## Chapter 2

### Risk management

### Chapter learning objectives:

<table>
<thead>
<tr>
<th>Lead</th>
<th>Component</th>
<th>Indicative syllabus content</th>
</tr>
</thead>
</table>
| A2. Evaluate risk exposure | (a) Evaluate the impact of risk  
(b) Assess the likelihood of risks.  
(c) Analyse the interaction of different risks | • Quantification of risk exposure  
• Risk maps |
| A3. Discuss ways of managing risk. | Discuss:  
(a) Roles and responsibilities  
(b) Risk tolerance, appetite and capacity  
(c) Risk management frameworks  
(d) Risk analytics | • Role of board and others in the organisation for identifying and managing risks  
• Risk mitigation including TARA – transfer, avoid, reduce, accept  
• Assurance mapping  
• Risk register  
• Risk reports and responses  
• Ethical dilemmas associated with risk management |
| C2. Recommend internal controls for risk management | (a) Discuss the Committee of Sponsoring Organisations of the Treadway Commission (COSO) internal control and risk management framework.  
(b) Assess control weakness.  
(c) Assess compliance failures.  
(d) Recommend internal controls for risk management. | • Governance and culture  
• Strategy and objective setting  
• Performance  
• Review and revision  
• Information, communication and reporting  
• Identifying and evaluating control weakness and compliance failures |
1. Risk management

The process of understanding and managing the risks that an organisation is inevitably subject to in attempting to achieve its corporate objectives. - CIMA

Traditional view of risk management

• The traditional view of risk management is to protect organisations from loss through conformance procedures and hedging techniques.
• The traditional view is about avoiding downside risk.

Modern view of risk management

• The modern approach is to take advantage of opportunities to increase overall returns within a business.
• This is about benefitting from the upside risk.

ENTERPRISE RISK MANAGEMENT (ERM)

This is a term given to the alignment of risk management with business strategy and the embedding of risk management culture into business operations.

ERM by COSO

COSO defines ERM as a process that:

• Is effected by the entity’s board of directors, management and other personnel.
• Is applied in strategy-setting and across the enterprise.
• Is designed to identify potential events that may affect the entity and manage risks to be within its risk appetite.
• Provides reasonable assurance regarding the achievement of the entity’s objectives.
Note:
Risk management has now transformed from a department-focused approach to a holistic, coordinated and integrated process that manages risk throughout the organisation.

Key principles of ERM

- Consideration of risk management in the context of business strategy.
- Risk management is everyone’s responsibility, with the tone set from the top.
- The creation of a risk-aware culture.
- A comprehensive and holistic approach to risk management.
- Consideration of a broad range of risks.
- A focused management strategy, led by the board.

- 4 objectives reflect the responsibilities of different executives across the entity and address different needs.
- 4 organisational levels emphasise the importance of managing risks across the enterprise as a whole.
- 8 components must function effectively for risk management to be successful. They are closely aligned with the risk management process and reflect the elements of the COSO view of an effective internal control system.
Internal environment:
- Tone of the organisation
- Includes the risk management philosophy
- Includes the risk appetite

Objective setting:
- Should be aligned with the organisation’s mission
- Needs to be consistent with the organisation’s defined risk appetite

Event identification:
Internal and external events that impact the achievement of an entity’s objectives must be identified

Risk assessment:
Risks are analysed:
- To consider their likelihood and impact
- As a basis for determining how they should be managed

Risk response:
- Managers seek risk responses to:
  - Avoid
  - Accept
  - Reduce
  - Share the risk
- The intention is to develop a set of actions to align risk with the entity’s
  - Risk tolerance
  - Risk appetite

Control activities
- Policies and procedures that help to ensure that the risk responses are effectively carried out

Information and communication:
- The relevant information is identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities

Monitoring:
- The entire ERM process is monitored
- It is modified if necessary
Benefits of ERM

- Enhances decision-making by integrating risks.
- Improves investor confidence and shareholder value.
- Focuses management attention on the most significant risks.
- A common language of risk management understood throughout the organisation.
- Reduces the cost of finance through effective risk management.

Risk management and shareholder value

**Ernst & Young’s model of shareholder value:**

\[
\text{Shareholder value} = \text{Static NPV of existing business model} + \text{Value of future growth options}
\]

The four stages of Ernst & Young’s model of shareholder value are:

1. **Establish what shareholders value about the company**
2. **Identify the risk around the key shareholder value drivers**
3. **Determine the preferred treatment for the risk**
4. **Communicate risk treatment to the shareholders**
Update to ERM framework (from 2017)
The update uses a new diagram – the double helix (below). The key principle is that ERM should be ingrained into everything the organisation does including setting the mission, vision and core values of the entity.

Risk is inherent in everything an entity does and it is therefore a risk that a strategy chosen by an entity may not be in line with the stated mission, vision and core values.

2. Risk management strategy

Risk appetite
This is the amount of risk that an organisation is willing to accept in the pursuit of value. This can be explicit in its values and strategies or may be implicit. It is determined by:

- **Risk capacity**: the amount of risk that an organisation can bear.
- **Risk attitude**: the overall approach to risk in terms of risk-taker or risk-averse.
- **Residual risk**: the risk a business faces after its controls have been considered.
RISK APPETITE FACTORS

| Nature of products being manufactured | • A high risk of product failure in certain products must be avoided due to the serious consequences of such events – e.g. aircraft.  
|                                           | • For some products, the risk of failure may be low – e.g. fizzy drinks. |
| The need to increase sales | • The strategy need to move into a new market will result in a business accepting a higher degree of risk than trying to increase its sales.  
|                                           | • The business will have a high risk appetite. |
| The background of the board | • Some are risk-takers – high risk appetite.  
|                                           | • Some are risk-neutral/risk-averse – low risk appetite. |
| Amount of change in the market | • Operating in a market with significant rapid changes leads an organisation to have a high risk appetite and vice versa.  
|                                           | • The organisation needs to accept a high degree of risk. |
| Reputation of the entity | • A company with a good reputation has a low risk appetite, and so accepts low risk.  
|                                           | • It does not want to lose its good reputation. |

Note: The higher the risk, the higher the return you can expect.

Features of risk management strategy

The CIMA and IFAC joint report in 2004 - Enterprise Governance - identified the following key features of a risk management strategy:

• Statement of the organisation's attitude to risk.
• The risk appetite of the organisation.
• The objectives of the risk management strategy.
• The culture of the organisation in relation to risk.
• Responsibilities of the managers for the application of risk management strategy.
• Reference to the risk management systems the company uses.
• The definition of performance criteria to evaluate the effectiveness of risk management.
An alternative process of risk management proposed by the Institute of Risk Management

This identified three elements:

1. **Risk assessment**, composed of analysis and evaluation of risk through a process of:
   - Identification
   - Description
   - Estimation

2. **Risk reporting**
   - Regular reports to the board and stakeholders.
   - Setting out the organisation’s policies in relation to risk.
   - Enabling the effective monitoring of risk policies.

3. **Risk treatment (risk response)**
   - The process of selecting and implementing measures to modify the risk.

   **Note**: Residual risk reporting will follow risk treatment.

3. **Identifying, measuring and assessing risks**

**Risk identification**

- The risk identification process is controlled by the **risk committee** or risk management specialists.

- The risks identified through this process are recorded in a **risk register**.

   **Note**: A risk register is simply a list of the risks that have been identified and the measures that have been taken to control each of them.

- A variety of methods can be used by a business to identify the risks that it faces.

**Risk register:**

- Risk title
- Risk likelihood
- The impact of the risk should it arise
- The name of the risk owner
- The date the risk was identified
- The date the risk was last updated
- Mitigation actions
- An overall risk rating
- Further actions
- The name of the action head
- The due date
- Target risk level (optional)
QUANTIFICATION OF RISK EXPOSURE:

The following techniques can be used to quantify risks:

- Expected values and standard deviation
- Volatility
- Value at risk (VAR)
- Regression analysis
- Simulation analysis

Expected value

- Summarises all the possible outcomes by calculating a single weighted average.
- Is a long-run average mean.
- Is usually not the most likely result, nor a possible result.
- Helps determine the average result if the same event were to occur several times.
**Formula for Expected Value:**

\[ EV = \Sigma px \]

Where:

\[ \Sigma = \text{sum of} \]
\[ X = \text{future outcome} \]
\[ P = \text{probability of the outcome occurring} \]

**Standard Deviation**

Standard Deviation is a measure of volatility and is a conventional measure.

- Compares the actual outcome with the expected value or mean outcome.
- Calculates how far on average outcomes deviate from the mean.
- The more actual outcomes vary from the average outcome, the more volatile the results and the more risk is involved in decision-making

**Formula for Standard Deviation:**

\[ \sigma = \sqrt{\frac{\Sigma (x - \bar{x})^2}{n}} \]

Where:

\[ \sigma = \text{standard deviation} \]
\[ \Sigma = \text{sum of} \]
\[ X = \text{each value in dataset} \]
\[ \bar{x} = \text{mean of all values in the dataset} \]
\[ n = \text{number of values in the dataset} \]

**Volatility**

Volatility is a means of assessing risk by looking at its potential volatility.

**Value at risk (VaR):**

- Allows investors to assess the likely scale of loss in their portfolio at a defined level of probability.
- Is becoming the most widely used measure of financial risk.
- Is enshrined in both financial and accounting regulations.
- Is based on the assumption that investors care mainly about the probability of large losses.
- The VaR of a portfolio is the maximum loss on a portfolio occurring within the given period of time with a given (usually small) probability.
Three components of VaR:
- A time period
- A confidence level
- An amount or percentage of loss

Formula for Value at Risk:
Standard deviation × Z-score

Regression analysis
- Used to measure a company’s exposure to various risk factors at the same time.
- Performed by regressing changes in the company’s cash flows against the risk factors.
- The regression coefficient will indicate the sensitivity of the company’s cash flow to these risk factors.

Simulation analysis
- Used to evaluate the sensitivity of the value of the company (or its cash flows) to a variety of risk factors.
- These risk factors are given various simulated values based on probability distributions.
- The mean and standard deviation are calculated in order to calculate an expected value.
- It is complex and time-consuming and limited by assumptions regarding probabilities.

RISK MAPPING
- A risk map identifies a risk and its significance and links that to the likelihood of its occurrence.
- This helps to prioritise risks in a business.
- Risks with significant impacts and a high likelihood of occurrence need more urgent attention than risks with a low impact and low likelihood of occurrence.
4. Risk response strategy

RISK TREATMENT/MANAGEMENT METHODS:

Avoid risks

- A company may decide that some activities are so risky that they must be avoided.
- There will always be work, but it is impossible to avoid all risks in commercial organisations as risks have to be taken to make a profit.

Transfer risks

- Risks are transferred wholly or in part to a third party.
- An example is an insurance company.

Pool risks

- Risks from different transactions can be pooled together; each transaction has its potential upside or downside risk.
- The risks tend to cancel each other out and are lower for the pool as a whole than for each item individually.
Diversification

- Diversification is a similar concept to pooling but applies to different industries or countries.
- The idea is that the risk in one area can be reduced by investing in the other area.

*Spreading risks by portfolio management*

Risks can be spread by expanding the portfolio of companies held. The portfolio can be expanded by integration, linking with other companies in the supply chain or diversification into other areas.

- **Backward integration**: refers to development into activities concerning the inputs to the organisation.
- **Forward integration**: refers to development into activities concerning the organisation’s output.
- **Horizontal integration**: refers to development into activities that complete with, or directly complement, an organisation’s present activities.

*Unrelated diversification:*

This is development beyond the present industry, into products or markets that bear no clear relationship with the present portfolio. The organisation may also want to enter into a completely different market to spread its risks.

*Problems with diversification:*

- Businesses compete by specialisation, and they complete successfully in the areas in which they specialise.
- It is difficult for companies to excel in a wide range of diversified businesses.
- Over-diversification may make an organisation more difficult to manage.
- Little advantage accrues to shareholders through diversification.

*Risk reduction*

- If the company cannot totally eliminate risk, it may reduce it to a more acceptable level.
- Internal control would reduce either the likelihood or the size of a potential loss.
- The cost of internal controls should justify the benefits.
- Hedging is reducing risks by entering into transactions with opposite risk profiles.
- Risk sharing with another party (such as insurance or a joint venture) is another potential strategy.
5. The Risk Cube

- Risk equals the volume of the cube.
- Risk is seen as the combination of threats that may exploit a vulnerability and cause harm to an asset.

*Residual risk is a combined function of:*

- A threat, less the effects of threat-reducing safeguards.
- A vulnerability, less the effect of vulnerability-reducing safeguards.
- An asset, less the effect of asset value-reducing safeguards.

Managing the risk can be undertaken by reducing the threat, reducing the vulnerability and/or reducing the asset value.
6. Risk reporting

- Risk reports are now part of UK annual reports.
- They are an important disclosure requirement.
- They are required by the managers of business and external stakeholders.

A risk reporting system includes:

- A systematic review of risk forecast (at least annually).
- A review of risk strategy and responses to significant risks.
- A monitoring and feedback loop on action taken.
- Assessment of significant risks.
- A system including material change to business circumstances.
- The incorporation of audit work as part of the monitoring and information gathering process.

7. Gross and Net risk

The risk report should show:

- **Gross risk**: an assessment of risk before the application of any control, transfer or management responses.

- **Net risk** (residual risk): an assessment of risk, taking into account the controls, transfer and management responses, i.e. after any controls have been implemented.

**Note**: If the residual risk (net risk) is considered to be too great, the company will need to:

- Not expose itself to the risk, or
- Put better controls over the risk in place.

**Residual risk** can be measured as a portion of profit/capital/turnover in order to help management make decisions.
Ability to bear risk: one approach to assess the ability to bear risk is to consider the financial consequences of the risk, in relation to:

- The organisation’s profits.
- Return on capital employed.
- The organisation’s expenditure budget (not-for-profit organisations).

8. Evaluating Risk Management Strategy

The risk management strategy will be evaluated once the company has:

- established its risk strategy,
- identified areas where it will reduce the risks,
- identified methods it will use to achieve the desired risk reduction.

Do benefits outweigh costs?

- The costs and benefits of risk measures such as internal controls can be evaluated, and a cost-benefit comparison can be carried out.
- The benefits from risk controls should preferably be measured and quantified; however, some benefits may have to be assessed qualitatively.
- The evaluation process should be based on the principle that the cost of the control measure should not exceed the benefits it provides.

Interaction between risks

Risk identification is very important, because risks are often interrelated.

E.g. compliance, environmental or fraud risk can possibly impact the reputation risk.
## 9. Risk Management Roles and Responsibilities

<table>
<thead>
<tr>
<th>Who</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| Board of Directors                       | • Overall responsibility for risk management.  
• Define risk appetite for the company.                                                                                                                                                                                                                                                                 |
| Audit Committee                          | • Board committee with responsibilities for reviewing internal audit control systems and working with auditors (external, internal).                                                                                                                                                                           |
| Risk Committee (unless covered under audit committee) | • Creating risk awareness and ensuring proper risk management within the organisation.  
• Establishing policies for risk management.  
• Ensuring the existence of adequate and efficient processes to detect, monitor and report risks.  
• Updating the company’s risk profile.  
• Reporting to the board and making recommendations on the risk appetite of the company.  
**Secondary objectives of the risk management committee:**  
• Advising the board on the risk profile of the company.  
• Acting on behalf of the board.  
• Ensuring that proper mechanisms are in place with respect to risk identification, risk assessment, risk assurance and overall risk management.  
• Continual review of the company’s risk management policy.  
• Ensuring proper communication of risk, policies and controls to employees and management. |
| Risk Management Group – risk manager     | • Provision of overall leadership for the risk management team.  
• Identification and evaluation of the risks affecting an organisation due to the organisation’s business operations and policies.  
• Implementing risk management strategies.  
• Seeking opportunities to improve risk management methodologies.  
• Monitoring the status of risk mitigation strategies and internal audit.  
• Developing, implementing and managing risk management programs and initiatives.  
• Maintaining a good working relationship with the board and risk management committee.  
• Liaising with insurance companies.  
• Ensuring compliance with business laws and regulations. |
| Internal Audit                           | • Reviews the internal controls.  
• Supports the management in the risk management process.                                                                                                                                                                                                                                                                 |


10. Chapter Summary

CHAPTER 2

Risk Management

Risk management

Risk Strategy

Risk management cycle

Conformance vs Performance

Formulate

Features:
- attitude
- appetite
- objectives
- culture
- responsibilities
- systems
- performance criteria

Identify risks
- risk appetite (attitude)
- capacity
- residual risk

reactive or proactive
internal or external

Quantify
- EV
- Volatility
- VAR

Risk committee, risk register

Assess risks

Risk mapping
- impact
- likelihood

Roles and responsibilities
- Risk Committee
- Risk Management Group
- Risk Manager

Implement and allocate responsibilities

Risk response
- avoid
- transfer
- pool
- diversification
- reduction
- hedging
- sharing

Monitoring of controls

Risk reporting
- gross risk
- net risk

Evaluate risk management strategy

Review

ERM
- 4 objectives
- 4 organisational levels
- 8 components

- did it achieve objectives?
- benefits vs costs