trivial*** changes to the Core Reading.

Module 1

Section 0

A new introductory note to ERM has been added. Replacement pages are provided.

Module 12

Section 1

A new section has been added introducing the role of the Chief Risk Officer. Replacement pages are provided.

Module 13

Section 4

A new section has been added on climate change risk. Replacement pages are provided.

Module 15

Tasklist

The IAA Note, Section 5.3, has been added to the list of reading in Section 5 of the Tasklist.

Page 7

Climate risk has been added to the first paragraph of Other risk types. This paragraph now reads:

Environmental risk, climate risk, legal risk, regulatory risk, agency risk, reputational risk, moral hazard, political risk, project risk and strategic risk are affected similarly to operational risks.

Module 25

Section 4

A new section on assessing / modelling climate change risk has been added. Replacement pages are provided.

Module 30

Section 1

A new section introducing and defining capital has been added. Replacement pages are provided.

Section 4

At the start of this section, some new Core Reading introducing the idea of capital allocation has been added. Replacement pages are provided.

A new example (Section 4.4) exploring the capital allocation issues arising for a general insurance company has been added. Replacement pages are provided.

Module 32

Section 1

A new section introducing the case studies has been added. Replacement pages are provided.

New case studies on Boeing (Section 1.9) and Covid-19 (Section 1.10) have been added. Replacement pages are provided.

Module 33

The term 'risk matrix' has been replaced with 'risk map.'

The definitions of concentration of risk, cyber risk and Value at Risk have been amended to:

Concentration of risk

Concentration of risk can be described as 'putting all your eggs in one basket'; that is, relying upon the success of one course of action which, if it fails, leaves no alternative. Concentration of risk may be the result of not being able to diversify (and therefore reduce) risk.

Cyber risk

Cyber risk is defined by the Institute of Risk Management as, 'any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems'. Typically, cyber risk occurs where there is online activity and/or the storage of personal data, such as due to security breaches or targeted attacks.

Value at Risk (VaR)

VaR is a simple measure of risk, representing the maximum potential loss on a portfolio over a given future period with a given degree of confidence.

2 Changes to the ActEd material

This section contains all the ***non-trivial*** changes to the ActEd text.

Module 4

Summary pages

The summary pages have been updated. Replacement pages are provided.

Module 5

Pages 15 and 16

The material comparing Basel II with Solvency II, and on Sarbanes Oxley has been updated. Replacement pages are provided.

Module 11

Summary pages

The summary pages have been updated. Replacement pages are provided.

Module 12

Summary pages

The summary pages have been updated. Replacement pages are provided.

Module 13

Summary pages and Practice questions

The summary pages have been updated to include material on cyber and climate change risk, and a new practice question has been added. Replacement pages are provided.

Module 20

Page 16 and Summary pages

The section on Threshold Exceedances has been modified. Replacement pages are provided.

Module 22

Practice questions

A new practice question (22.3) has been added. Replacement pages are provided.

Module 24

Practice questions

A new practice question (24.5) has been added. Replacement pages are provided.

Module 25

Summary pages and Practice questions

A new section on assessing climate change risk has been added to the summary pages, and a practice question (25.3) has been added. Replacement pages are provided.

Module 26

Section 3.2 and Summary pages

New sections on liquidity risk and regulatory / operational constraints and governance issues have been added, and the summary pages updated. Replacement pages are provided.

Module 27

Section 2

A new section (Section 2.8) on the number of contracts required for a hedge has been added. Replacement pages are provided.

Module 29

Section 3

The section on underwriting has been expanded. Replacement pages are provided.

Module 30

Section 2.4

A new example on how the SCR is calculated has been added. Replacement pages are provided.

Module 32

Section 1

The case studies (in Section 1.11) on Confederation Life and Orange County have been removed from the module, to make way for the new case studies on Boeing and Covid-19.

Module 34

Various links have been updated, and reference material on climate change risk added. Replacement pages are provided.

3 Changes to the X Assignments

Overall

The X Assignments have been changed significantly to reflect the online nature of the exams. We have not detailed all of the changes in this upgrade.

If you would like the new assignments *without* marking, then retakers can purchase an updated CMP or standalone X Assignments at a significantly reduced price. Further information on retaker discounts can be found at:

www.acted.co.uk/paper_reduced_prices.html

If you wish to submit your scripts for marking but have only an old version, then you can order the current assignments free of charge if you have purchased the same assignments in the same subject in a previous year, and have purchased marking for the 2022 session. We only accept the current version of assignments for marking, *ie* those published for the sessions leading to the 2022 exams.

4 Other tuition services

In addition to the CMP you might find the following services helpful with your study.

4.1 Study material

We also offer the following study material in Subject SP9:

- Flashcards
- ASET (ActEd Solutions with Exam Technique) and Mini-ASET
- Mock Exam and AMP (Additional Mock Pack).

For further details on ActEd's study materials, please refer to the 2022 *Student Brochure*, which is available from the ActEd website at **www.ActEd.co.uk**.

4.2 Tutorials

We offer the following (face-to-face and/or online) tutorials in Subject SP9:

- a set of Regular Tutorials (lasting a total of three days)
- a Block Tutorial (lasting three full days).

For further details on ActEd's tutorials, please refer to our latest *Tuition Bulletin*, which is available from the ActEd website at **www.ActEd.co.uk**.

4.3 Marking

You can have your attempts at any of our assignments or mock exams marked by ActEd. When marking your scripts, we aim to provide specific advice to improve your chances of success in the exam and to return your scripts as quickly as possible.

For further details on ActEd's marking services, please refer to the 2022 *Student Brochure*, which is available from the ActEd website at **www.ActEd.co.uk**.

4.4 Feedback on the study material

ActEd is always pleased to receive feedback from students about any aspect of our study programmes. Please let us know if you have any specific comments (*eg* about certain sections of the notes or particular questions) or general suggestions about how we can improve the study material. We will incorporate as many of your suggestions as we can when we update the course material each year.

If you have any comments on this course, please send them by email to **SP9@bpp.com**.

1

What is ERM?

Syllabus objectives

1.2 Describe the concept of ERM.

1.2.1 Define what is meant by ERM.

1.2.2 Describe the role of the following concepts in ERM:

- the holistic approach
- downside and upside risks
- measurement of risk
- unquantifiable risks
- responses to risk, and risk management.

0 ERM – an introductory note

The early modules of the SP9 course introduce the key concepts underlying ERM and discuss good practice in terms of framework, governance and culture. Students will be expected to be able to evaluate the quality of these aspects within a hypothetical organisation, and to recommend an appropriate framework or improvements given specific circumstances.

In one paragraph that is in fact the aim of the whole SP9 course – to introduce students to the concepts that they will be able to apply as members of a risk management function in a real-world enterprise. The fundamental philosophy of Enterprise Risk Management, and of this course, is that managing the risk of an entire organisation together is superior to individual risk management of individual areas.

This is often referred to as the 'holistic' approach, and is explored further later in this module.

This course is not intended to provide the definitive recipe for risk management, as there is no such thing. There are good practices, which are common in risk management functions, but every implementation of a risk management function is different, because every organisation is different.

This course is built around two textbooks, and so naturally presents the subject with two different biases. As students study the content in those two textbooks they will find it helpful to consider how the two authors present similar information in a different way, and evaluate how those two different presentations could best be used in any specific organisation.

The two textbooks referred to are *Financial Enterprise Risk Management* by Paul Sweeting, 2nd Edition and *Enterprise Risk Management: From Incentives to Controls* by James Lam, 2nd Edition. Each module in this course contains a 'Task list' setting out sections of the two textbooks to read, to help with drawing out the comparison. Alternatively, you may prefer to read each textbook, in turn, in its entirety. There is no right or wrong way but it is worth appreciating now that there is a lot of reading to be done for Subject SP9, which will require a significant time commitment.

Individuals need to have an understanding of an organisation, both from the risk and commercial side before applying the material in this course to that organisation. A lack of appreciation for the wider context (or perhaps even worse, a belief by the individual that they *do* have this appreciation when in fact they do not) will likely sabotage any attempts to improve risk efficiency in an organisation.

With that warning in mind, students may perhaps be asking how successful any attempt to teach Enterprise Risk Management can be. After all, if the design and implementation of an ERM framework has to be organisation-specific, how can it be encapsulated in an examinable subject?

The first thing to acknowledge is that the student who passes this subject will not be able to arrive at an organisation and implement the ideas they have studied without significant negotiation with their colleagues on the Board and Executive and without significant prior analysis of the organisation. Individuals need to behave professionally, recognising that other people may have different views to their own and that these people may be correct. Much of the material presented in this course is subjective, and the consensus as to what is best practice may change over time.

In practice, what is actually implementable may differ from the theoretically perfect – which is perfectly acceptable as long as it serves the ultimate goal of enabling the organisation to understand and manage its risks as well as possible.

At the time of publication of these Course Notes, if you are successful in passing the Subject SP9 exam, you will be invited to attend a CERA seminar. This seminar very much focuses on the practical implementation of the concepts and the presentation to the Board and other colleagues.

This course also cannot be comprehensive – within the constraints of one IFoA subject, it is impossible to cover every risk management technique that someone working in a risk department will use. For instance, the main risk to an occupational pension fund may well be covenant – the ongoing financial strength of the sponsor which provides part of the future funding. That potential concentration of credit risk is an inherent part of the design of the scheme and has to be analysed in a very different way than the credit risks of a whole portfolio of investments, which allow for diversification.

To take another example, a general insurer will need to find appropriate techniques to model insurance risk – which is typically the main risk for that kind of organisation. The specific details of those techniques is outside the scope of the syllabus.

Nevertheless, all of the content of this course is used day-to-day by thousands of risk departments around the world. Risk departments make regular decisions, based on the context of their organisation and how mature it is in its management of risk, as to what tools and techniques to adopt.

We also hope that you find this course enjoyable, and that it gives you an understanding and appreciation of these tools and techniques, some of which are quantitative (and will stretch your mathematical knowledge), others qualitative (challenging your ability to analyse and synthesise).

Just going through the motions of implementing ERM, without truly embracing its ethos, can increase the bureaucracy of an organisation and could even damage it. It could also be expensive – risk management measures are not cost-free.

Risk management needs to complement an organisation's commercial competitive advantage. The consequences of any additional workload added to the commercial side of the business must be considered, including doing so in the most efficient way.

A Glossary of terms is provided in Module 33. You may wish to refer to this occasionally as you encounter new concepts and terminology during your study of Subject SP9.

This page is deliberately left blank
so that you can easily remove and use the task list.

Module 4 Summary – Internal risk frameworks

Components of an ERM framework

An ERM framework should be *proportional* to the size, nature and complexity of the company. Successful implementation will be dependent upon there being a positive risk culture. The table below sets out the key components of an ERM framework together with associated concepts (many of which are developed in later modules).

Component	*Purpose*	*Associated concepts*
Corporate governance	to establish organisational processes and controls	• risk appetite, tolerance, capacity • risk limits / exception management • risk policies • roles and responsibilities • board structure (*eg* independence, NEDs, subcommittees) • risk culture • remuneration • resources / training / competency • third line of defence
Line management	to integrate risk management into business processes	• risk identification and management • pricing, product development • first line of defence
Portfolio management	to aggregate risk exposures, identifying diversification effects and risk concentrations	• holistic (all risks, all sources, upside and downside, consistency) • interdependencies (diversification, hedging, concentration of risk) • consistent risk taxonomy / register • second line of defence
Risk transfer	to pass on excessive risk cost-effectively	• alternative risk responses (reduce, remove, retain)
Risk analytics	to measure, analyse and report on risk	• consistent assessment / reporting • risk metrics and models • stress and scenario testing • reporting (frequency, content, KRIs)
Data and technology resources	to support the analytics and reporting	• credibility and relevance of data • in-house *vs* external expertise
Stakeholder management	to communicate and report on risk	• regulator • credit rating agencies • disclosure / market discipline

Risk culture

A company's risk culture is its shared values, beliefs and behaviours in relation to risk. In a *good* risk culture, employees do the right things, even if there is no specific rule or policy telling them what to do, rather than acting in their own interests. Culture is influenced from the top of the company by the behaviour of the Board and senior management.

A good risk culture will support the goals, activities and desired outcomes of a company by encouraging:

- consultation / participation
- communication / openness / sharing
- accountability (not blame)
- organisational learning (not box ticking).

Corporate governance

Corporate governance is the system whereby Boards of directors, or governing bodies, are responsible for the governance of their organisations upon appointment by shareholders.

It is concerned with improving the performance and conformance of companies for the benefit of shareholders, policyholders, other stakeholders and the wider economy.

Codes of Best Practice for corporate governance exist in some countries, *eg* The UK Corporate Governance Code, The Dey Report in Canada. Adherence with these codes is typically voluntary with a requirement to disclose compliance or non-compliance (in which case to explain why).

Common themes in best-practice corporate governance include:

- communication with stakeholders (disclosure and transparency)
- the independence of the Board (separate Chair and CEO, subcommittees for audit, remuneration and appointments comprising non-executive directors only)
- Board performance (regular and formal appraisal of individual directors, subcommittees and the full Board, training and development for new members)
- Board remuneration (commensurate with responsibilities, alignment with shareholder interests and the medium- to long-term objectives of the company)
- Board appointments (competencies, diversity, regular review).

Additionally / alternatively, there may be *statutory* requirements in relation to corporate governance, *eg* Sarbanes-Oxley and Dodd-Frank Act in the US.

Key stakeholders and their roles in corporate governance and ERM

The table below summarises the roles of the key stakeholders discussed in this module in relation to corporate governance and ERM, to help with differentiating between them.

Stakeholder	*Roles*
Board of directors	• governing company as a whole • responsible for risk management failures • ensuring effective ERM in place (oversight / stewardship) • setting risk appetite and approving risk policies • monitoring key risks • ensuring the implementation of an ERM framework • ensuring compliance with supervisory requirements • establishing / maintaining a supportive risk culture • setting organisational structure, roles and responsibilities • ensuring fit and proper risk personnel • reviewing lessons learnt • aligning remuneration with medium to long-term objectives
Risk subcommittee	• oversight of ERM on behalf of Board • setting risk policies • gathering information on key risks • assessing treatment of key risks by the RMF • ensuring the implementation of an ERM framework • reporting on risk, achievement of ERM objectives and compliance with supervisory requirements to the Board
Audit subcommittee	• monitoring integrity of financial statements • reviewing and monitoring internal assurance functions such as financial control, risk management and internal audit • recommending, monitoring, reviewing external auditor
Chief Risk Officer (CRO)	• providing overall leadership and direction for ERM • overseeing the development / implementation / maintenance of an ERM framework • reporting on risk to the Board and other stakeholders • managing the RMF (*see also Module 12*)
Line managers	• day-to-day managing of / reporting on risk • implementation of risk policies
All employees	• identifying new / increased risks • contributing ideas for opportunities • making suggestions for mitigating risks • identifying defective procedures and exceptions

The practice questions start on the next page so that you can keep the module summaries together for revision purposes.

3.2 Basel II *vs* Solvency II

There are many similarities between the two regulatory frameworks:

- They both describe requirements in three pillars, and each pillar deals with similar aspects of the company's risk (minimum capital requirements, supervisory review and disclosure).
- Under Pillar 1, both regimes adopt a risk-based approach to calculating the minimum capital requirement, and both consider credit, market and operational risk.

  An organisation can adopt the regulator's standard model (or formulae) or use an internal model (subject to regulatory approval) to calculate the minimum capital requirement.

  Available capital is 'tiered' to indicate its quality, with only the higher-quality tiers being recognised when assessing whether the minimum capital requirement is met.
- Under Pillar 2, both regimes require organisations to assess their *own* processes for identifying risks, managing risks and monitoring capital adequacy.

  The regulator has different levels of supervisory intervention dependent on the risk of available capital falling below the minimum requirement.
- Under Pillar 3, both regimes require organisations to publish details of their risks, risk management and capital adequacy.

  Providers of capital can assess this information to determine an appropriate cost of providing capital, hence imposing market discipline on organisations.
- Both frameworks are designed to be suitable for multi-national firms.
- Both regimes are 'mandatory' (Basel II is mandatory if the recommendations are adopted by the regulator of an individual country).

Question

Outline the key differences between these two regulatory frameworks.

Solution

- Basel II is based on the concept that the market participants are dependent on one another and that there is significant contagion risk in the banking sector. However, the Solvency II framework is not designed with systemic risk in mind as it is considered unlikely that the demise of one insurer will affect others.
- Overall, Basel II takes a more prescriptive approach than Solvency II, which is more principles based, leaving the details to the regulators in individual countries.
- Under Pillar 1, Solvency II requires the assessment of both a minimum capital requirement (MCR) and a solvency capital requirement (SCR). The SCR requires an insurance company to hold enough capital to cover adverse events, calibrated with a 99.5% probability over a one-year time horizon. Solvency II also requires the assessment of underwriting risk.

4 Sarbanes-Oxley

4.1 Sarbanes-Oxley Act

The Sarbanes-Oxley Act of 2002 has already been mentioned in Module 4, under consideration of corporate governance.

The 2002 'Sarb-Ox' or 'SOX' legislation resulted primarily from the (sudden) collapse of Enron and WorldCom, after which serious failings in the accounting reports from these companies were uncovered. The aim of the legislation is to improve the reliability of corporate disclosures in order to protect shareholders. It is primary legislation in the US, rather than a voluntary code as in the UK.

Some key features are:

- the formation of a Public Company Accounting Oversight Board (PCAOB) to inspect the published accounts of quoted firms and to prosecute any accountancy firm deemed to be in breach of the regulations
- increased accountability of CEOs and CFOs of public companies, whereby they are both personally required to certify that the financial reports do not contain any untrue statements of material facts, and are personally responsible for these financial disclosures
- that each published report must contain an *internal control report* (ICR), which commits management to maintain proper internal controls and review their effectiveness
- the CEO and CFO are legally responsible for setting up, maintaining and evaluating internal controls , and reporting any issues to the external auditors
- requirement for there to be an audit committee staffed by independent directors, and at least one 'financial expert'
- banning the provision of audit and non-audit services by the same external firm to ensure auditor independence
- limiting the length of appointment of the external auditor within a firm to five years
- making it illegal for directors to interfere with the audit process
- making it illegal for any employee to alter, conceal, falsify or destroy records or documents with intent to impede or influence an investigation
- a strengthening of the separation of analyst and investment bankers.

Key themes for management to consider as part of their governance, risk and compliance (GRC) systems include:

- Are controls identified and documented?
- Are controls consistent across the business?
- Do controls address the critical factors – *ie* are the right controls in place?
- Do the controls include risk management?
- What testing procedures are required before signing off the ICR?

Module 11 Summary – Stakeholders

Categories of stakeholder

Stakeholder objectives and the nature of the relationship between a stakeholder and an organisation have an influence on:

- the organisation's risk appetite
- the risks that might arise because of the relationship.

One categorisation of stakeholders that attempts to classify the different objectives / relationships is as follows:

- principals: contribute capital, or receive capital from a company
- agency: paid by principals to perform a role on their behalf
- controlling: supervise principals and agents
- advisory: advise principals and agents
- incidental: affected by behaviour of principals and agents.

The table overleaf outlines key stakeholders from these categories and their perspectives.

Stakeholder management

A key component of stakeholder management is transparency in the communication of key risk management information and recognition of different communication needs.

Conflicts between stakeholders

The separation of ownership and management means owners (shareholders) do not need to get involved in day-to-day management and can benefits from managers' expertise.

Agency risk arises when the interests of the agents (*eg* managers, employees) are misaligned with those of the principals (*eg* shareholders). This is often due to poor remuneration structures that fail to align such interests in an appropriate way.

Other conflicts arise due to:

- different objectives of debtholders and equity holders
- dominance of the CEO and employees who try to win favour
- managers / employees wanting to protect job security by making low-risk decisions
- regulators whose remuneration / prospects are enhanced by financial crises (and hence the need for greater regulation)

Agency costs include the costs of mitigating agency risk, *eg* monitoring the actions of others and seeking to influence them.

Key stakeholders and perspectives

Stakeholder	*Perspectives*
Shareholders	• seek good risk-adjusted returns • want to protect against a collapse of the share price • seek value creation through risk taking • have diverse time horizons and limited power individually
Customers / policyholders	• seek good value for money and security of company • individually weak, collectively stronger • customer management: acquisition and retention, loyalty and satisfaction, knowing the customer, handling crises
Directors	• duty of care to understand business and provide challenge • ensure compliance with regulation • conflict of interest with personal goals, *eg* remuneration
Employees	• seek continued profitability and security of company to safeguard benefits and job security • employee management: recruiting and screening, training and development, retention and promotion, firing and resignation
Regulators	• seek to ensure compliance, protect stability of markets • balance between consumer protection / efficiency of markets • balance between timely interventions / market self-correction
Government	• set regulation • take actions, *eg* lender of last resort, nationalisation • seek tax revenues, re-election, prevention of contagion
External auditors	• perform annual review of accounts and risks • duty to report honestly and openly on state of company
Credit rating agencies	• assess creditworthiness of companies, which affects the ability of such companies to raise capital • conflict of interest as paid by companies being rated, but tempered by desire of rating agencies to maintain reputation
Creditors	• seek security of repayment of interest / capital
Subcontractors / suppliers	• affected by company failure via loss of future income and counterparty default risk
Pension scheme trustees / members	• seek security of the pension scheme, which depends on covenant of sponsoring company
General public	• may be many of the above stakeholders, also taxpayers • influenced by rapid dissemination of news via media
Shareholder service providers	• act on behalf of shareholders to express views, proxy vote • conflict of interest as provide other services to companies
Business partners	• seek success of strategic alliances

1 The Chief Risk Officer

1.1 The view from the CRO's seat

This section aims to give students a little more context by considering the role of the CRO (the Chief Risk Officer) before the course dives into the details of ERM. The author of this section has been CRO in two very different UK financial institutions – one the UK general insurance subsidiary of a major global financial services group and one a not-for-profit government-linked organisation with similarities to life assurance companies and pension funds. The section has been reviewed by other members of the IFoA's CRO group to ensure that the inevitable resulting bias does not dominate.

The role of the CRO, focussing on oversight and design of all risk management activity in one executive seat, is a new one, dating back only to the 1990s, first emerging in financial services. However, it is one that has shown its value in helping organisations navigate through various difficulties that have beset those industries – the Global Financial Crisis of the late 2000s, the persistent low interest rates of the 2010s and the Covid-19 recession of 2020. In recent years the role of the CRO, and the activities it is responsible for have been mandated in regulation regimes around the world, including Solvency II in the EU, the Senior Managers' Insurance Regime in the UK and APRA's Prudential Practice Requirements in Australia.

Interestingly, James Lam is accredited with being the first person to coin the phrase, 'Chief Risk Officer'. He worked as the CRO at GE Capital from 1993.

As the module on Principle Terms says, the CRO's role is to have responsibility for overall leadership and development of ERM within the organisation. *Development* of ERM is the focus of this course, so it will not be expanded further here. *Leadership* of ERM has three main components.

- **The first is leadership of the ERM concept in the organisation, ensuring that decision makers are provided with appropriate and comprehensive risk information prior to decisions being made. This role is a key part of the second line of defence (this term was introduced in Module 8), independent of the first line of defence functions. This role is a combination of advocacy and explanation with challenge and oversight of what other functions are doing. Understanding the business and the drivers of business decision-making is very important for this role, as is an ability to translate between different technical functions' ways of saying the same thing.**
- **The second is taking a role within the leadership of the organisation as a full member of the Board or Executive Committee, regardless of the actual decisions made. Whatever the organisation decides, the CRO should ensure that the appropriate risk information is developed and shared to describe the emerging status of activity. The principle of collective responsibility for decision making inevitably means that there is occasionally a conflict between this role and the first role, and it is an important part of the activity of any CRO to navigate this conflict.**
- **The third is leadership of the team which implements the ERM framework. That is a leadership role like any other in an organisation, requiring the same mixture of people development skills, HR process knowledge and team organisation as, say, a Chief Actuary. The purpose of this role is to ensure that quality risk analysis and synthesis is provided for the other two components.**

In most ERM frameworks the CRO has little *power*, and therefore has to use *influence* to ensure that risks are managed well. This is almost inevitable – in order to maintain independence from the first line the CRO needs to ensure that accountability for decision-making remains with the first line. However, a good ERM framework will provide useful information to support that decision-making and will not simply get in the way.

The CRO's ERM framework is inevitably quite *abstract and philosophical*. In a well-run company it will look to codify existing good practice, and by doing so will help to identify where it can be improved. No CRO can be expert in the technical detail of every area of the organisation, but they need to have enough experience of the business and the way senior managers work that they can challenge their colleagues from a position of credibility. This means that *diplomacy* is a key part of the CRO's toolkit.

On a more technical level, it is important the CRO has a good grasp not only of the ERM concepts covered by this course, but of some other subject areas relevant to the work of the organisation for which they are CRO. Importantly this should include an understanding of the limitations of those subject areas, as an important part of the CRO's role is to be able to act as a *devil's advocate* – speaking up for a point of view that is not otherwise covered, in order to minimise the risk that the organisation succumbs to 'groupthink'.

In the case of a financial services organisation, for instance, one very important subject area covered is *economics.* This encompasses both the macroeconomic environment in which it and its customers trade and invest and the microeconomic forces at work as it selects products to sell and prices them. Another, often closely related, is *mathematical modelling* – because it is a tool that is key to helping the organisation understand the possible outcomes of the decision it makes.

Both these subjects are ones where it is both important to be rigorous and easy to be overconfident – it is easy to present the appearance of mathematical certainty through the use of statistical or economic techniques. It is therefore important that the CRO has the humility to acknowledge that the application of these techniques is subject to very significant uncertainty – and the gravitas to stand up to others who may want to apply them inappropriately. One of the author's favourite quotes is, 'All models are wrong, but some are useful' (usually attributed to the statistician George Box) – it is important to be able to recognise which models are not useful!

This rapid overview of the work of a Chief Risk Officer and its contradictions and challenges should not discourage the student. The work of a risk function which this course presents is fascinating, both intrinsically and because it has an important influence on the development and implementation of the strategy of the organisation it serves.

The above viewpoint outlines the varied roles, responsibilities and skills of a CRO. These are analysed and summarised in subsequent sections.

Module 12 Summary – Governance functions and the role of the CRO

Governance systems

Governance and assurance systems are processes and structures designed to give the Board of Directors confidence that the ERM framework is effective.

Chief Risk Officer (CRO)

The Board's (visible) support for the CRO is critical to the success of ERM. The CRO:

- often reports to the CEO or CFO
  - associated conflicts of interest can be reduced if the CRO *also* has a dotted reporting line to the Board (or risk subcommittee), which becomes a solid line under extreme circumstances
- ideally, the CRO should be a Board member and lead the risk subcommittee.

The responsibilities of the CRO include:

- providing overall leadership and direction for ERM
- overseeing the development / implementation / maintenance of an ERM framework
- managing the various risk functions, *eg* the RMF
- ongoing risk policy development and monitoring of adherence
- reporting on risk to internal decision makers and external stakeholders
- challenging and overseeing other areas of the business are doing with regard to risk
- managing / optimising the risk portfolio
- appropriate allocation of capital to business activities
- developing data systems and risk models to carry out high-quality risk analysis, monitoring and management
- safeguarding the company's financial and reputational assets
- maintaining expertise, and advising on matters of risk management
- supporting an appropriate risk culture across the business

A CRO requires many skills, including:

- leadership
- evangelism
- advising / consulting
- stewardship
- technical.

The risk management function (RMF) / central risk function (CRF)

The roles of the RMF / CRF include:

- giving advice to the Board on risk
- assessing the overall risks being run by the business
- comparing overall risk exposures with risk appetite
- acting as a central focus point for reporting by staff of new and enhanced risks
- giving guidance to line managers on the identification and management of risks
- monitoring progress on risk management
- pulling the whole picture together.

Models for interaction between the RMF / CRF and the business units

Various models exist to describe how the RMF / CRF might interact with the business units (each with benefits and shortcomings):

- offence vs defence
- policy and policing
- partnership.

There are many challenges faced in trying to align the interests of business units with that of the risk management function. These include how to:

- resolve conflicts
- manage risk function staff who work within the business units
- align remuneration incentives between the parties
- measure non-financial (*eg* operational) risks.

In order to create value and align interests, it is important for risk management to be integrated into business activities such as:

- business strategy development
- new product development
- pricing
- business performance measurement
- risk and incentive compensation / remuneration.

Influences on governance structures

The way in which a company chooses to structure the relationship between its RMF / CRF and the rest of the business will vary considerably according to the:

- existing governance structures
- size and nature of the business
- risks faced by the business
- autonomy / accountability of the business units in the current structure.

If a company has multiple risk management functions, *eg* across different geographical locations, it is important that these are co-ordinated and communicate effectively to avoid a silo mentality. Having a consistent engagement and reporting processes with the different business units will help to ensure an effective ERM framework.

Monitoring functions

In addition to the Board of Directors and the RMF / CRF, the stakeholders that have a monitoring role in relation to risk management include:

- the compliance function
- the internal audit function
- external audit.

The practice questions start on the next page so that you can keep the module summaries together for revision purposes.

Solar storms are themselves not new. However, scientists are now starting to understand that the resulting increase in neutron radiation can significantly disrupt the modern electrical and computer systems that we rely on for communications, banking, transportation *etc*. Significant investment is being made today in places like the Rutherford Laboratory in the UK to understand the effect of the emerging risk of a potentially catastrophic neutron storm (such as the 1859 Carrington event) on today's technology.

4.3 Emerging IT risks

Given the increasingly reliance of companies on computers and the internet, IT-related risks are a significant area of emerging risk. These include:

1. cyber security
2. cloud computing
3. social media

Cyber risk

Cyber risk is a notable example of a risk which can be considered to be 'emerging' in terms of having rapidly changing characteristics.

It is defined by the Institute of Risk Management as 'any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems'.

This typically is connected to online activity, internet trading, technological networks and the storage of personal data. Risks include hacking, security breaches, espionage, data theft, extortion, privacy breaches and cyber terrorism.

The implications can include business interruption, reputational damage and legal liability, with associated costs of communications, resolution, compensation, loss of business and possibly fines and legal costs. There may also be infrastructure threats and risks to the physical safety of individuals.

Although it is now a well-recognised risk area, the nature and source of cyber attacks and exposures is constantly changing, and typically under-reported, and hence difficult to monitor and manage.

Controls include having strong IT security, including firewalls and malware protection, clear policies and governance for users, and incident management processes. Regular review is essential and there is benefit in information sharing and collaboration across entities (*eg* the EU Cyber Security Directive).

It may be possible to purchase cyber insurance to cover losses relating to damage to, or loss of information from, IT systems and networks – such losses may be excluded from general liability insurance coverage.

Cyber insurance may for example cover:

- **loss of or damage to digital assets**
- **business interruption**
- **legal defence and damages costs**
- **required communications to customers**
- **reputational damage**
- **third party losses (*eg* customers).**

The insurance company may also provide expertise and assistance in managing the incident.

4.4 Climate change risk

Another notable example of an emerging risk is climate change risk. This can be defined as the risks arising from adverse changes in the physical environment and secondary impacts in the economy at a regional or a global scale.

Climate change risks can broadly be classified into three categories. In its 2015 report, "The impact of climate change on the UK insurance sector", the Prudential Regulation Authority described three categories of risk arising from climate change: physical, transition and liability risks:

1. **Physical risk – risks arising from the first-order effects of environmental changes such as greenhouse emissions, pollution and land use. The effects may be chronic, such as global warming and sea level rise, or they may be acute events, such as instances of extreme weather.**

   Such risks may arise in the short-term from damage to property and from business disruption due to the changing frequency and severity of extreme weather events such as hurricanes, droughts and flooding.

   In the longer-term, chronic impacts may dominate, such as rising temperatures, rising sea levels and changes to rainfall patterns affecting use of land for agriculture and local workforce availability. Some areas will become less habitable, potentially causing large scale migrations that trigger social unrest and disrupt economic activity.

2. **Transition risk – risks arising from the economic, political and market changes as part of the move to a low-carbon economy, that is, an economy with significantly lower emissions of greenhouse gases due to much lower fossil fuel use and possibly negative emission technologies such as carbon capture and storage.**

   Sources of transition risk include:

   – **policy measures (*eg* carbon taxes and energy efficiency standards)**
   – **technological change (*eg* a move to renewable energy and electrical vehicles)**
   – **changing customer preferences (*eg* increased demand for 'green' products).**

3. **Liability risks – relate to the potential costs from injured third parties seeking compensation because they have suffered loss or damage from the impacts of climate change.**

An increasing number of lawsuits are being brought, albeit with limited success so far. For example:

- **the Mayor of New York tried to sue oil and gas companies to recover the costs of measures to increase the city's resilience to climate change**
- **ExxonMobil successfully defended itself against allegations of misleading investors by a historic failure to acknowledge climate risks to its business.**

It is possible that actuaries and their clients could face legal claims themselves in future if they fail to consider climate-related risks.

Question

Describe in detail the potential impact of these three categories on the risk profile of a life insurance company.

Solution

Physical risks

- Mortality and morbidity rates may increase due to:
  - the direct impact of severe weather events, *eg* hurricanes, drought, flooding
  - increased prevalence of vector-borne diseases, *eg* malaria
  - increased air and water pollution
  - crop failures, food and water shortages (from droughts and flooding)
  - worsening nutrition and hygiene
  - increased likelihood of pandemics
  - mass migration leading to overcrowding and social unrest
  - deterioration in transport infrastructure resulting in problems accessing healthcare.
- These transition effects could manifest as a 'shock' impact (*eg* from an adverse weather event) or a 'trend' impact' (*eg* from gradually rising temperatures).
- The effects may be more severe for policyholders of certain ages (older), in certain geographical locations (*eg* areas prone to flooding, coastal areas), with pre-existing health conditions, or in certain occupations (*eg* agriculture).
- If the life insurer sells annuities as well as assurance contracts, the above (adverse) effects are partially hedged.
- It is also possible that mortality and morbidity rates decrease in certain geographical locations due to reduced prevalence of cold temperatures, and hence:
  - lower rates of influenza
  - lower risks associated with cold housing conditions, *eg* hypothermia.
- Physical risks may also impact adversely on the insurer's asset values …

  … *eg* increased instances of extreme weather could result in economic losses to many companies.

- Operational risks may increase, for example:
  - property damage and business interruption to the life insurer itself, *eg* if based in a geographical area that is susceptible to climate change
  - suppliers or outsourcers used by the insurer vulnerable to business interruption.
- Regulatory capital requirements may increase as the adverse weather events (in respect of which the insurer seeks resilience) become more extreme.

Transition risks

- Market risk from both changes in (and increased volatility in) asset values is likely to increase, for example:
  - falls in the value of investments in companies that produce fossil fuels (*eg* coal, oil and gas extraction), as carbon taxes and energy efficiency standards increase
  - falls in the value of investments in energy intensive companies (*eg* manufacturers, chemical industries, forestry), as the costs of production increase
  - increases in the value of investments in green technologies (*eg* producers of renewable energy, electric vehicles), as both consumer and regulatory demand for these technologies increases.
- These transition effects could manifest as a 'shock' impact (*eg* if investor sentiment or regulation suddenly change) or a 'trend' impact (more gradual shifts).
- Strategic risk may increase if the life insurer fails to plan adequately for these impacts (*eg* fails to divest from companies likely to be adversely affected from climate change).
- Similarly, there may be an increase in reputational risk by association, with companies that are carbon intensive, or if the life insurer itself fails to reduce its carbon footprint.
- The expenses of transitioning may be higher than expected.
- Regulatory capital requirements may increase as the insurer seeks protection from climate-related market risks.

Liability risks

- There may be increased credit default risk and market risk in respect of investments in companies who are adversely affected by liability risk (*eg* general insurance companies).

As companies have become more conscious of Corporate Social Responsibility and investors have demanded greater disclosure around firms' exposure to climate change, actions and metrics related to climate change are forming a more prevalent component of the disclosures in annual reports, even where there are no formal requirements.

Question

Suggest metrics that could be used by a life insurance company to monitor exposure to the impact of climate change.

Solution

Possible metrics (not exhaustive) include:

- composition of insured lives by, *eg* age, geographical location, exposure to pre-existing health conditions, occupations, products
- potential ultimate mortality rates, *eg* in countries with extreme temperatures / rainfall
- weather related metrics, *eg* temperature, rainfall
- value (absolute or percentage) of investments held by the insurance company that are:
  - allocated to low-carbon or renewable technologies
  - allocated to carbon intensive industries
  - physical, *ie* property, infrastructure projects, located in coastal or flood zones
  - exposed to physical and transition risks (low / moderate / high)
- carbon footprint by asset class / sector / industry / company invested in
- results of climate risk scenario / stress tests, *eg* a climate risk VaR
- the insurance company's own:
  - greenhouse gas emissions / carbon footprint
  - exposure to business locations vulnerable to business interruption / displacement
  - alignment with government target reductions in emissions
- similar metrics to those above for the insurance company's suppliers / outsourcers
- revenue generated by the insurance company from sustainable solutions, *eg* solar panels on the roofs of its offices
- operational expenses to address climate change risk mitigation / regulation
- capital expenditure on low-carbon technologies or renewable energy
- reserves set aside for climate-related legal actions
- reputation / brand / customer / employee satisfaction index scores (with a focus on how the insurance company is managing climate change risk if possible)
- executive remuneration that is linked to the achievement of climate change initiatives.

Emerging market practice, guided by the framework introduced by the Taskforce for Climate Related Financial Disclosures (TCFD), may drive the foundation of future regulatory frameworks, or simply become a 'must have' expectation.

The TCFD was set up, with a global remit, to help investors, lenders and insurance underwriters better assess the risks and opportunities associated with climate risk. In its 2017 report (Recommendations of the Task Force on Climate-related Financial Disclosures), it recommends that all organisations make climate-related disclosures in their mainstream financial reports.

Many advantages of such disclosure are promoted, for example:

- more informed business and investment decisions
- better shareholder engagement
- help with complying with other (*eg* regulatory) disclosure requirements.

Wider aims are to advance assessment practices and techniques and to encourage organisations to demonstrate responsibility and foresight in their consideration of climate issues.

The TCFD recommends that climate-related disclosures incorporate the following four elements:

1. governance – in relation to climate change risks and opportunities
2. strategy – the impact of risks and opportunities on an organisation's strategy and the resilience of that strategy to climate-related scenarios
3. risk management – the processes used to identify, assess and manage climate risks
4. metrics and targets – used to assess and manage climate risks.

There is significant regulatory interest in the nature and level of disclosure and as regulatory frameworks continue to develop formal requirements are likely to increase.

To deal with the financial risks from climate change in their work, actuaries need to use data and make financial judgements about the future. Traditional tools that do not allow for constraints and dynamic interactions do not describe that future.

In particular, traditional actuarial approaches, based on using past experience to predict the future, are not appropriate for modelling climate change. This is because natural catastrophes from physical risks are becoming increasingly severe and transition risks are evolving rapidly as regulation and customer behaviour shift. Climate-related risks are characterised by a high level of uncertainty, over diverse time horizons, with multiple interactions between the various physical, transition and liability risks. Hence, forward-looking techniques such as scenario analysis, which can allow for constraints and dynamic interactions, are preferable.

The TCFD recommends that organisations use scenario analysis as a tool for understanding the drivers and strategic implications of climate-related risks and opportunities. Scenario analysis (which is covered in more detail in Module 15) is a process whereby the impact of a range plausible future hypothetical scenarios are considered. Scenario analysis allows for interactions between combinations of climate-related risks.

To consider climate change, actuaries will need to help people navigate problems through time, often over decades. It is likely that in future we will see a greater connectedness between climate-related actions of regulators, governments and individuals. Such coordinated actions might magnify systemic risks. Uncertainties will be higher than demonstrated in historic data.

4.5 Identification and analysis

The broad process for identification, analysis and related decision-making follows that for any other risk. However, the nature of emerging risks is such that additional issues arise.

A more holistic view is initially required for emerging risk identification, considering all possible impacts of the new risk, before this is reduced to the more structured approach typically taken for known risks within a risk framework. A key identification tool is *horizon scanning*: the systematic search for potential developments over the longer term, with the emphasis on those changes that are at the edges of current thinking.

Horizon scanning was first mentioned in Module 6 as a risk identification technique recommended in the UK Treasury's Orange Book. It was also mentioned in Module 8 as a more strategic planning tool.

For this to be effective, it requires input from experts who understand the underlying drivers and the technological / scientific / economic / socioeconomic aspects. It may be that expertise in the relevant areas is not available within the organisation and may be difficult and/or costly to obtain, and there will therefore be reliance on relevant external sources. Sources of information for the identification and analysis of emerging risks can include academic journals and websites relevant to the specific area.

It is unlikely that there will be a definitive study on any particular aspect (as, by definition, emerging risks have not yet been subject to substantial analysis), so each needs to be assessed from different angles and sources. Risk management decisions then need to be weighted according to the credibility and reliability of the underlying 'evidence'. Continual monitoring of developments in relevant research will be important in order to refresh these decisions.

The more alarmist media reports can be useful in alerting the organisation to potential areas for further investigation, but should not in themselves be used as a basis for decision-making.

For companies where the potential financial impact rests on the likely future legal approaches to such emerging factors (*eg* general insurance companies) there is an added layer of uncertainty that requires analysis. There may be nervousness within an organisation that early identification of a potential risk could lead to a greater duty of care or liability under law. However, companies who actively identify and consider such emerging risks will be the ones that are ready to meet and react to such risks, and can thus reduce the risk of exposure to retrospective liabilities.

An analysis of trends is important, as is the need to monitor regulatory and lobbying activity in that sector. All such analysis should be performed by the relevant experts.

When analysing trends, it is important to keep dependencies in mind. Changes in dependency, and the corresponding reduction in diversification, have been a key driving factor in many past risk events.

The importance of dependencies is a key theme in Subject SP9 and will be discussed in more detail later in the course.

5 Bias

Without a supportive risk culture, it is possible that risks are not identified, assessed or reported in a true and honest way. This is known as the *problem of bias*, and often occurs in the context of project appraisal.

5.1 Sources of bias

Bias might arise:

1. intentionally, *eg* where a manager deliberately underestimates a risk to achieve a specific personal goal, such as forwarding their own career or avoiding the scrutiny of the risk management function
2. unintentionally, *eg* where a manager inaccurately assesses a risk due to lack of experience or time.

If the culture is less than optimal, the reporting of risks can be subject to bias. This often arises in project appraisal, for example, where project champions (perhaps anxious to advance their own careers or obtain political advantage) may tend to minimise the risks in the hope of getting the project approved.

There are many ways in which bias can be introduced into project appraisal, either by accident or design:

- **Insufficient care may have been devoted to the identification or analysis of risks.**
- **Key risks may have been accidentally or deliberately omitted.**
- **Incorrect assumptions that certain risks are independent of each other may have concealed the true likelihood of 'chain reactions' of adverse events.**
- **The likelihood of disasters occurring may have been underestimated because of inadequate past experience.**
- **Cashflows may have been guessed or, worse, deliberately biased towards optimism.**
- **Insufficient account may have been taken of the future ups and downs of the economic cycle.**
- **The risks associated with new technologies may have been given inadequate attention.**
- **Not all the effects of the project on the sponsor's other business may have been considered.**
- **Credit may have been taken for benefits not directly attributable to the project.**
- **The assumptions on which the estimates are based may not correspond with senior management's views of the world in future.**
- **Arithmetic or spreadsheets may contain errors which lead to substantially incorrect evaluation, or there may be failures of logic in building the model.**

Bias can similarly take place in reporting to the Board about the ongoing risks facing the whole enterprise.

Module 13 Summary – Business analysis, risk identification and initial assessment

Process for risk identification and initial assessment

1. Analyse the business operations and wider environment. Ensure that the business has clear objectives.
2. Identify key risks to the business objectives in a structured way.
3. Obtain agreement on the risks faced, the relationships between them, and accountabilities for each risk and its management.
4. Evaluate the risks in terms of probability, severity and interdependency, gross and net of existing controls.
5. Produce / update the *risk register* (a central document detailing all the risks faced by a company), prioritising top risks for further analyses ('deep dives'), quantification and risk mitigation.
6. Review the risk register regularly, especially in times of change. (Ideally, integrate assessments into everyday business operations.)

Tools for identifying risks

A range of idea generation tools exist to help organisations identify risks:

- SWOT analysis
- risk check lists
- risk prompt lists
- risk taxonomy
- case studies
- process analysis.

Risk identification techniques

Various techniques exist with which to implement the above tools:

- brainstorming
- independent group analysis
- surveys
- gap analysis
- Delphi technique
- interviews
- working groups.

Risk concepts

1. exposure
2. volatility
3. probability
4. severity
5. time horizon
6. correlation
7. capital.

Inherent vs residual risk

Inherent risk is the risk to an entity in the absence of any actions that management might take to alter the risk's likelihood or impact.

Residual risk is the remaining risk after management has taken action to alter the risk's likelihood and impact. It may also be a secondary risk resulting from taking another risk response action.

Risk maps and heat maps

A risk map illustrates the effect that a risk might have on a company by ranking risk exposures by severity on the x-axis and probability on the y-axis. A risk map may also illustrate the results of control effectiveness by mapping both the inherent and residual risks.

A heat map plots severity against control effectiveness rating.

Emerging risks

Emerging risks are:

- either new risks, or changes in already known risks (or their control effectiveness)
- subject to high levels of uncertainty and ambiguity
- difficult to quantify using traditional risk assessment techniques
- important since they may represent a new business opportunity or have a significant impact on profitability, operations or strategy.

Trends giving rise to emerging risk management challenges include:

- globalisation
- technology (cyber risk)
- changing market structures
- restructuring of businesses.

Emerging risks might be identified using *horizon scanning*, with input from experts and external sources of information (*eg* academic journals).

Cyber risk

Cyber risk is the risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.

It is an emerging risk, characterised by rapidly changing characteristics.

Example risks include hacking, security breaches, espionage, data theft, extortion, privacy breaches and cyber terrorism.

Risk controls include strong IT security (*eg* firewalls, malware protection), clear policies and incident management processes, regular monitoring and cyber risk insurance

Climate change risk

Climate change risk is defined as the risks arising from adverse changes in the physical environment and secondary impacts in the economy at a regional or a global scale.

They can be classified as:

- physical – relating to first-order effects of environmental changes
- transitional – arising from a shift to a low carbon economy
- liability – arising from injured parties seeking compensation.

Climate change is an emerging risk, characterised by high levels of uncertainty over impact and time horizons.

There is increasing interest from regulators with regards to the nature and level of disclosures made by organisations on climate risk. Recommendations have been made by the Taskforce for Climate Related Financial Disclosures (TCFD).

Assessment of climate change risk requires forward-looking techniques such as scenario analysis, which can allow for constraints and dynamic interactions, rather than traditional actuarial tools based on historic data.

Bias

Without a supportive risk culture, it is possible that risks are not identified, assessed or reported in a true and honest way – this is known as the 'problem of bias'. Bias may arise intentionally or unintentionally.

Examples of behavioural bias in financial decision-making are: overconfidence, anchoring and representative heuristics.

The problem of bias can be reduced by:

- incorporating checks and balances into the risk identification and assessment process, such as:
  - validating the work via independent review
  - referencing similar projects
- introducing an *optimism bias*, where the capital cost is increased by a percentage

Module 13 Practice Questions

13.1 Outline seven risk concepts with which employees of a company should be familiar.

13.2 Describe how:

(i) probability and severity can be combined so as to quantify the risk associated with a range of possible future events.

(ii) risk concentration can be reduced in respect of financial risks and operational risks.

13.3 List the reasons that bias may be present in project appraisal.

13.4 Describe briefly three areas of emerging IT risks.

13.5 Describe how climate change may affect an insurance company's ERM framework. [10]

Exam style

13.6 For each of the following situations, describe any potential problems of bias and propose corrective actions:

Exam style

Situation 1: An external consultant advises a company to make a £1*m* investment in a new business unit, which he suggests he is employed to run. [2]

Situation 2: The designer of a new oil rig claims he has saved £5*m* in construction costs by eliminating certain back-up systems arguing that these features are redundant as they have never been used when installed on existing rigs. [2]

Situation 3: The project manager overseeing a major public sector IT system integration project reports to the relevant government minister that the project is due to complete on track and on budget in a year's time. [4]

Situation 4: A student actuary's spreadsheet model reveals previously unknown mortality margins in an annuity product. The results of the model are used to propose a pricing change to take advantage of the additional margin. [2]

[Total 10]

The solutions start on the next page so that you can separate the questions and solutions.

13.5 Impact of climate change risks on an insurance company's ERM framework:

Corporate governance

- An organisational structure, roles and responsibilities, and reporting lines in respect of climate change risk will need to be established. [1]
- The company could appoint a board member responsible for climate change risk … [½]

  … and/or establish a separate board subcommittee. [½]
- Climate change risk should get sufficient discussion time at Board meetings. [½]
- Risk appetite / tolerance statements on climate change should be set and approved. [½]

  Climate change risk should be incorporated (appropriately and proportionately) into risk policies … [½]

  … and compliance with the policies monitored regularly. [½]
- An appropriate risk culture should be established to encourage reporting of climate change risks and sharing of ideas relating to risk mitigation and opportunities. [½]
- Training and education on climate change risk should be provided to enhance understanding throughout the company. [½]

Line management

- It will be necessary to introduce a process to identify new risks from climate change … [½]

  … and owners of these risks assigned to manage them. [½]
- The impact of climate change risk should be integrated into business processes such as:
  - setting premiums
  - product development
  - setting policy terms and conditions
  - reserving and solvency capital requirements
  - capital allocation
  - investment decisions
  - business continuity planning. [½ for each, maximum 2]
- New operational processes may be introduced in response to consideration of the impact of climate change, *eg* paperless offices, no company cars. [½]
- There may be requirements to relocate offices or staff should acute climate change events occur. [½]

Portfolio management

- The company's risk taxonomy needs to be updated to include climate change risk definitions. [½]
- An understanding should be developed of the interactions between the different climate change risks: physical, transition and liability … [½]

  … as well as the interaction of these risks with other risk categories, *eg* market, credit, operational, strategic, compliance, reputational risks … [½]

  … so that concentrations of risk and diversification benefits can be recognised. [½]

Risk transfer

- The insurance company should seek out cost-effective ways of transferring climate change risk, *eg*:
  - insurance of its own premises against business interruption, property damage [½]
  - reinsurance of mortality claims in respect of weather-related perils, including catastrophe reinsurance [½]
  - alternative risk transfer products, *eg* weather-related derivatives, catastrophe bonds. [½ for any ART example]

Risk analytics

- Scenario testing should be used, as a forward-looking approach, to assess the impact of a range of hypothetical climate-related scenarios. [1]
- The model should be dynamic, allowing for full interactions between different risk types … [½]

  … and the impact of risk management actions to address climate change risk. [½]
- Risk reports should include appropriate KRIs in respect of climate change … [½]

  … as well as losses from past risk management failures due to climate change risk. [½]

Data and technology resources

- Using past data is unlikely be a good predictor of future climate change risk …

  … due the rapidly changing nature of the risks and the future uncertainties involved. [½]
- Data will need to be collected from a wide range of external sources … [½]

  … and actuarial judgement applied to weight its credibility and relevance. [½]

3.5 Advantages and disadvantages of the GEV distributions

We can also use GEV distributions to investigate the limiting distributions for the minimum values of a distribution. If $H(x)$ is the limiting distribution for the standardised maximum value for a particular γ, then $1-H(-x)$ is the limiting distribution for the standardised minimum value from the same original distribution.

Question

Outline two key limitations of the GEV approach.

Solution

1. A key disadvantage of the GEV approach is that a lot of data (and hence information) is lost (as everything apart from the maxima in each block is effectively ignored).

2. The choice of block size can be subjective, and represent a compromise between granularity (*eg* 1-in-100 or 1-in-1000 estimates) and parameter uncertainty.

4 The generalised Pareto distribution (GPD)

As an alternative to focusing upon a single maximum value, we can consider *all* the claim values that *exceed* some threshold as extreme values.

4.1 Threshold exceedances

If we let X be a random variable for losses, with cumulative distribution function, F, then the *excess distribution over the threshold*, *u*, has the distribution function:

$$F_u(x) = P(X - u \le x \mid X > u) = \frac{F(x+u) - F(u)}{1 - F(u)}$$

for $0 \le x < x_F - u$ where $x_F \le \infty$ is the right endpoint of X.

More generally we find that, for a large class of underlying *iid* distributions of loss data, as the threshold increases, *ie* as $u \to x_F$, the distribution of the threshold exceedances will more closely resemble a generalised Pareto distribution.

4.2 The CDF of the GPD

The GPD is a two-parameter distribution with CDF:

$$G(x) = \begin{cases} 1 - \left(1 + \dfrac{x}{\gamma\beta}\right)^{-\gamma} & \gamma \neq 0 \\ 1 - \exp\left(-\dfrac{x}{\beta}\right) & \gamma = 0 \end{cases}$$

$\beta > 0$ is a scale parameter and γ is the shape parameter.

The CDF for the *standardised GPD* is given by setting $\beta = 1$.

Question

Describe the GPD distribution. (*Hint: sketch examples and refer to any bounds.*)

Solution

For the GPD:

- there is a lower bound ($x \ge 0$) when $\gamma > 0$
- there is also an upper bound ($0 \le x \le -\gamma\beta$) when $\gamma < 0$
- if $\gamma > 0$ then the GPD becomes the Pareto distribution
- if $\gamma = 0$ then the GPD becomes the exponential distribution.

Module 20 Summary – Extreme value theory

Low frequency / high severity events

Lack of data (especially from severely stressed time periods) makes such extreme events hard to model accurately. Modelling the full distribution can help overcome this difficulty. But, the form of distribution may still be incorrect in the tails, *eg* where:

- the 'true' distribution is more skewed or leptokurtic than is indicated by the available data
- the parameter estimates are inappropriately influenced by the main bulk of the data in the middle of the distribution
- features change over time, *eg* heteroscedasticity, structural breaks.

Better modelling of the tails of the data can be done through the application of extreme value theory.

The generalised extreme value distribution

If:

- losses X_i are *iid* with cumulative distribution function, F
- $X_M = \max\left(X_1, X_2, \ldots, X_n\right)$ are the *block maxima*
- $\beta_1, \ldots, \beta_n > 0$ and $\alpha_1, \ldots, \alpha_n$ are a suitable sequence of real constants

then, if n is sufficiently large, the distribution of the standardised block maxima $\frac{X_M - \alpha_n}{\beta_n}$ is approximately described by the generalised extreme value (GEV) family of distributions:

$$H(x) = \lim_{n\to\infty} P\left(\frac{X_M - \alpha_n}{\beta_n} \le x\right) = \lim_{n\to\infty} F^n\left(\beta_n x + \alpha_n\right).$$

The three parameters of the GEV family determine:

- location (α)
- scale (β)
- shape (γ).

The GEV distribution can be used to analyse a set of observed losses in two different ways.

1. select the maximum observation in each block (the return-level approach)
2. count the observations in each block that exceed some set level (the return-period approach).

Parameters for the GEV distribution can be estimated using MLE or the method of moments. The choice of the number of blocks determines the trade-off between the granularity of information provided and the variance of parameter estimates.

A disadvantage of this approach is that it ignores a lot of data (all non-maxima).

The generalised Pareto distribution

If we let X be a random variable for losses, with cumulative distribution function, F, then the *excess loss distribution over the threshold*, u, has the distribution function:

$$F_u(x) = P(X - u \le x | X > u) = \frac{F(x+u) - F(u)}{1 - F(u)}$$

for $0 \le x < x_F - u$ where $x_F \le \infty$ is the right endpoint of X.

More generally we find that, for a large class of underlying *iid* distributions of loss data, as the threshold increases, *ie* as $u \to x_F$, the distribution of the threshold exceedances will more closely resemble a generalised Pareto distribution.

The two parameters of the GPD family determine scale (β) and shape (γ).

The empirical mean excess loss function is defined as:

$$e(u) = \frac{\sum_{i=1}^{N} (X_i - u)\, I(X_i > u)}{\sum_{i=1}^{N} I(X_i > u)}$$

To select a suitable threshold (above which a GPD is fitted to the data), determine the lowest threshold above which the empirical mean excess loss function, $e(u)$, is linear in u. The slope of this line is related to the shape parameter γ. Typically, the chosen threshold is likely to be around the 90-95th percentile of the complete distribution. Above this threshold, a GPD can be fitted to the selected data by using MLE or the method of moments to determine the parameters.

There is a trade-off between the quality of approximation to the GPD (good for high thresholds) and level of bias in the fit (lower for lower thresholds).

Asymptotic property

When the *maxima* of a distribution converge to a GEV distribution (which is the case for all commonly used statistical distributions), the *excess* distribution converges to a GPD distribution with an equivalent shape parameter γ.

Module 22 Practice Questions

22.1 List the features of the returns on individual equities that have been suggested by time series analyses.

22.2 If the risk-free rate of return is 2%, the equity risk premium derived from the market is 4% and RiskPro plc, (an ungeared company which pays no tax), has a beta of 1.25, calculate (assuming the CAPM applies):

(i) the expected return from the market

(ii) the expected return from shares in the company

(iii) the cost of capital used by the management in evaluating projects.

22.3 Exam style

A leading economist has said that when it comes to modelling changes in future foreign exchange rates or interest rates with time series models, it is more important that the model predicts the direction of the change than the amount of the change.

Discuss when it may be sufficient to model only the directional change *vs* modelling the amount and the direction of the change. [5]

The solutions start on the next page so that you can separate the questions and solutions.

Module 22 Solutions

22.1 Features of the returns on individual equities that have been suggested by time series analyses include:

- returns are rarely independent and identically distributed
- there is little evidence of serial correlation, however there is some evidence of momentum effects (short term) and mean reversion (longer term)
- volatility appears to vary over time, but …
- … there is evidence of serial correlation in absolute or squared returns, *ie* extreme returns appear in clusters, known as *volatility clustering*
- return series are *leptokurtic*, *ie* more peaked and heavier tailed than a normal distribution.

22.2 (i) ***Expected return from the market***

Market return = risk-free return + equity risk premium

= 2% + 4% = 6%

(ii) ***Expected return from the company shares***

Using the security market line equation from CAPM, we have:

$$E_i = r + \beta_i \left(E_M - r\right)$$

$$= 2\% + 1.25\left(6\% - 2\%\right)$$

$$= 7\%$$

(iii) ***Management cost of capital***

The cost of capital should be 7% (as above) to meet investors' expectations.

This assumes that no tax is payable, and that a project that yields a return of 7% would offer the same return to equity shareholders.

22.3 Modelling the direction of change vs amount of change

Any model needs to be fit for purpose – it will be important to understand the purpose of the model before deciding whether to model only the direction rather than the amount of change. [1]

It may be sufficient to model the directional change only:

- if there is a lack of past data, and it is not statistically credible to model the amount of the change [½]
- if the rate changes are expected to be small and/or relatively invariable (insensitive to parameter choices) over time [½]
- if the size of the changes shows no discernible pattern (*ie* appears random). [½]

It may be necessary to model the amount as well as the direction of the change:

- when modelling extreme movements, as the amount of change is very important and cannot be ignored [½]
- if there is a large quantity of data and/or if the amount of the change is expected to be variable (sensitive to parameters chosen) over time [½]
- when the process is mean-reverting, although arguably could make the directional change mean-reverting [½]
- when considering risk appetite, as it is necessary to understand the scale of the risk as well as the direction. [½]

In order to predict the amount as well as the direction of the change, more parameters are likely to be required in the model. [½]

However, this may lead to 'overfitting' of the model and potentially spurious results. [½]

In financial time series models, this trade-off between goodness of fit and number of parameters can be measured by statistics such as the AIC and BIC. [½]

Missing the direction means that any estimate of the amount is effectively amplified by a factor of 2 (the answer should have been +2% and not minus 2%). [½]

[Maximum 5]

Module 24 Practice Questions

24.1 Explain how the operational risk capital can be calculated under the following models:

(i) implied capital model

(ii) income volatility model

(iii) capital asset pricing model.

24.2 You are a specialist risk consultant and you have been approached by the directors of a small manufacturing company. The company has not previously actively managed operational risk in any formal way and the directors are seeking your advice.

(i) Suggest reasons why the directors might have become interested in operational risk management at this time.

(ii) Explain the main advantages of a more formal approach to operational risk management.

(iii) Describe the benefits that the directors could expect to see if they enforce an effective operational risk management process.

24.3 (i) Distinguish between bottom-up and top-down approaches to assessing operational risk.

(ii) Describe bottom-up approaches to assessing operational risk.

(iii) State four top-down models that can be used in assessing operational risk.

(iv) Outline the main problems with all of the top-down models.

24.4 Give reasons why operational risk might NOT be best measured simply as a percentage of a company's revenue.

24.5 Compare the data typically used by a company for modelling credit risk with that for modelling operational risk. [7]

Exam style

24.6 (i) Define operational risk. [1]

Exam style

(ii) Explain why a company may find it difficult to assess its operational risk exposure. [3]

A company has identified the following three main operational risks it faces:

- Risk 1: IT system failure.
- Risk 2: Staff injury following health and safety breach.
- Risk 3: Earthquake in the vicinity of the firm's headquarters.

It chooses to model its operational risk exposure over the coming year using the following simple model and generates results using Monte Carlo simulation.

- Risk 1: Assumed to be certain to occur, with the impact of the failure equally likely to take any value between £0 and £10 million.
- Risk 2: Assumed to occur with probability 30%; if the risk does occur the financial impact will be £1 million paid in compensation to the injured staff member.
- Risk 3: Assumed to occur with probability 5%; if an earthquake does occur its financial impact is assumed to be equally likely to take any value between £0 and £100 million.

(iii) Carry out four simulations of the company's operational risk exposure for the following year, using the pseudo-random numbers provided on page 190 of the *Tables* in the following way:

- Column 1 is used to generate a value for the impact of Risk 1.
- Column 2 is used to assess whether Risk 2 occurs.
- Column 3 is used to assess whether Risk 3 occurs.
- Column 4 is used to generate a value for the impact of Risk 3, should it occur.

Use values from row 1 for the first simulation, values from row 2 for the second simulation and so on. [5]

(iv) Describe another method of simulating results from a model. [2]

[Total 11]

Any model for operational risk needs to cope well with the outer tail of the loss distribution. Extreme value theory (EVT) may be appropriate in this context but the lack of internal data means that this approach is not widely used.

Alternatively, perhaps due to such a lack of data, a simpler approach might need to be adopted under which it is assumed that losses are related to the volume of transactions (by number or value) and to apply a weighting to the actual or expected volume of transactions.

Bottom-up models often use statistical analysis.

(iii) ***Top-down models***

- implied capital model
- income volatility model
- economic pricing model
- analogue model.

(iv) ***Problem with top-down models***

All these models fail to capture successfully low probability, high consequence risk events.

All these models do not consider specific individual activities / incidents. There is no assessment of the effect of individual events, so these models do not help in minimising future losses by improving procedures in this area.

24.4 A percentage of revenue bases the capital charge purely on the size of the institution. Although this is often a good measure of the risk:

- some insurers take on much more complex risks, which lend themselves to a greater chance of operational risk in the form of settlement failures, legal or litigious risk, IT problems and even fraud. So two insurers of the same size may have different levels of operational risk.
- some insurers operate internationally, which adds a significant layer of difficulty and potential operational risk.
- some insurers have taken great steps to avoid operational risk, by documenting procedures, having well-trained staff, *etc*. However, they will not benefit if capital is determined by size only.

24.5 Comparison of data for modelling credit and operational risks

Similarities

For both types of risk, data is needed to determine both the expected frequency and severity of losses. [½]

For both types of risk, both internal and external data sources are likely to be used. [½]

Differences

The main different types (data splits) of credit risks are government, company and individual. [½]

Operational risk data is more heterogeneous and so more data splitting is likely to be needed. [½]

There are a wide variety of readily available and credible data sources on the different sources of credit risks, *eg*: [½]

- credit rating agencies on the creditworthiness of governments and companies [½]
- credit scoring agencies on the creditworthiness of individuals [½]
- corporate bond prices / credit spreads / credit default swap prices on the likelihood of company default. [1]

Operational risk data is likely to be less easy to source and more sparse in quantity. [½]

For example, although information on internal process errors is generally easy to obtain … [½]

… other data on operational risks may not be readily available, *eg* near misses that are not recorded for fear of staff recriminations … [½]

… or credible, *eg* data on events that do not happen frequently such as a severe fraud event. [½]

External data on credit risk are likely to be subject to greater scrutiny than operational risk data, which makes them more robust / reliable. [½]

External data on operational risk is likely to be less relevant to the specifics of the organisation concerned … [1]

… due to differences, *eg* in operating processes, business mix, size, governance and controls. [½]

Operational risk data is likely to be more qualitative … [½]

… and more (subjective) expert judgement needed, *eg* to construct worst-case scenarios. [1]

Operational risk events appear to occur more randomly through time. [½]

Credit risk is likely to be more influenced by the economic cycle … [½]

… and contagion risk. [½]

Therefore, it may be necessary to adjust historic credit risk data to reflect this. [½]

[Maximum 7]

3 Assessing non-life insurance risk

As with demographic risk, non-life insurance risk can be broken down into:

- level risk – dealt with here using a combination of experience and risk rating
- reserving risk, which includes:
  - volatility risk
  - catastrophe risk – especially incidence risk arising from concentrations of exposures, *eg* geographic
  - trend or cycle risk.

Question

Discuss how the nature of non-life insurance risks differs from demographic risks.

Solution

Trend or cycle risk – is more likely to correspond with the economic cycle (than for demographic risk), and so is best assessed using scenario analysis. However, generally, non-life insurance risks have a shorter period of exposure than life insurance risks so longer-term changes in risk factors are less important than a correct assessment of the risk factors themselves.

Unlike demographic risks, non-life insurance risks can be divided into two broad categories, depending on incidence rates:

- high frequency, *eg* motor
- low frequency, *eg* excess-of-loss reinsurance, where the intensity has greater variability.

There is the added complication that the *intensity* of claims also needs to be assessed (whereas for demographic risk the intensity, *eg* the pension scheme benefit, is known or defined by some other variables).

The key distinction between life and non-life insurance risk is that non-life policies may experience (many) more than one claim and move through (many) different states over the lifetime of the policy.

4 Assessing climate change risk

Climate change risk was introduced in Module 13. In this section, we recap on the different types of risk and then extend to consider how climate change risk may be modelled.

4.1 Types of climate change risk

Question

Describe the three types of climate change risk: physical, transition and liability.

Solution

1. Physical risk – risks arising from the first-order effects of environmental changes such as greenhouse emissions, pollution and land use. The effects may be chronic, such as global warming and sea level rise, or they may be acute events, such as instances of extreme weather.

   Such risks may arise in the short-term from damage to property and from business disruption due to the changing frequency and severity of extreme weather events such as hurricanes, droughts and flooding.

   In the longer-term, chronic impacts may dominate, such as rising temperatures, rising sea levels and changes to rainfall patterns affecting use of land for agriculture and local workforce availability. Some areas will become less habitable, potentially causing large scale migrations that trigger social unrest and disrupt economic activity.

2. Transition risk – risks arising from the economic, political and market changes as part of the move to a low-carbon economy, that is, an economy with significantly lower emissions of greenhouse gases due to much lower fossil fuel use and possibly negative emission technologies such as carbon capture and storage.

   Sources of transition risk include:

   - policy measures (*eg* carbon taxes and energy efficiency standards)
   - technological change (*eg* a move to renewable energy and electrical vehicles)
   - changing customer preferences (*eg* increased demand for 'green' products).

3. Liability risks – relate to the potential costs from injured third parties seeking compensation because they have suffered loss or damage from the impacts of climate change.

   An increasing number of lawsuits are being brought, albeit with limited success so far. It is possible that actuaries and their clients could face legal claims themselves in future if they fail to consider climate-related risks.

4.2 Modelling climate risk

There is widespread concern among policymakers and financial regulators of the damage that climate change could cause to the financial system and, conversely, the role that the financial system can play in achieving an orderly transition to a low carbon economy.

Question

Outline how the financial system (*eg* investors, providers and regulators) can influence the transition to a low carbon economy.

Solution

- Investors can increase investment in green technologies, renewable energy sources, sustainable transport …

  … and decrease investment in companies with high levels of emissions, such as fossil fuel producers, manufacturing companies.

- Investors can engage with the management of investee companies to help put pressure on them to reduce emissions …

  … or to support them in transitioning, *eg* to using lower carbon energy sources.

- Banks can redirect financing (loans) to sustainable projects.
- Asset management companies can offer 'low carbon' investment bonds.
- Corporations can issue 'green' bonds.
- Credit rating agencies can incorporate environmental, social and governance (ESG) factors into their assessment of the creditworthiness of organisations.
- Index providers can construct 'low carbon' indices, to enable the benchmarking of fund performance and to provide a basis for passive trackers.
- General insurance companies can introduce exclusion clauses, increase premiums, or refuse to underwrite risks that are deemed damaging in respect of climate change.
- Governments can introduce policies and tax incentives to drive investments in a more environmental direction …

  … as well as establishing public-private partnerships to advance sustainable economic development by providing finance and risk management tools.

- Regulators can require financial providers to hold solvency capital in respect of climate change risk …

  … and to disclose their approach to managing climate change risk.

In May 2017, the IFoA issued a risk alert highlighting that actuaries are expected to consider climate risks and communicate their approach.

This risk alert advocates that actuaries should consider the following, when providing advice:

- all investors should consider the potential implications of climate-related risks on their invested assets
- institutions with short-term liabilities (*eg* general insurers and re-insurers) should evaluate and manage the impact of extreme weather
- institutions with long-term liabilities (*eg* life insurers, re-insurers and pension funds) should evaluate and manage the impact of changing patterns of temperature and disease on mortality and morbidity
- institutions with unfunded or partially funded liabilities should evaluate and manage the impact on the covenant of the sponsor or other funding bodies.

A particular challenge is that the future may look very different to the past, so models that are calibrated using past data may give misleading results. Modelling the potential financial impacts of physical and transition risks is a major focus of current research. The quantification of these impacts is challenging because of the multiple levels of uncertainty. Not only is there uncertainty about the climate system itself and how it will respond to increasing atmospheric concentrations of greenhouse gas emissions, but there is much uncertainty about future levels of greenhouse gas emissions. These will depend on the responses of governments, regulators, businesses and individuals, both to climate change targets and to technological and economic developments.

The uncertainty means a wide range of possible outcomes and there are many different pathways that lead to similar climate outcomes yet have different economic impacts. For example, a long-term equilibrium rise in global average temperatures of (say) 3°C relative to pre-industrial times might arise from various different trajectories of energy consumption levels and mix of energy sources.

The Taskforce for Climate Related Financial Disclosures (see Module 13) recommends that organisations use scenario analysis as a tool for understanding the drivers and strategic implications of climate-related risks and opportunities. Scenario analysis can be used to assess the impact of a range plausible future hypothetical scenarios, and can allow for interactions between combinations of physical, transition and liability risks.

Assessing climate change risk

Assessing climate change risk is particularly challenging since:

- the future may look very different to the past, so models that are calibrated using past data may give misleading results
- there are multiple levels of uncertainty in the climate system itself, levels of greenhouse gas emissions and the reactions of various stakeholders to climate change targets and technological / economic developments
- there are many different pathways that lead to similar climate outcomes yet have different economic impacts.

The practice questions start on the next page so that you can keep the module summaries together for revision purposes.

Module 25 Practice Questions

25.1 An insurance company has just sold one-year term assurance contracts, each with a sum assured of £350,000, to a group of 100 healthy lives of the same age.

Calculate the probability it will have to pay out £1 million or more in respect of these policies for:

(i) the lives aged 50, where $q_{50} = 0.002$, and

(ii) the lives aged 60, where $q_{60} = 0.008$.

25.2 Compare the nature of funding liquidity risk in a life insurance company to that in a bank.

25.3 (i) Define liquidity risk in respect of a financial institution. [2]

Exam style

(ii) Outline the actions that a bank should include in a liquidity crisis contingency plan. [3]

XYZ bank has categorised its assets and liabilities by time to maturity as follows (figures in $*m*):

Maturity bucket	*Assets*	*Liabilities*
1 day	-	-
1 day – 3 months	2,388	3,330
3 months – 6 months	3,770	10,680
6 months – 1 year	5,341	8,954
1 year – 5 years	19,164	7,854
over 5 years	29,060	26,704

(iii) By considering the liquidity gap at each duration, assess XYZ's liquidity position. [4]

ABC bank's balance sheet is as follows:

Assets	*$m*
Cash	785
Trading assets	3,142
Investment assets	2,356
Loans to banks	16,965
Loans to customers	48,223
Other assets	628
Total assets	72,099

Liability & Equity	*$m*
Deposits (instant access)	21,991
Deposits (limited access)	13,509
Term deposits	30,316
Other payables	1,257
Short-term borrowings	628
Shareholder's equity	4,398
Total liabilities and equity	72,099

(iv) Using appropriate ratios, assess ABC's liquidity position. [6]

[Total 15]

The solutions start on the next page so that you can separate the questions and solutions.

Module 25 Solutions

25.1 We need to find the probability of at least 3 deaths occurring during the year, ie the probability that a $Binomial(100, q_x)$ distribution takes a value of at least 3. For a life aged x, this can be calculated from the complementary probability (the probability of getting a value less than 3) as:

$$1-\left\{(1-q_x)^{100}+\binom{100}{1}q_x(1-q_x)^{99}+\binom{100}{2}(q_x)^2(1-q_x)^{98}\right\}$$

(i) if $q_{50}=0.002$, this gives $1-(0.8186+0.1640+0.0163)=0.0011$

(ii) if $q_{60}=0.008$, this gives $1-(0.4479+0.3612+0.1442)=0.0467$

25.2 Funding liquidity risk is the risk that a company cannot raise the cash to pay its liabilities as they fall due.

Many believe the roots of the 2007-08 credit crisis lie in liquidity risk.

To analyse liquidity risk we need to look at:

- the marketability of the assets and how this could change in a crisis
- the term of the liabilities and the chance that they could be called before term.

Life insurance company

Assets of life companies are generally invested globally and diversified across many different asset categories. Many of these are illiquid such as property, unquoted shares, corporate bonds and preference shares, and even private equity. However, the vast majority of these assets are readily saleable, and even in the event of a global crisis, not all of these assets will become unmarketable.

The liabilities are generally long term (endowment policies, pension policies, *etc*) and many have no option to cash in the liability prior to term. In some cases, risks do exist but are relatively small:

- for example, an endowment policy can be surrendered, but the terms are generally not guaranteed
- unit trust holders can sell their units at any time, but these assets are held separately and are generally more marketable.

There is therefore little liquidity risk.

Bank

The assets of a bank can be longer term and illiquid (for example, mortgages extended to homeowners for up to 25 years, corporate loans, car finance *etc*.

Generally speaking, liabilities are much shorter term, for example deposits and wholesale market funding from other banks.

There is therefore significant liquidity risk.

Banks have overcome this problem in the past through a mixture of:

- lending shorter term
- increasing the capital held in reserve
- developing the ability to repo the bonds that they hold
- developing the ability to securitise certain illiquid assets to raise cash.

As seen recently, in a crisis market situation, some of these sources cannot be relied on.

25.3 (i) ***Liquidity risk definition***

Funding liquidity risk is the risk that a financial institution will incur losses because of an inability to obtain funds to meet expected and unexpected current obligations as they fall due (or at least without excessive cost) or, more broadly, an inability to manage of short-term cashflow requirements. [1]

Market liquidity risk is the risk that a financial institution will incur losses because of insufficient capacity in the market to handle asset transactions at the time when the deal is required (without a material impact on price). [1]

[Total 2]

(ii) ***Liquidity contingency plan actions***

- Report information on cash movements to senior management in a timely manner.
- Set out clear accountability on who is responsible for managing a liquidity crisis.
- Put a plan in place to adjust mix / nature of assets and liabilities.
- Secure back-up sources of funding identified and secured (*eg* contingent equity, such as cat-e-puts).
- Understand bank's ability to limit cash outflows (*eg* contract terms allowing suspension of withdrawal from deposit accounts).
- Categorise bank's borrowers and trading partners in terms of their priority for settlement.

[½ each, maximum 3]

(iii) ***Liquidity gap analysis***

Maturity bucket	*Assets*	*Liabilities*	*Liquidity Gap*	***Cumulative Gap***
1 day	0	0	0	**0**
1 day – 3 months	2,388	3,330	–942	**–942**
3 months – 6 months	3,770	10,680	–6,910	**–7,852**
6 months – 1 year	5,341	8,954	–3,613	**–11,465**
1 year – 5 years	19,164	7,854	11,310	**–155**
over 5 years	29,060	26,704	2,356	**2,201**

[2 for final column]

Using this approach, over a one-year period, the XYZ's assets are insufficient to cover the liabilities due (it has a gap of –\$11,465*m*). Beyond 5 years, the liquidity position has improved (assets exceed liabilities by \$2,201*m*). [1]

The actual liquidity position may be slightly better / worse than this as:

- the categorisation into such broad maturity buckets is relatively crude
- the timings of some asset and liability cashflows may be unknown / variable
- the analysis ignores the ability to liquidate assets early
- assets may be worth less under a market liquidity stress scenario. [½ each]

[Maximum 4]

(iv) ***Liquidity analysis***

Liquidity ratio

Liquid assets = 785 + 3,142 = 3,927, and short-term liabilities = 21,991 + 13,509 = 35,500.

Liquidity ratio = liquid assets / short-term liabilities = 3,927 / 35,500 = 11.06% [1]

This is very low. ABC's liquid assets only form a small proportion of its short-term liabilities. [½]

The ratio would be expected to be in excess of 100% (*ie* short-term assets should exceed short-term liabilities). [½]

Net loans to net assets ratio

Loans = 16,965 + 48,223 = 65,188, and total assets = 72,099.

Ratio of loans to assets = 90.4% [1]

ABC's ratio is very high, showing it has a high proportion of its assets tied up in illiquid loans. [1]

A low ratio shows a good liquidity position. [½]

Loans to deposits ratio (LTD)

Loans = 65,188, and deposits = 21,991 + 13,509 + 30,316 = 65,816.

Ratio of loans to deposits = 99% [1]

This ratio indicates how heavily ABC's loans (non-liquid assets) are funded by deposits (liquid liabilities). [½]

At almost 100%, ABC is relying almost entirely on its deposits to finance its loans. [½]

Such deposits may be very volatile, with the instant access and limited access deposits particularly vulnerable (*eg* during a run on the bank) and these account for over half of the total deposits book. [½]

[Maximum 6]

[Award marks for other suitable liquidity ratios and comments, 1 per calculation and ½ per comment, maximum 2 per ratio]

3.2 Risk transfer

Risk transfer may also be known as *reassigning risk* or *deflecting risk*.

Risk transfer strategies involve passing the risk in question to another organisation, or another part of the same organisation.

There are several ways in which risks can be reduced through transfer, *eg* through:

- insurance
  - provides capital if an event occurs (known as *contingent capital*) in return for a premium
- **reinsurance**
- **co-insurance**
- **sharing the risk with a policyholder via product design**
- **securitisation**
  - packaging risk into a marketable investment
- **purchase of some forms of derivative**
- *alternative risk transfer (ART) products*
  - combine features of derivatives and insurance and are discussed in detail in later in this module
- outsourcing.

A common form of risk transfer within insurance is a policy excess or co-payment, which returns some of the risk to the policyholder.

Risk transfer must be based on a good mutual understanding of each of the parties' objectives. It must also recognise the ability of the party assuming the risk to take action and understand the context of the risk, and it must be cost-efficient.

Cost Risk transfer normally has a cost over and above the expected loss. This cost represents the reward that the party to whom the risk is transferred requires in order to accept that risk, and potentially also to contribute to their own profit. Furthermore, if risks are transferred then the cedant (the party transferring the risk) not only has removed the potential for downside exposure, but may also have removed the potential for upside.

Some risk transfer designs can preserve some or all of the upside (*eg* some derivatives, or profit-sharing arrangements within reinsurance treaties) but this will increase the cost.

Capacity

The effectiveness of transfer as a risk response might also be constrained by the capacity of the 'market' to which it is being transferred. For example, there may not be capacity (or appetite) in the reinsurance market to accept significant quantities of longevity risk on immediate annuities.

Counterparty risk

Risk transfer by definition involves a third party, such as an investment bank or reinsurer, and thus introduces counterparty risk. For example, the failure or default of a reinsurance company will return the risks to the cedant.

Liquidity risk

Risk transfer can introduce liquidity risk. For example:

- under a reinsurance arrangement, there is a risk that the reinsurer delays the settlement of claims, causing a liquidity strain for the ceding insurer
- under exchange-traded derivatives contracts, there is a risk that margin calls are higher than expected or required at inopportune times.

Regulatory / operational constraints and governance issues

There may be regulatory restrictions that reduce the effectiveness of risk transfer. For example, there might be a maximum permissible amount that can be transferred to a single counterparty. Or the permitted reduction in regulatory capital may be capped for some forms of transfer, which can reduce the attractiveness of such options.

Even if there are no regulatory constraints, there may be internal constraints or considerations. For example:

- contract terms and conditions may limit the amount of transfer that can take place
- the transferring organisation will need to assess whether it has the requisite expertise to execute the risk transfer, and subsequently to monitor its effectiveness
- the volume and type of risk transfer needs to be commensurate with the organisation's risk appetite / tolerances.

Question

Outline characteristics of ERM (as distinct from traditional RM) that aid the risk transfer process.

Solution

ERM can aid the risk transfer process by:

- providing a framework in which:
  - an organisation's net exposure to each type of risk can be assessed and diversification of risk can be recognised, so avoiding the costs of over hedging
  - the costs of different risk transfer strategies can be assessed
- helping to establish *consistent* risk transfer policies across an organisation.

Module 26 Summary – Risk optimisation and risk responses

Risk control

Risk management is not simply about minimising risk. Risk management can optimise the risk / return profile of the organisation, with respect to its risk appetite, by:

- supporting selective growth of the business
- supporting profitability through risk-adjusted pricing
- using limit setting to control the size and probability of potential losses
- employing techniques to manage existing risks.

Portfolio management techniques and ERM

Five fundamental concepts in risk portfolio management are:

1. risk
2. reward
3. diversification
4. leverage
5. hedging.

Measures of return that reflect the risk taken to achieve the return, include:

- RAROC – can be based on actual or expected return and capital
- the Sharpe ratio – a measure of out-performance of a portfolio per unit of risk.

Organisations need to adopt a risk optimisation strategy which can be aligned to shareholder expectations.

Mean-variance portfolio theory (MVPT):

- can be extended to any portfolio of risks, *eg* an organisation's projects
- states that optimal combinations of risky assets can be determined without any knowledge of the investor's preferences towards risk and return (the separation theorem)
- states that the investors' choice from the set of efficient portfolios will be determined by their risk appetite or, equivalently, their utility function.

Applying active portfolio management:

- encourages companies to 'unbundle' the business into component projects
- provides a mechanism for aggregating risks across the business
- provides a framework in which risk concentration limits and asset allocation targets can be set
- influence investment, transfer pricing and capital allocation decisions.

Although there is little evidence that active portfolio management adds value, passive management is not an option because there is no appropriate (project) index to track.

Risk responses

The key types of risk response:

- rejection (avoidance / removal)
- acceptance (retention)
- transfer
- management (treatment / reduction without transfer).

Good risk responses are economical, well matched to the risk, simple, active, flexible and dynamic.

Residual risks result from: decisions to retain risks, secondary risks, imperfect hedges, and/or an inability to transfer or fully mitigate risks.

Risk transfer

Risk can be transferred:

- to another part of the same organisation
- to another party, *eg*: insurance, sharing with the policyholder, ART, outsourcing.

Considerations when transferring risk include cost effectiveness, loss of upside potential, market capacity, counterparty risk, regulatory and operational constraints, risk governance issues.

Risk reduction without transfer (risk management, risk treatment, risk mitigation)

Risks can be reduced without transfer by:

- taking on uncorrelated (or negatively correlated) risks
- increasing the size of a portfolio
- greater matching of assets and liabilities
- implementation of strong internal controls and governance
- robust underwriting practices, analysis using appropriate homogenous groupings and taking into account both past and likely future trends
- robust due diligence practices, and tightly worded agreements
- remuneration and bonus systems that align agents' interests
- increased capital or funding.

Risk acceptance (risk retention, absorbing risk, tolerating risk)

Risks may be accepted by an organisation if:

- the risk is trivial
- taking the risk is a component of its core business
- it appears to be the most economical approach
- it acts as a diversifier to another retained risk
- there is no alternative.

ART

ART products are non-traditional risk transfer products which often combine features of both (re)insurance products and financial risk protection products utilising the capital markets (*eg* derivatives).

ART may:

- improve the focus on core business, and capital efficiency
- provide a quick and potentially more tailored solution, although more complex and bespoke arrangements can take time to develop
- reduce total costs, although they may involve higher initial costs
- stabilise earnings
- help establish a market price for risk
- simplify administration by reducing the number of risk transfer arrangements, although the use of ART could potentially increase operational risks, and changes may need to be made to methods of risk assessment and management to accommodate its use.

The practice questions start on the next page so that you can keep the chapter summaries together for revision purposes.

Futures are standardised and they are only available on a limited set of underlying assets. Hence it may be difficult to match the risk exactly. If the asset whose price is to be hedged is not exactly the same as the asset underlying the futures contract then the resulting basis risk is known as *cross hedging risk*.

Basis risk reduces to zero as expiry approaches if there is no cross-hedging risk and no uncertainty as to the associated cashflows (income, benefits or costs).

Example

An asset is currently held but must be sold in one year's time at the then market price. The market risk is to be eliminated using a hedge.

A futures contract is available, on the same underlying asset, but with two years to expiration. There are no associated cashflows (income, benefits or costs) other than the payment of margin.

A hedge is established by entering into a short position in this futures contract now ($t=0$). One year later (*ie* at $t=1$) the underlying asset is sold and the hedge is closed out (by entering into an offsetting long position in the same futures contract, the clearing house then recognising and cancelling the two matched opposite positions).

The associated cashflows are as follows:

	Actual cashflow at time 1	**Total cashflows under the contract, if held to expiry, *ie* to time 2** (see note below)
Short futures position (established at time 0)		$F_0 - F_2$
Long futures position (established at time 1)		$F_2 - F_1$
Sell underlying at time 1	S_1	
Total (see note below)	$F_0 - F_1 + S_1 = F_0 + B_1$	

Hence the position exposes us to basis risk, as the total cashflow is a function of the uncertain basis at $t=1$.

Note that in summing up these cashflows we (like Sweeting) are ignoring the marking to market process and the time value of money!

2.8 The number of contracts required for a hedge

In theory, in the absence of basis risk, the number of contracts required in order to hedge a particular position is simply the ratio of the number of units being hedged (or the value of the portfolio being hedged) divided by the number of units underlying the futures contract (or the value of the futures contract). The approach differs depending on whether we are dealing with a commodity future or a financial future.

Commodity future example

Airlines have significant fuel needs and are highly exposed to the risk of changes in aviation fuel prices. Many airlines attempt to protect against excessive future fuel bills by buying fuel derivatives. Historically, there was no thriving *aviation fuel* futures market, so aviation fuel was mainly hedged with *heating oil* futures. This is because the price of heating oil moves in almost the same way as the price of crude oil (although it also allows for the costs and capacity constraints in the oil refining process).

Below, we calculate the number of futures contracts required for a hedge. Let:

- N_Y be the number of barrels of oil being hedged
- N_F be the number of barrels of oil underlying one futures contract.

In the absence of basis risk, the number of futures contracts required for the hedge, N_h is:

$$N_h = \frac{N_Y}{N_F}$$

However, since the (heating) oil underlying the futures contract is not an exact match to the aviation oil being hedged , we need to adjust the number of futures contracts by the 'optimal hedge ratio', h , which is calculated as follows:

$$h = \rho \frac{\sigma_Y}{\sigma_F}$$

where:

- σ_Y is the volatility of the per-unit price of the oil being hedged
- σ_F is the volatility of the per-unit price of the future
- ρ is the coefficient of correlation between the two prices.

Hence, allowing for basis risk, the number of futures contracts required for the hedge, N_h is:

$$N_h = h \frac{N_Y}{N_F}$$

Financial future example

For index futures, we adopt a similar approach to above but using the beta of the portfolio being hedged, *ie* the number of futures contracts required for the hedge, N_h , is:

$$N_h = \beta_Y \frac{V_Y}{V_F}$$

where:

- V_Y is the value of the portfolio being hedged
- V_F is the value of one futures contract (being the index level multiplied by the contract multiplier (see example below)
- β_Y is the beta of the portfolio being hedged relative to the index underlying the future.

Question

An investor has a portfolio of equities worth £1.5m. The investor is looking to hedge the portfolio with a FTSE-100 index future. The index is currently at 7,500 and the contract multiplier is £10 per index point. The beta, β_Y, of the portfolio relative to the FTSE-100 index, is 1.6.

Calculate the number of FTSE-100 index futures contracts required to hedge the portfolio optimally.

Solution

The contract value is determined by taking the product of the contract multiplier (£10 per index point) and the index value (7,500).

The optimal number of FTSE-100 index futures contracts that should be shorted in order to hedge the portfolio is therefore given by:

$$N_h = \beta_Y \frac{V_Y}{V_F} = 1.6 \frac{£1,500,000}{7,500 \times £10} = 32$$

2.9 Managing foreign exchange or currency risk

Currency hedging may employ one or more of the following:

- *currency forward* – the company may agree to buy/sell foreign currency at an agreed rate at a future date. The pricing of the forward is based on the current (*spot*) rate of exchange adjusted for the difference in interest rates between the two currencies. The company will know the rate of exchange on its cashflows and will not suffer from any deterioration in rates, but equally it will not benefit from any improvement.
- *currency swap* – effectively a series of currency forwards
- *currency future* – similar to a currency forward but traded via an exchange
- *currency option* – in return for a premium, the company buys the right, but not the obligation, to buy/sell foreign currency at an agreed date for an agreed price. This allows the company to lock into an exchange rate but benefit from any beneficial changes in exchange rates.

Question

Outline why currency exposures are typically hedged in respect of overseas bonds but are not hedged in respect of overseas equities.

Solution

Taking currency risk does not provide any additional systematic return. Hence, for overseas bonds, currency exposures are typically hedged (unless a particular view of likely currency movement is held). However, for overseas equities the situation is more complex (*eg* due to the need to establish net exposures) and so hedging is either approximate or not attempted.

Note that the *purchasing power parity* theory of exchange rates suggests that, in the long-term, exchange rates change in line with the difference in the inflation rates of the two relevant economies − thus mitigating the need to hedge currency risk.

Rather than use derivatives, it is also possible to use cashflow management techniques to manage currency risk, such as:

- *netting* – the company uses revenue in a particular currency to meet any amounts owing in the same currency. The cashflows are unlikely to match exactly and any residual amount may need to be hedged using alternative techniques.
- *leading and lagging* – the company may attempt to bring forward (*lead*) or delay (*lag*) foreign currency cashflows in order to exploit expected movements in exchange rates.

3 Management of other risks

The following material considers the management of liquidity, systemic, demographic, insurance and environmental risks.

Liquidity risk

Managing liquidity risk requires a company to actively monitor its liquidity requirements (*ie* it must know how much cash it will need in the short / medium term and check it has sufficient cash-like assets).

This monitoring must be both within and across legal entities. The differing transferability of liquidity assets (or *fungibility)*, due to exchange and other regulatory barriers, is a particular difficulty for multi-nationals.

Question

Describe three methods of managing *market* liquidity risk, and three methods for managing *funding* liquidity risk.

Solution

Market liquidity risk can be managed by:

1. varying investment strategy
2. using swaps
3. having a contingency fund consisting of high-quality, liquid assets.

Funding liquidity risk, a particularly important issue for banks, should be considered alongside credit risks. It can be managed by:

1. diversifying sources of funding (by type and term)
2. continuously monitoring the ability to raise additional capital
3. contingency sources of funding from their bank (*eg* a line of credit) to draw upon in times of stress.

Systemic risk

As discussed in the previous module on managing credit risk, a business can manage some systemic risks by ensuring it deals with a wide range of counterparties (thereby avoiding concentration). Internal limits can ensure undue exposure to a specific counterparty / industry sector is limited.

Question

Describe examples of activities designed to reduce or eliminate *feedback risk* (the spread of risk through a financial system).

Solution

Activities designed to reduce or eliminate feedback risk (the spread of risk through a financial system) include:

- investing only in exchange-traded instruments, so as to pool (diversify) counterparty risk
- suspension of trading on the stock exchange by *circuit breakers* if there is a large market movement (*cf* Lam page 242 'Knight Capital')
- governments or central banks intervening to prop up a bank (by acting as a lender of last resort), or reduce financial consequences (*eg* by reducing interest rates)
- regulations that require establishment of additional reserves (*eg* Basel III requires companies to build up additional reserves in the 'good times')
- avoiding regulations that increase pro-cyclicality, *eg* solvency regulations that encourage all similar organisations to adopt similar investment and risk-mitigation strategies
- physically separating types of businesses (*eg* the separation of investment banking and retail banking under the US 1933 Glass-Steagall Act, which was repealed but is now being actively pursued following the Global Financial Crisis).

Demographic risk, non-life insurance and environmental risks

Demographic and other insurance risks can be managed:

- before the risk is accepted, *eg* through underwriting
  - by applying exclusion clauses (or in the extreme, rejecting the application)
  - by increasing the premiums charged / reducing the benefits promised
  - by imposing excesses
  - through no-claims discount systems
- after the risk has been accepted:
  - by transferring the risk, *eg* through reinsurance, purchasing annuities, a longevity swap, securitisation
  - through reduced risk concentration, *eg* by growing the business
  - through improved diversification, *eg* by business line, risk factor
  - through implied hedging, *eg* of mortality and longevity risks.

Many of the Alternative Risk Transfer (ART) products described in Module 26 are designed to manage these risks.

1 Capital

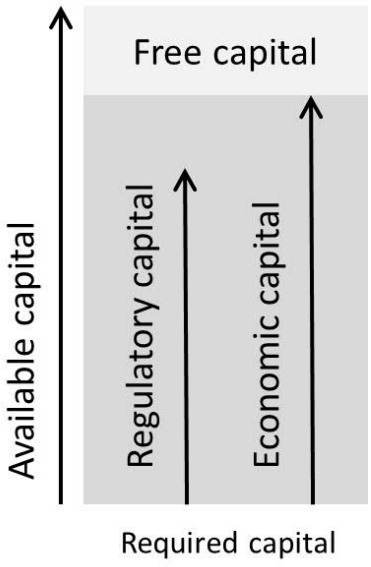
1.1 Definitions of capital

The capital that an organisation has access to acts as a buffer in the event the organisation faces risks that impact its balance sheet. Allowing for differences between various valuation bases, it corresponds to an item that might be known by a variety of terms, including as *Net Asset Value*, *Shareholders' Funds*, *Free Assets*, *Free Reserves*, and *Own Funds*. Whichever name it is known by, it effectively corresponds to capital that 'belongs' to the stakeholders who provide capital, and is not expected to be needed if events turn out according to the central estimates of the organisation.

It may help to think back to Subject CB1, and the makeup of the balance sheet, where capital is the assets less the liabilities. This capital is also known as 'available' capital, and comprises items such as ordinary share capital, retained earnings, revaluation and other reserves.

Unless the organisation is under material financial distress, the capital available is usually significantly above the regulatory and economic capital that might be calculated by an economic capital model.

Here, a distinction is being made between capital that is *available* to an organisation and capital that the organisation is *required* to hold. This requirement may be driven by the regulator (regulatory capital) or internally by the organisation (economic capital). These two assessments of required capital may be different and the reasons for this are discussed later in this module. Any available capital in excess of the required capital is generally referred to as free capital. The following diagram illustrates how the different types of capital link in with each other.



1.2 Economic capital

In this chapter we are mainly concerned with *economic capital* (or *risk capital*), or simply '*capital*'.

Although there are many different definitions of capital in use, there are some common threads:

- capital should provide sufficient surplus to cover *adverse outcomes*
- with a given level of *risk tolerance*
- over a specified *time horizon*.

Question

State three definitions of capital that result from the three main interpretations of the meaning of 'adverse outcomes' (above).

Solution

The three main interpretations of 'adverse outcomes' result in the following definitions of capital:

1. the surplus needed to cover all potential outgoings, reductions in assets and/or increases in a company's liabilities at a given level of risk tolerance over a specified time horizon
2. the surplus needed to maintain a given level of solvency at a given level of risk tolerance over a specified time horizon
3. the excess of the value of the assets over the value of the liabilities at a given level of risk tolerance at a specified time horizon.

Unlike the first two definitions, the third definition above focuses on the values of the assets and liabilities *at* the specified time horizon – rather than the funding position (cashflow or surplus) of the company *throughout* the time period concerned.

Question

State three metrics that might be used to set an appropriate level of risk tolerance.

Solution

The appropriate risk tolerance level might be set with reference to:

1. a certain *percentile* of the loss distribution
2. extreme loss *values*
3. the possibility of some key *indicator* (*eg* credit rating) falling outside an acceptable level.

All assets are taken at *fair value* (normally market value). Broadly, the company's capital consists of the excess of its assets over its liabilities and is classed as tier 1, 2 or 3 depending on how readily the capital can be called upon if required.

Solvency Capital Requirement (SCR)

The SCR must be achievable with 99.5% confidence over a one-year time horizon and may be based on a *standard formula*, or on a firm's approved *internal model*.

Question

Outline the basis of the standard formula, and the standards that any approved internal model must satisfy.

Solution

The standard formula:

- is based on a specific deterministic basis but with some stochastic elements (*eg* for the valuation of guarantees)
- deals with market risk through limited admissibility of some assets, plus a number of stress tests (*eg* a fall in equity returns, changes in interest rates)
- deals with credit risk through limiting exposure to individual counterparties (*eg* reinsurers)
- deals with underwriting risk by requiring additional solvency margins, generally calculated by reference to business volumes (*eg* premiums) or risks (*eg* claims incurred, sums assured).

The internal model must satisfy certain standards including:

- a *use test, ie* the company must actually use the model in its decision making and risk management systems
- statistical quality standards – to ensure assumptions are realistic and reliable
- calibration standards – to ensure the output can be used to properly calculate the SCR
- profit and loss attribution
- validation standards
- documentation standards.

Example

Under the standard formula, the SCR for certain risk types is calculated using stress tests. For each risk, the insurance company determines the company's balance sheet on an unstressed (best estimate) basis and then on a stressed basis. The undiversified SCR for each risk is the difference between the net asset value, $V_0(A) - V_0(L)$, on the unstressed basis and the net asset value, $V_1(A) - V_1(L)$, on the stressed basis.

Below is an example of how we might calculate the SCR in respect of equity risk for an insurance company that sells a mixture of conventional and unit-linked contracts. We assume a stress comprising a 40% fall in equity values (although in practice, the stress may be a different percentage). We assume that the unstressed balance sheet is as follows:

- $V_0(A) = £100m$ (of which £50m in equities)
- $V_0(L) = £60m$
- net asset value, $V_0(A) - V_0(L) = £40m$

We then conduct an equity stress test, assuming that equity values fall by 40% over the next year. The stressed balance sheet may be as follows:

- $V_1(A) = £80m$ (reflecting a reduction of 40% of £50*m*)
- $V_1(L) = £45m$ (we have assumed here that some of the liabilities are unit-linked and their value has also fallen)
- net asset value, $V_1(A) - V_1(L) = £35m$

The undiversified SCR in respect of equity risk is the difference between the net asset values, *ie* £40*m* – £35*m* = £5*m*.

Minimum Capital Requirement (MCR)

The MCR is €3*m* plus a margin based on premium or reserve amounts. The MCR must be achievable with 80 – 90% confidence over a one-year time horizon. Failure to maintain the MCR would result in withdrawal of the company's authorisation.

The qualitative requirements of Pillar 2 were described in Module 5.

The *hurdle rate* of return on capital is a standard against which an organisation's activities must be measured. If a proposed activity does not offer a RAROC above the hurdle rate then that is one basis upon which it might be rejected.

EIC can be used in setting performance targets and executive remuneration.

Question

Outline two key factors to be considered when determining an appropriate hurdle rate.

Solution

The hurdle rate should:

1. reflect the cost of capital (*eg* WACC was considered under project appraisal in Subject CB1)
2. allow not only for the risks inherent within a proposal, but also the degree to which those risks diversify (or hedge) existing risks.

Shareholder value (SHV) and Shareholder value added (SVA)

Unlike RAROC and EIC, SHV and SVA assess the intrinsic economic value of an organisation as a going concern (*ie* over an extended period).

SHV captures the present value of all future cashflows (*ie* a perpetuity):

$$SHV = discounted\ value\ of\ all\ future\ cashflows$$

$$= capital \times \left(\frac{RAROC - g}{hurdle - g} \right)$$

where: g = prospective future growth rate of the organisation (usually over three to five years).

SVA measures the extent that SHV exceeds the capital invested:

$$SVA = Discounted\ value\ of\ economic\ value\ added$$

$$= capital \times \left(\frac{RAROC - g}{hurdle - g} - 1 \right)$$

4 Capital allocation

This section considers a situation where an organisation has used a model and risk analysis to calculate the required capital at the overall level.

Why allocate capital?

As discussed in the previous section, the shareholders or equivalent stakeholders who provide capital expect the organisation to earn a return on their capital by undertaking business activities.

Consider the RAROC measure:

$$RAROC = \frac{risk\text{-}adjusted\ return}{capital}$$

An organisation with too much capital will make a smaller return on capital employed than it might otherwise do, and possibly a smaller return for the amount of risk it is taking than the shareholders or equivalent expect.

This has two consequences:

1. **First, the organisation needs to have specific plans to make a return to the shareholders or equivalent, usually as dividends, to ensure that it does not operate with more capital than it can effectively use.**

   In general, returning capital that is not being used effectively, will increase the organisation's (aggregate) RAROC, by reducing the denominator proportionately more than it will impact the numerator.

2. **Second, the organisation needs to allocate capital to business operations. Different lines of business have different risk levels, and so need to be supported by different levels of capital.**

   For RAROC to be a measure by which different business operations of the organisation can be compared in a fair and meaningful way, the denominator of the RAROC must reasonably reflect the exposure to risk that that business operation presents to the organisation.

   For example, take an organisation with two business operations, each delivering the same risk-adjusted returns but with very different risk exposures. If the capital allocation is even (*ie* 50:50) then the RAROC of each business operation is the same, providing senior management with no basis upon which to distinguish between the two. However, the business operation with the lower risk exposure is actually more capital efficient.

   By adjusting the allocation (using methods such as those discussed later in this section), fairer and more meaningful RAROC metrics can be used to inform management decisions. For example, a decision might be made to adjust prices and/or business volumes to optimise capital efficiency. Hence RAROC is a function of the choice of method of allocating capital.

The textbook reading and the remainder of this unit outline some of the considerations that organisations make when they decide how to allocate capital.

What capital should be allocated?

There are many different ways of allocating capital, and of deciding on what capital to allocate. Sweeting (page 488) implies by his use of the word, 'requirement', that an organisation should allocate the economic or regulatory capital, but this leaves the question open as to what the organisation should do with the difference between actual capital and this requirement.

In other words, what should be done with the free capital? Should this also be allocated or retained centrally?

How should capital be allocated?

The next question is then how this should be translated in a fair way into capital requirements at the level of individual business units, products or other 'segments'. This can be important for business planning, performance measurement (return on capital) and pricing purposes.

There is likely to be no single way of achieving this allocation of capital, with a combination of methodologies generally resulting in a better overall approach.

Note that we are generally (*) considering a *notional* allocation of *risk capital* (which itself is an output from a model). It is not a *physical* distribution of *money* (in the sense of *working* capital).

Nevertheless, the (notionally) allocated capital amounts are important, as the values are then applied to management processes, which in turn will have a significant impact on business decision-making. For example, total allocated capital (being a measure of risk) may be used as a basis for: pricing, risk control limits, performance measurement, *etc.*

(*) *An exception is if we are looking at allocation across regulated entities (eg different geographies) – then capital will be physically allocated (but then each entity will have it is own regulatory capital requirement and allocation issues).*

Question

Explain how the allocation of capital affects pricing, risk control limits and performance measurement.

Solution

The capital allocation process should be set up to link risk to performance measurement, *eg* a business unit's success should be measured relative to the risk it takes in its operations, which should in turn reflect the amount of capital the company is willing to allocate to the business unit.

The amount of capital that is allocated to each business unit:

- determines the business unit's performance (as measured by RAROC, for example)
- could affect, directly or indirectly, the remuneration of the unit's managers and, consequently, their level of motivation and behaviour
- may dictate the amount of business the business unit can write (as each policy written consumes capital and the total amount of capital is limited)
- determines, in part, the price at which business can be written (*eg* a minimum price might be determined by a stipulated minimum RAROC).

4.1 Allowing for concentration / diversification of risk

Any method of allocation needs to allow for concentration / diversification of risk between the business units. In particular, not all business areas have the same degree of risk. Some allocations of capital may result in the less risky areas subsidising the riskier areas.

Adjustments for correlation and dependency

At an aggregate level most approaches to the evaluation of the capital requirement and its allocation to different units involve taking into account correlation and dependency.

In making these adjustments it is important to remember that the level of dependency between different lines of business and risk categories might be different during times of stress from those experienced under normal conditions.

As required capital is typically calculated with reference to extreme events, tail dependency will have to be considered carefully. It is often then case that total required capital as well as the related capital allocation is very sensitive to the choice of dependency structure (*eg* copula) used to aggregate the risks.

Diversification benefit

For any business with a number of different areas, unless all risks are perfectly correlated with each other, the total capital required will be less than the sum of the capital over all individual risky projects.

This *diversification benefit* can be shared across the business. The company must decide how to allocate capital across the different areas of the business.

Some approaches to capital allocation calculate capital required for each business unit and/or risk category followed by an adjustment for the benefit of diversification. This adjustment is retained at the level of the enterprise and not passed on to the individual units.

An alternative approach is to calculate the capital required at the level of the enterprise, and then to allocate this capital in a fair way across all units, including the diversification benefit (see next section).

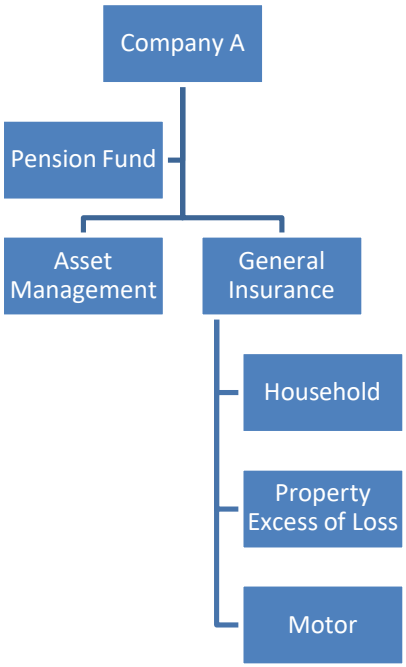
Different organisations will make different decisions as to how to solve the problems posed by this module. What is important is that the solutions are clearly articulated and consistently understood.

In the next section we consider some of these problems posed, and the decisions that need to be made via an example.

4.4 Example

The process of allocating capital can easily be the most challenging process undertaken by a risk modelling unit. To explain why, let us consider a notional Company A. This company runs an asset management business that accepts third-party institutional funds as well as managing the company's own investments. Its main business is as a general insurer, writing household, property catastrophe excess of loss, and motor lines. It also sponsors a legacy defined benefit pension fund, which is significantly underfunded.

The structure of Company A may be represented graphically as follows.



Company A's *asset management* business is very capital light – most of the economic risks are run by the owners of the assets managed. Accordingly, it would receive a small allocation.

The *household* business buys most of its catastrophe reinsurance from the in-house catastrophe excess of loss line of business. It is a diversified portfolio of small individual risks and therefore would receive a fairly small allocation relative to its size, measured by premium income.

The *catastrophe excess of loss* line is very capital intensive as it runs the risk of very large claims. It therefore would receive a very large allocation relative to its size, measured by premium income.

The *motor* line is exposed to individual large claims, but there is little aggregation of risk. It therefore would receive a moderate allocation relative to its size, measured by premium income.

The *pension fund* is not a profit centre. However it exposes Company A to risk.

Question

Describe the risks that are likely to be faced by Company A in relation to its legacy defined benefit pension fund.

Solution

Risks to Company A in relation to the legacy defined benefit scheme include:

- funding risk – the risk that Company A needs to pay higher contributions to the scheme than expected to make good a shortfall, due to, for example:
  - longevity risk, resulting in benefits being paid for longer than expected
  - inflation risk, resulting in higher pension payments than expected
  - investment risk, *eg* from worse than expected investment returns, a market crash, mismatching of assets and liabilities, failure to recognise climate change risk.
- covenant risk, *ie* a poor assessment of Company A's current and ongoing financial ability to support the scheme, exposing Company A to the risk of needing to pay higher contributions to improve the security of the scheme
- liquidity risk, *eg* insufficient liquid assets being held to meet funding obligations as they fall due and therefore assets being realised at inopportune times …

  … and at a lower value than would otherwise be the case
- operational risks such as:
  - regulatory risk, from changes in regulation, *eg* gender equalisation of benefits
  - governance risks, *eg* impact of trustee bias or mismanagement of trustee conflicts of interest
  - administrative risks *eg* administrative errors leading to unexpected costs
  - cyber risks, *eg* a data or security breach leading to fines, reputational damage.

Under Solvency II, insurance companies are required to consider the risk that a pension scheme poses in the assessment of the SCR. In particular consideration should be given to the impact that adverse events may have on the scheme, and hence on the sponsoring company, as well as any commitment to make good a shortfall in the scheme.

The following questions need to be considered as part of any work to consider capital allocation. Some need to be considered before the work is done, while others can only be considered during the work. All questions should be addressed, as far as possible, in advance of any risk events occurring.

Questions relating to the pension fund

- **How should the risk of the pension fund be recognised?**

  For example, should the risk be measured as a multiple of any shortfall in the pension fund, or should the risk be measured based on the additional funding requirements needed under adverse stresses?

- **Should a proportion of capital be carved out and notionally allocated to the fund, recognising that it is effectively expected to make a zero return?**

  Allocating some of the available capital to the pension fund would reduce the free capital available to invest in projects that would be expected to make a non-zero return.

- **Does it provide a better shareholder return in the long run if Company A suspends dividends for a while so as to make the pension fund fully funded?**

  Suspending dividends now will reduce shareholders short-term income yield. However, by reducing the pension fund's deficit (sooner), total required capital will reduce (sooner) and so RAROC will increase (sooner). That deferral may, on balance, be beneficial to medium- / longer-term investors.

- **If that choice is made, what will the attitude of those shareholders be to the failure to provide them with income in the short run?**

  Will shareholders (especially those with short-term investment horizons) vote against the reduction? Will the share price be adversely affected?

Questions relating to the catastrophe excess of loss line

- **When there is a bad catastrophe year, how should the financial loss be recovered?**

- **Should capital be withdrawn from the catastrophe excess of loss line, so suppressing its business volumes?**

  As mentioned in an earlier question in this module, the capital allocated to a particular line of business may dictate the amount of business that that unit can write (as each policy written consumes capital and the total amount of capital is limited).

- **Is it better to allocate *more* capital to that line, in expectation of higher future premiums and therefore higher future returns?**

  By increasing the risk capital allocation to the catastrophe excess of loss line, its managers have greater freedom to generate higher business volumes, and hence to generate a greater subsequent RAROC.

- **Will that be seen as a reward for failure and cause friction between the business lines?**

Questions relating to the household line

- **How should Company A decide on the level of catastrophe excess of loss its household line buys?**

  The level of catastrophe excess of loss reinsurance may be determined by a number of factors such as the cost of the reinsurance *vs* the benefit in terms of the reduction in risk (and hence in terms of reduced volatility in profits and in reduced required capital), the risk tolerance of that line and hence the desired retention level (attachment point).

- **Should it allow the household underwriting team to decide on their own purchase?**

  This might result in them deciding to buy with a low attachment point, to protect their own results in the event of a catastrophe.

  Here 'results' is referring to the household line's underwriting result, which is only one of the performance metrics which should be considered. The lower the attachment point, the less risk is retained by the household line, and hence the more stable the results are likely to be. However, a lower attachment point means a greater reinsurance cost

- **Or should it set the attachment point centrally based on what is optimal for the company?**

  From the perspective of capital efficiency, one way of seeking to optimise the attachment point would be to maximise expected RAROC. The lower (higher) the attachment point the lower (higher) the risk retained and the lower (higher) the capital allocation to the household line (all other things being equal). That reduces (increases) the denominator in the RAROC metric, however the numerator will also be reduced (increased) by the higher (lower) cost of reinsurance.

  A higher (centrally determined) attachment point might result in the household underwriting team deciding to restrict their business volumes so as to reduce the chances of them failing to meet profit targets as a result of a catastrophe – and so cause an expense strain.

  A higher attachment point means that the household line retains more risk and so there is a greater chance that profits are adversely affected by a catastrophic event. One way of countering this is to take on less risk in the first place, *ie* to restrict business volumes.

  The 'expense' strain referred to is the fact that the household line is less likely to be able to cover its overheads if fewer policies are written.

Questions relating to the motor line

- **What level of capital should be allocated to the motor line?**

  It is weakly correlated with the other lines, so should it receive a very small allocation to recognise that – which will incentivise the motor team to boost their volumes and hence their potential profits and bonuses?

  The weak correlation means that the motor line is acting as a diversifier to the other lines, *ie* reducing the overall risk. If we employed a capital allocation method (*eg* Euler) that recognises the diversifying contribution of each line, this would the allocation of capital to the motor line.

On one hand, a reduced capital allocation may act as a restriction on the amount of future new business that can be written. On the other hand, it means that the performance of the motor line, as measured by RAROC, may increase (due to a lower denominator).

If the bonuses of the sales team are linked to RAROC, this may incentivise the team to write more business. Additionally, a high RAROC relative to other lines may mean that the motor line's ranking (or priority) within Company A is potentially improved.

Furthermore, a low capital allocation reduces the 'cost of capital' charge in the premiums, helping to make premiums for the motor line more competitive, which in turn would boost volumes.

- **Or should it receive a much larger allocation to recognise that it runs a significant risk of large claims?**

  This is referring to one of the introductory statement, which says the motor line is exposed to individual large claims.

- **If the allocation is much larger than the allocation typically used in the market, this could force the team to price at a level above what the market can stand, and so significantly reduce their volumes.**

  A higher capital allocation results in a higher 'cost of capital' charge in the premiums, making premiums for the motor line less competitive.

Questions relating to the asset management line

- **How should the asset management team be incentivised?**

  Although their impact on the economic risk of Company A is small, they have a material contribution to the operational risk.

- **Can the methodology of capital allocation be adapted so as to take account of this contribution?**

This page has been left blank so that you can keep the chapter summaries together for revision purposes.

1 Case study summaries

These case studies will provide useful material for students to consider as they prepare to meet Syllabus Objective 2.7. The variety of case studies presented and the different ways in which they are presented by the textbook authors will indicate that there is no unique recipe to enable managers to solve the problems posed by ERM.

However, there is a single common feature to all the case studies involving business failure. It is very rare for a business to fail significantly purely because of financial and economic factors. They are usually triggered or exacerbated by a failure to manage operational, strategic or governance risk.

Wherever possible, students should identify the root causes of a major loss or failure. For example:

- **Barings failed because of structural weaknesses that Nick Leeson exploited, and which were exposed by the Kobe earthquake (Sweeting, page 535).**

  The root cause of the failure of Barings Bank was an operational risk: inadequate internal management controls. The collapse of the bank was ultimately caused by a different operational risk (the Kobe earthquake) and market risk, but the collapse would not have happened if proper internal controls had been in place.

- **LTCM failed because of a failure by management to understand the weaknesses in the models it used, a failure that was exposed by the Asian currency crisis (Sweeting, page 543).**

- **Société Générale suffered multi-billion Euro losses because its managers failed to oversee Jérôme Kerviel's trading book adequately, a failure that came to light because the market went against the trades he had put on the books (Lam, pages 17-18).**

These three examples are very dramatic, yet the causes (poor oversight, poor model understanding and poor oversight) would have been identified by an effective ERM system.

In the examples discussed below, students should consider the relative importance of all categories of risk.

The case studies in Sweeting are largely self-explanatory. While it is useful to be familiar with the details of the case studies, it is more important to understand the lessons from each case study and to be able to relate those to other institutions.

The Notes below provide some more detail on some of these case studies (from Sweeting and other sources) and provide references for you to do further research.

1.1 Global financial crisis

The global banking sector experienced spectacular growth in revenues and profits in the 10 years to 2006. Worldwide profits in the sector grew to \$788*bn* in 2006 (compared to \$630*bn* in the oil and gas sector). Revenues in the sector accounted for 6% of global GDP. Profits per employee were 26 times higher than the average for all other industries. The financial markets were awash with liquidity. Low interest rates (in part due to the demand from China for cheap US government bonds) led to cheaper borrowing and a housing market bubble. Banks securitised these mortgages, with the main purchasers of these securitised assets being other banks.

However, facing the collapse of the US housing market in 2008 all this changed. Banks struggled to maintain sufficient liquidity as they were unsure about their own (and other banks') exposure to the complicated web of securitised assets with uncertain value. Liquidity in the market dried up as banks were unwilling to lend to each other. This led to some institutions going bust, while others were recapitalised by public (or private) money.

With hindsight, the crisis may have been foreseeable. Certainly there are mistakes that were made and lessons to be learned, including:

- a failure to understand and report the risks inherent in business activities
- products (such as CDOs) that were over-complex and were not well understood by those buying and selling them
- an overdependence on cheap debt
- remuneration that encouraged short-termism and valued subjective accounting profits above risk management and cash
- the unbundling of business models (particularly the outsourcing of mortgage sales), meaning many businesses had poor (and even unethical) sales practices – *eg* lending to sub-prime borrowers at rates that failed to reflect the risks
- de-regulation of the financial sector, which allowed risk to propagate unchecked through the system
- poor corporate governance, which led to some bad decision-making at Board level (such as RBS's ill-judged acquisition of ABN-AMRO)
- credit rating agencies that struggled to keep pace with the complex products and banks that 'gamed' the system – CDOs were deliberately engineered to AAA using the agencies' own (flawed) models resulting in widespread mispricing of risk.

Further references:

- Lam pages 287 – 289
- http://en.wikipedia.org/wiki/2008_financial_crisis
- Roger Bootle, 'The Trouble with Markets' ISBN-13: 978-1857885583

1.2 Barings Bank

Barings Bank was the oldest merchant bank in London, founded in 1762. It collapsed in 1995 after one of the bank's employees, Nick Leeson, lost £827*m* speculating on futures contracts.

Leeson was supposed to be arbitraging, seeking to profit from differences in the prices of Nikkei futures contracts listed in Japan and in Singapore. This involved buying futures contracts on one market and simultaneously selling them on another at higher prices. The margins on arbitrage trading are very thin, so volumes traded by arbitrageurs must be very large to gain any meaningful profit. As one is buying something at one market while selling the same thing in another market at the same time, almost all risks are hedged and the strategy should be risk-free. However, instead of hedging his positions, Leeson speculated on the direction of the Japanese markets.

- Minimum Funding Requirement (MFR) *(since replaced by the statutory funding objective)*
  - obligation on employers to maintain sufficient assets
  - increased security for members.

Other consequences of mis-selling and Maxwell

- greater mistrust of financial institutions by the public – perhaps fuelled by little publicity being given to the extensive recoveries (Maxwell) and redress actions (mis-selling)
- increased 'blame culture'
- imposition of MFR resulted in restricted investment policy, increased costs and, consequently, an unwillingness of employers to maintain defined-benefit schemes
- greater engagement by the public with financial issues and improved financial sophistication of investors
- growing demand for greater disclosure of information, transparency of operations and accountability of agents.

1.8 Space Shuttle Challenger

The Challenger disaster is widely used as a case study in areas such as engineering safety, the ethics of whistle-blowing, communications, group decision-making and the dangers of 'groupthink'.

Ultimately, the Presidential Commission that investigated the loss of the space shuttle concluded the accident was due to a lack of attention to NASA's normally high quality and safety standards, partly as a result of pressure on the organisation to accelerate the shuttle's launch schedule:

'The unrelenting pressure to meet the demands of an accelerating flight schedule might have been adequately handled by NASA if it had insisted upon the exactingly thorough procedures that were its hallmark during the Apollo program. An extensive and redundant safety program comprising interdependent safety, reliability and quality assurance functions existed during and after the lunar program to discover any potential safety problems. Between that period and 1986, however, the program became ineffective. This loss of effectiveness seriously degraded the checks and balances essential for maintaining flight safety.' (Source: Report of the Presidential Commission on the Space Shuttle Challenger Accident, Chapter 7.)

Hence, the key ERM lessons are:

- to ensure the decision-makers and leaders understand the risks that are being taken in the enterprise
- not to succumb to pressure to hit artificial targets (*eg* sales targets or launch dates) at the cost of good risk management.

Further reference:

- http://science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/table-of-contents.html.

1.9 Boeing

How do you know whether your ERM system is effective? Like all control work, it can sometimes feel that you can only ever get things wrong. For instance, Lam (pages 336-7) presents a case study on Boeing and Airbus.

The modern airline industry, throughout its value chain – from manufacture to delivery to servicing to operation – is generally extremely well-regarded in the risk management community for its strict safety-first processes, its openness to admitting error and for learning from its mistakes. Effectively the industry, the governments which regulate it and the passengers who use it, have zero risk appetite for failure that causes injury or death.

Lam describes both manufacturers focussing on improvements made to their operating processes to, 'cut back on their costs by reducing the chance of expensive mistakes'.

What Lam could not have known was the unfolding drama concerning the new narrow-bodied airliner, the 737 MAX. Within two years of its launch, two new aircraft had crashed, resulting in the loss of 346 lives. All the aircraft of that type were grounded. Both crashes were traced to the same fault, with Boeing and the US regulator, who had granted approval, both criticised by the US House of Representatives.

To date, the impact of this risk materialising has incurred a cost to Boeing of tens of millions of US Dollars, has damaged the firm's reputation and led to a number of Executive and Board changes.

Was Boeing's ERM system to blame? It is hard to know as external commentators. The purpose of an ERM system is to ensure that risks are properly managed and to alert the decision makers to the risk position continually.

Did the Board of Boeing know about the impact on safety of cost reductions? Did it recognise the risk of reduced Board challenge when the roles of Chair and Chief Executive were combined? Were actions taken as a result of these risks? Were the actions effective?

Or, was the assessment of these risks within the ERM system defective? Were the risks missed altogether? Was the presentation of the risk information suitable for the audience?

Or, were the decisions made in full knowledge of the accurate and appropriate risk assessments? The ERM system cannot prevent decisions that with hindsight look poor. One of the most challenging aspects of a CRO's role is to continue providing risk information even though the decision is different from that which the CRO might advise.

This example highlights the three parts of ERM leadership mentioned in Module 12:

1. **leading the implementation of the ERM framework across the organisation, including providing risk information**
2. **being part of the leadership of the organisation, including being part of decision making, and**
3. **leading the work of the risk management function.**

Problems can arise in all three roles.

Ideally, the CRO will implement an ERM framework which provides the right information to the right people, that supports the decisions made (including providing risk metrics that help make the decision work, whether it was the one favoured by the CRO or not) and ensuring that the risk function produces high quality risk analysis and synthesis.

Writing this review from the perspective of 2020 also brings into focus another major risk event, one which has unexpectedly dominated the agenda globally during the year – the 2020 Covid-19 pandemic.

1.10 Covid-19

Major risk events tend to be analysed publicly some time after the event, as they are either constrained with a single organisation or emerge as a result of complex interlinkages between organisations which take time to unravel. However, CROs and risk departments often have to react in real time when dealing with smaller risk events as they emerge, and make recommendations based on incomplete and partial information.

The 2020 Covid-19 pandemic illustrates a mixture of both: it is a major risk event, but is having to be dealt with by most, if not all, organisations in real time.

This section is being written in December 2020 – the first vaccination programmes are being rolled out in the UK and the US, and the EU has just granted approval for the vaccine. However a new mutation has just been identified, which appears to be far more contagious and there is a threat of further, more draconian, economic and social lockdowns.

Background

During December 2019 a new Coronavirus, SARS-CoV-2, was identified, which results in a disease known as Covid-19. This disease is highly contagious, but has a reasonably long asymptomatic incubation period during which carriers can transmit the disease. It results in painful and disruptive symptoms, which can persist for months. It is deadly to many of those infected, especially those who are elderly or who have underlying health conditions.

By March 2020 the disease had spread widely across Asia, Europe and beyond, and most countries began various programmes of lockdown – effectively banning a substantial amount of economic activity and providing very substantial government support to a very wide range of businesses.

The Response of Risk Managers

Prior to 2020, pandemic risk will have been on many organisations' risk registers. It is most likely to have been analysed as an operational risk scenario – for instance, 'Let us assume that 25% of our staff are off sick', and possibly as a mortality risk scenario – for instance, 'Let us assume that our mortality rates are 10% higher in one year than we expect.'

Pandemic risk was also on government risk registers. It was widely reported in 2020 that pandemic flu was the highest impact risk identified by regular UK government risk civil emergency risk reviews. Being reported is not the same as being believed. Being believed is not the same as doing something about it. It is notable that those countries with recent experience of fast-moving pandemics, notably in parts of Asia, seem to have been much better prepared than countries without that experience. For most of Europe and North America the last similar event was the influenza pandemic of 1918-1920.

This situation highlights two important factors in risk management. First, the pandemic is a classic black swan risk: a risk that is very low probability with very high impacts and which seems obvious in hindsight. It is very difficult to encourage people to think about mitigants to black swan risks.

Black swan risks were defined in Module 15.

Second, even if a Board was convinced that mitigants were required for a pandemic risk, what, on its own, should it do. Put another way, the actions that have been taken by governments worldwide in response to the pandemic were unthinkable in January 2020. Any mitigant at organisational level could be swept away by a government action. It is impossible to know what actions a firm wishing to be well-prepared could take to be confident of being better off as a result.

Perhaps the best strategy is to respond appropriately to the developing situation, which indeed is how most organisations have had to react. Those with risk functions, it is hoped, will have assessed the risks as they have been identified, and fed that intelligence into the decisions made by their organisations. In this section, I have set out the examples of emerging risk considerations. To provide some structure, the following material will use elements of the risk taxonomy implicitly provided in Unit 3.

Financial market risks

This section considers market risk, interest rate risk, foreign exchange risk, basis risk, credit risk, counterparty risk, liquidity risk.

In March 2020 the financial markets saw very significantly increased volatility, with very substantial selloffs. During late February and early March both FTSE100 and S&P500 lost about a third of their value. There were also wild variations in both government bond yields and in bond spreads. During this period of volatility there were three main financial market risk questions for financial institutions to address:

(a) What is this asset value and interest rate volatility doing to our current capital levels? Do we need to take urgent action to return them to an acceptable level?

(b) How is the volatility impacting our risk limit system? Are we in breach of any of our risk appetites, for concentration, liquidity, or value? Should we change our risk appetite to accept any breaches as a temporary measure or should we take action to restore exposure so that it is within appetite?

(c) To reflect the emerging situation, will the regulators make changes which affect the capital and risk limits that are permitted? How quickly will the regulators respond?

Since March, most investment indices have rebounded very significantly. CROs have to consider whether this is a signal of confidence in the economic future, or irrational optimism signalling a future correction, perhaps once government support is withdrawn and the true extent of economic scarring becomes clear, and advise their colleagues accordingly. An organisation needs to understand its risks so that it is confident it is resilient to responses at any point including at the two extremes.

Economic risk and strategic risk

For all organisations there was an urgent requirement to understand the potential impact of government economy shut-down measures on their finances, and to work out how best to access government support. Some organisations had no choice but to accept that support as the price of staying afloat in the hope of better times to come. However, it is notable that some organisations who had access to that support either turned it down or later returned it, to mitigate reputational risk.

For instance, in early December 2020, five major UK supermarkets collectively returned over £1.5bn they had been granted by central government to cover local property taxes. This illustrates how risk can be considered at different levels: at the organisation level, receiving funding relieved pressure on the profit and loss account. At the sector level though, receiving support while making additional profits was deemed to be reputationally difficult.

Returning the financial support had important side effects. It sent a strong market signal to all those reliant on the economic health of supermarkets – their suppliers, the investors who own the properties they rent, the transport companies who provide their logistics, their staff, the pension funds who rely on them, and their equity and debt holders. Returning the money sent a clear message of economic strength.

Were the supermarkets which failed to announce such a move signalling relative economic weakness, or were they signalling a higher risk appetite for reputational damage? What was the CRO advising the Board?

It is not too early to consider strategic risk, especially at sector level. There are some sectors – notably non-food retail and transport – and some locations – notably city centres where there is a concentration of office space – that seem likely to emerge from the pandemic with their previous strategic assumptions significantly changed.

The strategic risk will not be limited to single sectors and locations. There is a risk of contagion to all organisations with economic exposure to them. CROs of all firms should be starting to understand the extent of their reliance on other firms in their value chain and possibly geographic location.

At the macro-economic level, governments around the world were faced with decisions that relied on risk assessments. Fundamentally, governments had to balance:

- **the health of their populations with their economic output**
- **their population's demographics**
- **the costs of a slowdown**
- **the capacity of their health services, the mental health of their citizens**
- **the education of their children**
- **the impact on future tax rates**

with

- **different methods of reducing transmission**
- **testing facility and capacity**
- **disease transmission modelling, tracing functionality and/or building immunity**

arrayed around a virus that is showing a tendency to mutate.

This dilemma illustrates how risk-related decisions need to be taken in real time, and often without full understanding of the facts. All countries had access to some mathematical and economic modelling to understand the risks, but modellers quite rightly pointed out that their models were inherently uncertain and contingent on very significant assumptions. Alongside the political imperatives (*eg* not to cancel Christmas, to 'follow the science' when convenient – reminding us that political risk is real), it is clear that the possible scope of the CRO's remit is vast.

Insurance and demographic risks

All organisations with exposure to life and health contingencies have had to reassess the models on which they base their decisions. They were built on an assumption of relative stability, and so the very unusual circumstances have tested those models. It will be some time before it is clear how the year will impact models. It is possible that the increased mortality in 2020 in many countries will result in any of reduced, unchanged or increased mortality in future years, depending on which lives have been lost and how the future longevity of those who have been sick will be affected.

General insurance companies have had significant exposure to risk. Business interruption policies will often have a clause which provides coverage in the event of businesses being shut by a disease. Claims under this clause are rare, and some insurers sought to exclude all claims from Covid-19, relying on their understanding of what they had intended by the wording in their policy.

However, a court case in the UK brought by the FCA, the UK conduct regulator, challenged this interpretation, granting cover to many policyholders, but also making it clear that the specific wording and the specific circumstances of the claimant need to be taken into account.

This is an example giving rise to a number of possible risks:

- **pricing risk (were products priced properly?),**
- **legal risk (were terms and conditions correct?),**
- **reinsurance risk (will the reinsurer pay?),**
- **reserving risk (do reserves have to be recalculated?),**
- **operational risk (do claims handlers know what to look for?) *etc*.**

Not only will this case expose some insurers to claims they had not expected to cover, it will have resulted in reputational damage to those insurers who chose to fight the court case.

Operational risks

This section considers environmental risk, legal risk, regulatory risk, political risk, agency risk, and project risk.

Although these risks are described separately in the taxonomy in Module 3 they are grouped together for the purposes of this discussion. This grouping of similar risk types is not unusual – for a Board presentation where it is important to present salient information only to avoid overloading Board papers, it can be important to simplify the detail of what a function is doing. All these risks are typically understood in a similar way – using qualitative risk registers and high-level approximate financial analysis rather than detailed mathematical modelling. They are also managed in a similar way – using good quality processes and controls around those processes rather than mitigated mainly by holding capital.

Most firms will have had business continuity plans in place, which will have been tested to some extent. These will have included plans in response to office closures. However, the usual expectation would have been that an office closure was localised and temporary.

In response to this, the usual contingency plan would have been to transfer staff either to a different office of the same firm or to a 'Work Area Recovery' site – a third-party office that is kept available and ready to use on short notice. The expectation would have been that customer-facing functions and those directly supporting them day-to-day would transfer location and provide as good a service as possible. Some back-office functions, often including risk and actuarial functions, would have either worked remotely or simply suspended operations for a period.

It seems unlikely that any firm will have planned for a need to discourage or ban office working for a period that at the time of writing has extended for nine months. Nevertheless, most firms have proved to be extremely resilient, and have continued to work effectively during the period of the pandemic. This has been the result of a combination of factors: hard work by IT departments to change configuration and enable remote working, rapid adaptation to new circumstances, temporary acceptance of risks that are not usually tolerated, reconfiguration of offices so that they can be used as safely as possible by those who cannot work remotely, and goodwill from staff and customers alike.

This widespread operational resilience to completely unexpected circumstances illustrates the importance of understanding and managing operational risks. In fact, because of the work that firms and their regulators had previously done, and did during the course of the pandemic, most firms were able to respond very effectively. It is an undoubted success of good enterprise management, and good ERM. The outlier firms which have not been able to respond well will undoubtedly have seen their reputations significantly damaged.

This aspect of the pandemic also illustrates that risk scenarios are never going to be perfect. The short-term office closure considered and the widespread staff sickness modelled were not what happened. Nevertheless, they provided information which was of use in managing the actual scenario.

Reputational risk

We have touched on reputational risk in our discussions of other risk types above. This is not unusual. The risk of reputational damage is sometimes considered as a consequence of other risk types rather than as a risk in its own right. The connection between a risk event becoming known, any reputational damage occurring and any consequential loss of customers or of profits is hard to describe accurately, since public opinion can be mercurial.

The most advanced organisations will have involved their communications departments or advisers throughout the pandemic to manage reputation proactively, ensuring that press, government and regulators, rating agencies and customers have a good impression of the efforts the organisation is making to mitigate the impacts of the pandemic. This work is made considerably easier when the organisation has a good story to tell, so relies heavily on other risk mitigation activity.

It is important not to forget the organisation's own staff. Staff have a substantial influence on public reputation, whether via social media or via their interactions with customers, friends and family. An organisation whose staff can confirm that they have been treated well and supported to juggle work and family commitments through an extremely unusual time is more likely to maintain a good reputation.

Summary

These observations are tentative and partial. The Covid-19 pandemic provides an excellent real-life example of the landscape within which CRO's, risk functions and ERM frameworks will be tested, now and in the future. In due course, no doubt more detailed analysis will be undertaken, and some of the observations made will prove to have been wrong. Future CROs will learn from the mistakes of this generation of CROs to enable them to help their organisations to manage their risks better.

Question

Outline the ERM lessons that can be learned from the Covid-19 case study (and therefore which might be applied to manage future emerging risk situations).

Solution

- Emerging risks can have an extremely wide-ranging impact and should not be siloed into traditional risk categories (*eg* pandemic risk should not be modelled uniquely as a mortality risk, or an operational risk).
- Black swan events can have devastating consequences and should not be ignored because they are thought too rare to occur.
- Risk registers are good places to record risks but not necessarily to drive action. (Reporting risk is not the same as believing risk and believing risk is not the same as doing something about it.)
- Countries with recent experience of pandemics, *eg* in Asia, were better prepared.
- More facilitation is needed to help stakeholders to engage with black swan events, to discuss the interdependencies and to create a scenario.

  In particular, understanding the reliance on other organisations in the value chain as well as the impact of geographic location is important (contagion risk).
- The most resilient organisations were ones who:
  - had well-developed BCPs and crisis recovery plans (although these needed to be adapted, they provided a good framework of considerations)
  - communicated reassuringly with staff and customers, and were accessible
  - were able to support staff technologically, to work from home
  - had staff who presented a positive view of their companies, *eg* via social media or interactions with customers
  - were able to adapt quickly to changing customer needs, adapting products and services.
- It is important for an organisation to understand its operational risks and to manage them through good quality processes and controls (rather than uniquely by holding capital)
- ERM must be dynamic – no matter how well-prepared an organisation is for an event; the reality is one that is constantly changing and subject to uncertain actions by third parties.

  For example, political risk is very real.

- It is unclear how the pandemic will impact on future modelling, *eg* of mortality / morbidity. There is a lot of uncertainty involved.
- Having the ability to assess and monitor risks quickly, so as to be able to feedback and respond rapidly is important.

  In presenting information to the Board, consideration should be given to what is salient and to simplify the detail, so as not to overload the Board with information.

1.11 Risk transfer case studies

- Honeywell (Lam page 124)
- Barclays (Lam pages 124-125)

1.12 ERM Implementation case studies

As mentioned in Module 31, Appendix 3 of the IAA Note describes three examples of ERM programmes in various businesses:

- the successful implementation of an ERM strategy involving building a capital model in a large insurer
- a cautionary tale of an over-engineered ERM project in a large insurer
- an apparently successful ERM project in a global insurer, but one where 'success' was measured by the quality of the process, not the quality of the impact on business outcomes.

2 Lam's lessons learned

Companies' processes should allow them to learn from their own mistakes and from the mistakes of other companies.

In order to avoid major losses and disasters, companies must have organisational learning processes that enable them to:

- be open to discuss their own past mistakes
- be able to learn from those mistakes
- be aware of the mistakes of others
- adopt industry best practices.

These learning processes may include:

- internal meetings of senior executives and managers
- examination of external events and problems
- visits to other institutions to benchmark practices
- building a widely accessible and searchable database of insights
- training new starters in risk management
- recording losses in a risk event log
- reviewing important incidents and policy violations.

Examination of past events by Lam has led to seven key lessons.

Lesson 1 – Know your business

The most important lesson is that everyone from front-line employees to the Board should 'know the business'.

In credit risk management, 'know your customer' is a key tenet.

Everyone must understand how their accountabilities affect the risks of the organisation. Business managers should 'know the risks' in the business.

Failure to know the risks led to the problems with Kidder Peabody where management failed to supervise, understand and monitor the activities of the trading desk. The supervisors and auditors did not understand the risks in the trading being undertaken.

In the case of Metallgesellschaft, the company failed to understand the cashflow risks inherent in its hedging strategy.

34

References and further reading

Syllabus objectives

This module does not refer to any syllabus objectives.

It contains references to further reading you may choose to do either to enhance your wider appreciation of the topics covered by the syllabus, or to look at after you have passed the Subject SP9 examination, *eg* for CPD purposes.

0 ERM in General

The Core Reading for Subject SP9 refers to part, but not all, of the following texts:

- *Enterprise Risk Management From Incentives to Controls* – Second edition – James Lam.

  Wiley, 2014. ISBN: 9781118413616

- *Financial Enterprise Risk Management* – Second edition – Paul Sweeting.

  Cambridge University Press, 2017. ISBN: 9781107184619

- *Note on Enterprise Risk Management for Capital and Solvency Purposes in the Insurance Industry* – International Actuarial Association

  Published 31 March 2009

  http://www.actuaries.org/CTTEES_FINRISKS/Documents/Note_on_ERM.pdf

- *Insurance Criteria: Evaluating the Enterprise Risk Management Practices of Insurance Companies* – Standard & Poor's

  https://www.actuaries.org.uk/documents/insurance-criteria-evaluating-enterprise-risk-management-practices-insurance-companies

- *Risk analysis and management for projects: a strategic framework for managing project risk and its financial implications* – Institution of Civil Engineers, and Institute and Faculty of Actuaries, 2002. Thomas Telford Ltd.

The following are well-established ERM textbooks which used to be, but are no longer required reading for Subject SP9. They were not written specifically with actuarial students in mind:

- *Simple Tools and Techniques for Enterprise Risk Management* – Robert J Chapman.

  Wiley, 2006. ISBN: 0-470-01466-0

- *Quantitative Risk Management: Concepts, Techniques and Tools* – McNeil, Frey & Embrechts.

  Princeton University Press, 2005. ISBN: 0-691-12255-5

Other general risk management texts and publications include:

- *The Essentials of Risk Management* – Crouhy, Galai and Mark.

  McGraw-Hill, 2006. ISBN: 0-07-142966-2

- *The Orange Book: Management of risk – principles and concepts* – HM UK Treasury

  https://www.gov.uk/government/publications/orange-book

The Core Reading for Subject SP9 refers to the Core Reading from the following earlier subjects:

- CS1 Core Reading
- CS2 Core Reading
- CM2 Core Reading
- CP1 Core Reading

1 Specific ERM topics

Corporate Governance (Module 4)

UK Corporate Governance Code (2018):

https://www.frc.org.uk/directors/corporate-governance-and-stewardship/uk-corporate-governance-code

Walker Review of Corporate Governance:

https://webarchive.nationalarchives.gov.uk/+/www.hm-treasury.gov.uk/d/walker_review_261109.pdf

Mandatory risk frameworks (Module 5)

Solvency II: http://www.bankofengland.co.uk/pra/pages/solvency2/default.aspx

ORSA: http://www.naic.org/cipr_topics/topic_own_risk_solvency_assessment.htm

Actuarial Profession: https://www.actuaries.org.uk/upholding-standards

Advisory risk frameworks (Module 6)

We highly recommend you take a look at The Orange Book. It can be downloaded at https://www.gov.uk/government/publications/orange-book. It is easy to read and reinforces many of the key messages from the SP9 course.

The Canadian Integrated Risk Management Framework was replaced in late 2010 with an updated version called 'The Framework for the Management of Risk'. This can be downloaded from http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422

The IRM/AIRMIC/Alarm standard and other useful risk management resources can be downloaded from the IRM website at http://www.theirm.org

Behavioural finance (Module 13)

Nigel Taylor (2000), 'Making actuaries less human: lessons in behavioural finance', Staple Inn Actuarial Society (SIAS):

https://sias.org.uk/media/1187/making-actuaries-less-human-lessons-from-behavioural-finance.pdf

Climate change (Modules 13 and 25)

The Prudential Regulation Authority (PRA) report entitled, "The impact of climate change on the UK insurance sector":

https://www.bankofengland.co.uk/prudential-regulation/publication/2015/the-impact-of-climate-change-on-the-uk-insurance-sector

The June 2017 recommendations of the Task Force on Climate-related Financial Disclosures (TCFD):

https://assets.bbhub.io/company/sites/60/2020/10/FINAL-2017-TCFD-Report-11052018.pdf

The May 2017, IFoA risk alert on climate change:

https://www.actuaries.org.uk/system/files/field/document/Risk%20Alert%20-%20Climate%20Change%20FINAL.pdf

Copulas (Module 18)

Articles on copulas from *Risk* magazine:

https://www.risk.net/topics/copulas

Market Risk Management – The Greeks (Module 27)

CM2 Course Notes – The Actuarial Education Company

Credit risk management – Due diligence (Module 28)

For an extensive due diligence checklist see 'The Financial Risk Manual - A Systematic Guide to Identifying and Managing Financial Risk' J. Holliwell, ISBN-13: 9780273624189.

Operational risk management – Tokyo-Mitsubishi and NatWest (Module 29)

'Risk Management', Crouhy, Galai and Mark (page 597) ISBN-13: 978-0071357319

Capital (Module 30)

The following paper used to be, but is no longer, required reading for Subject SP9.

- *Specialty Guide on Economic Capital* – Society of Actuaries

  Version 1.5, dated March 2004

  https://www.actuaries.org.uk/documents/specialty-guide-economic-capital