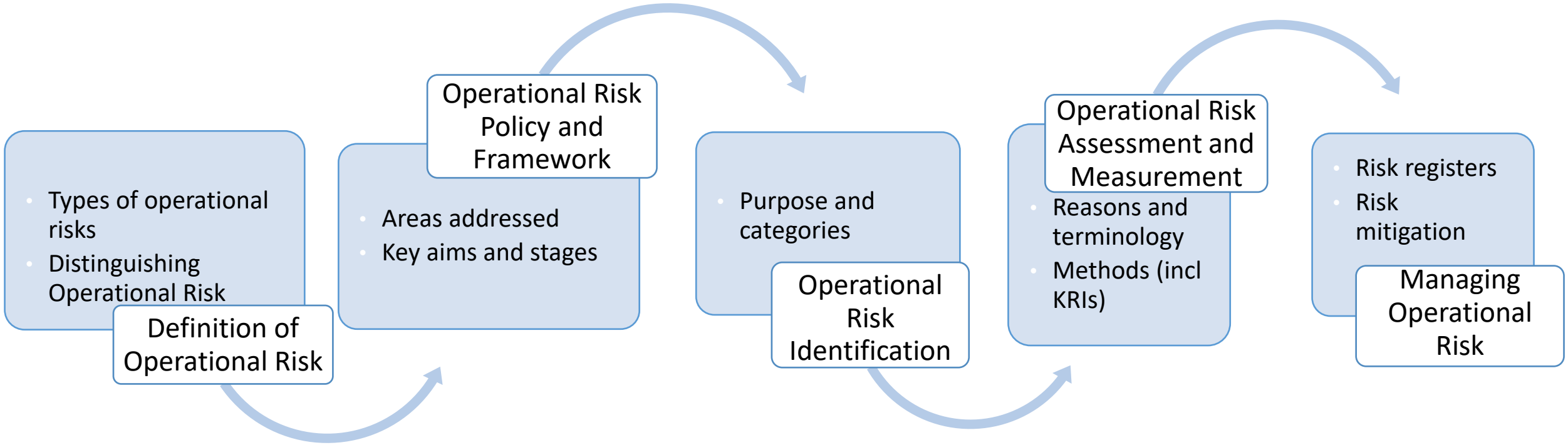
Chapter 3

Operational Risk

Questions - 15

EMERGING MARKET
FINANCIAL TRAINING

Chapter Summary



Definition of Operational Risk

Basel Committee Definition

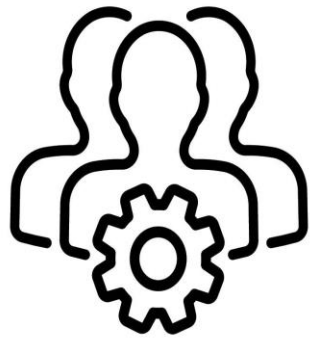
The risk of loss resulting from **inadequate** or **failed internal processes**, people and systems or from external events.

- It covers **legal risk.** E.g.: fines, penalties and punitive damage
- Excludes **reputation risk**

Basel Operational Risk Event Types

The following are crucial elements of an effective operational risk management framework:

- Clear risk oversight by the board and senior management
- A strong **operational risk culture**
- A strong **internal control culture**
  - Clear lines of responsibility and Segregation of duties
- Effective **internal reporting**
- **Contingency planning**



EMERGING MARKET FINANCIAL TRAINING

Types of Operational Risks

Internal fraud

Losses due to acts of a type intended to **defraud**, **misappropriate property** which involves an **internal party**

External fraud

Losses due to acts of a type intended to **defraud**, **misappropriate property** by a **third party**

Employment practices and workplace safety

Losses arising from acts inconsistent with employment, **health or safety laws**, from payment of **personal injury claims**.

Types of Operational Risks

Business disruption and systems failures

Losses arising from disruption of **business or system failure**

Execution, delivery, and process management

Losses from **failed transaction processing** from relations with trade counterparties and vendors

Clients, products and business practices

Losses arising from an unintentional or negligent **failure to meet a professional obligation** to specific clients

Damage to physical assets

Losses arising from **loss or damage to physical assets** from natural disaster or other events

EMERGING MARKET FINANCIAL TRAINING

Financial Crime

Insider information and market manipulation

Prohibit certain undesirable practitioner behaviours, collectively known as **market abuse**

Examples

- Insider dealing

When an insider **deals based on information** which is not known to the market.

- **Improper disclosure**

Where an insider improperly **discloses inside information** to another person

- **Improper dissemination**

Giving out **information that conveys a false** or misleading **impression about an investment**

Financial Crime

Money laundering and terrorist financing

Oblige financial services firms to **monitor financial transactions** and report any that appear suspicious to reduce the likelihood of criminal proceeds being moved around.

Three stages to money laundering operation

Placement

This is the introduction of **dirty money into the financial system**

Layering

This involves moving the **placed money around the system** to make it difficult for the authorities to link the placed funds with the ultimate beneficiary of the money.

Integration

The ultimate beneficiary appears to be **holding legitimate funds**. The money is regarded as ‘integrated’ into the legitimate financial system.

EMERGING MARKET FINANCIAL TRAINING

Question Time

What is Financial Crime ?

A. Risks that affect one firm, or a group of firms, can affect the stability of the whole financial system

B. Involve taking money or other property that belongs to someone else, to obtain a financial or professional gain.

C. Risk of loss arising from changes in the value of financial instruments.

D. Risk is the exposure of a firm's financial condition to adverse movements in interest rates.

Financial Crime

AML Provisions & Terrorist Financing Provisions

- Customer identification
- Record keeping
- Reporting suspicious activity

Set of Risk Management Responses on Financial Crime

Educating staff on:

• Society , the firm & the individual

- Putting systems and controls in place to mitigate the **risk of occurrence**.
- **Monitoring staff compliance** with the internal and external rules.
- **Escalating behavioural exceptions** to a specific individual.
- **Penalizing contravention** with the rules.

Distinguishing Operational Risk

Operational Risk as a Distinct Risk Class

Historically, organizations had accepted operational risk as an **unavoidable** cost of doing business and considered any risk that was not market or credit risk to be operational.

Operational Risk and its Consequential Effects

When an operational risk **materializes**, it often causes other risk issues:

Reputational risks

If clients or the media become **aware of the issue**.

Compliance/Regulatory risks

Certain process failures will result, for example, in customers not being **treated fairly.**

Credit risks

Areas in the credit function where operational risk issues can lead to losses are

- **data errors**, lack of **adequate monitoring** & **legal risk**

Distinguishing Operational Risk

Operational Risk and its Consequential Effects (cont…)

Market risks

An **undetected error** in the portfolio management system might lead to a breach of a market risk limit.

Liquidity risks

A process breakdown in the finance department could lead to the firm having **insufficient liquidity** to pay staff salaries.

Investment risks

Carelessness on the part of a fund manager, coupled with a process that contains no subsequent checking, could cause a mandate limit breach

Operational Risk Policy

Defining the

- firm's **operational risk appetite.**
- methodology used to **identify the operational risks**.
- methodology used to **measure the significance of the identified risks**.

Assigning responsibility to line managers to mitigate **actions required to reduce risk** exposures.

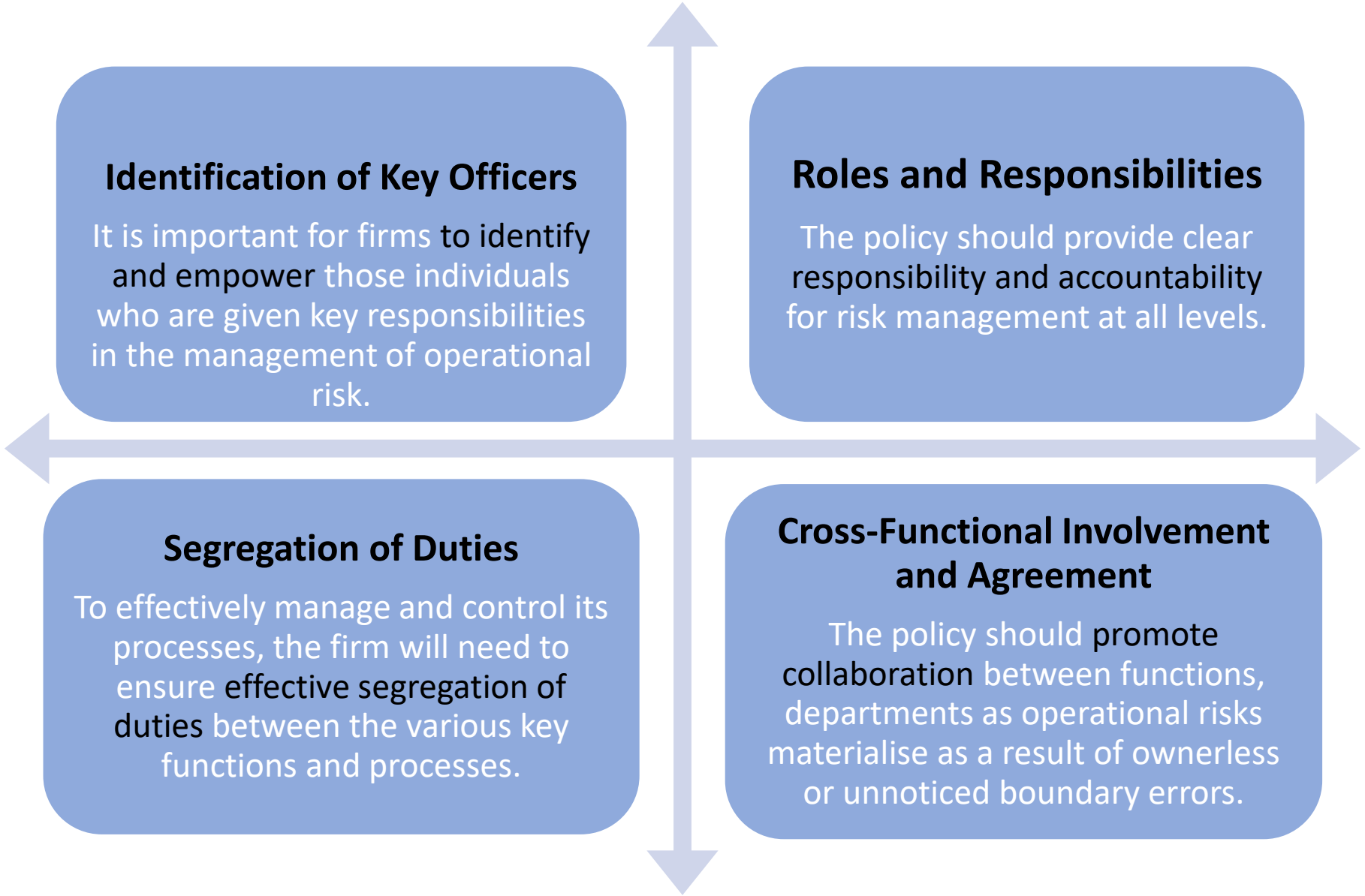
Assigning responsibility for **monitoring the effects of the mitigating actions.**

Establishing the reporting for risk issues to all levels of the organisation to ensure **transparency and aid the decision-making process.**

Operational policy which exists globally

- A balance between the **global standardization** and **regional differences**.
- **Objectivity** when risk prioritisation needs to be performed.
- A sense of fairness when **rewarding risk performance**.
- Centralised control of the overall **capital adequacy assessment**.

Areas Addressed by An Operational Risk Policy



Operational Risk Framework

Operational Risk Management Function

- Work with managers to **assess and quantify risks**.
- Provide a **solid or dotted reporting line** for risk representatives.
- Support the operational risk system used by the business to track their risks.
- Benchmark **good industry practice**.
- Provide risk oversight.
- Ensure issues are **properly escalated**.
- Conduct **qualitative operational risk** analysis e.g.
  - HR reports from exit interviews
  - **Internal audit reports**, and the rate at which audit points are closed by the business
- Conduct statistical modelling to quantify the firm's operational risk profile for regulatory and other purposes

Operational Risk Framework

Management of Risk and Reduction of Potential Impact and Likelihood of Occurrence

The key to reducing the likelihood of a risk materialising is to:

Clearly identify the risk **before it occurs**

Establish **clear ownership** for the risk

Set up and monitor appropriate **risk indicators**

If the risk does materialise, its impact can be reduced by ensuring:

Speedy **escalation to senior management** if their help is necessary

An owner will be **assigned to fix** the problem

Appropriate **insurance policies** are in place

EMERGING MARKET FINANCIAL TRAINING

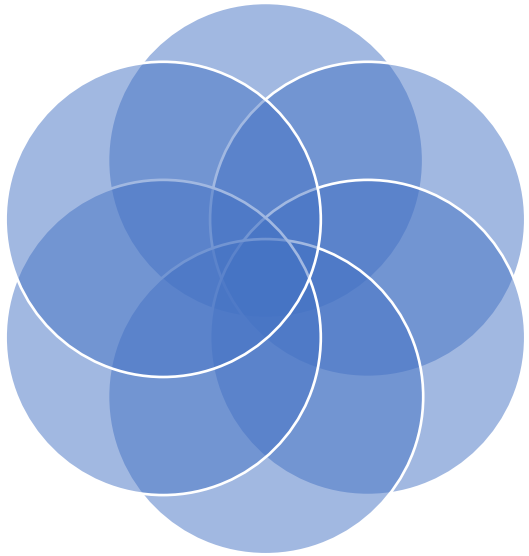
Operational Risk Framework

Identification and Assessment of Risks

Clearly identify the firm's risks using methods such as :

Self-assessment

Audit reviews



key risk indicators (KRIs)

External loss data

Risk and control assessment workshops

Loss data causal trend analysis

Operational Risk Management

Operational Risk Management

Risk identification – clearly **identify the firm's risks** using methods such as self-assessment key risk indicators (KRIs) risk and control assessment workshops, loss data causal trend analysis, external loss data, audit reviews.

Risk measurement and assessment – score the impact and the **likelihood of the risk** against pre-defined criteria.

Management and control – ensure **appropriate controls** are in place to mitigate the risk.

Risk monitoring – **monitor the risk and control indicators** and other risk management information (MI), and act before they reach their predefined danger limits.

Risk reporting – reporting of risk MI should include indicators, the risks and controls to which they relate.

Operational risk policy – lessons learned during the operation of the risk framework are used to update the policy.

Question time

What is Operational Risk?

A. Risks that affect one firm, or a group of firms, can affect the stability of the whole financial system

B. Risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

c. Risk of loss arising from changes in the value of financial instruments.

D. Risk is the exposure of a firm's financial condition to adverse movements in interest rates.

Operational Risk Identification

Operational Risk Identification and Categorisation

Identifying and categorising operational risks helps firms to establish their risk profile and appetite for risk.

Categorising the risks will enable:

The provision of more succinct **management risk information**.

A better understanding of where in particular the firm's operational weakness lie **processes , systems ,people vulnerability to external events**

A sound basis for **operational risk capital** allocation across the different categories

A common language for **discussing, assessing and managing risk** that allows clear and transparent communication and decision-making

Self-Assessment Risk Identification

This involves a checklist of the risks that a particular area of the firm faces

Self-assessment as a single method of measurement has limitations as:

It is subjective and open to abuse and manipulation by managers. So, it should be independently validated

Combining the scores received from the participants for each risk into a single score for that risk can be difficult

Application of Risk Categorisation

People risks	Process risks	System risks	External event risks
Inadequately defined roles and responsibilities	Lack of written procedures	System unavailable during peak hours	Threat of terrorist action
Lack of succession plan for key staff	Absence of defined process	Data becomes subtly corrupted	Customer commits fraud against the firm
Staff not competent for role	Manual intervention causes pinch-points	Passwords being shared by staff	Outsource supplier delivers late
Improper staff conduct	Absence of escalation procedures	Denial of service (DoS) attacks	

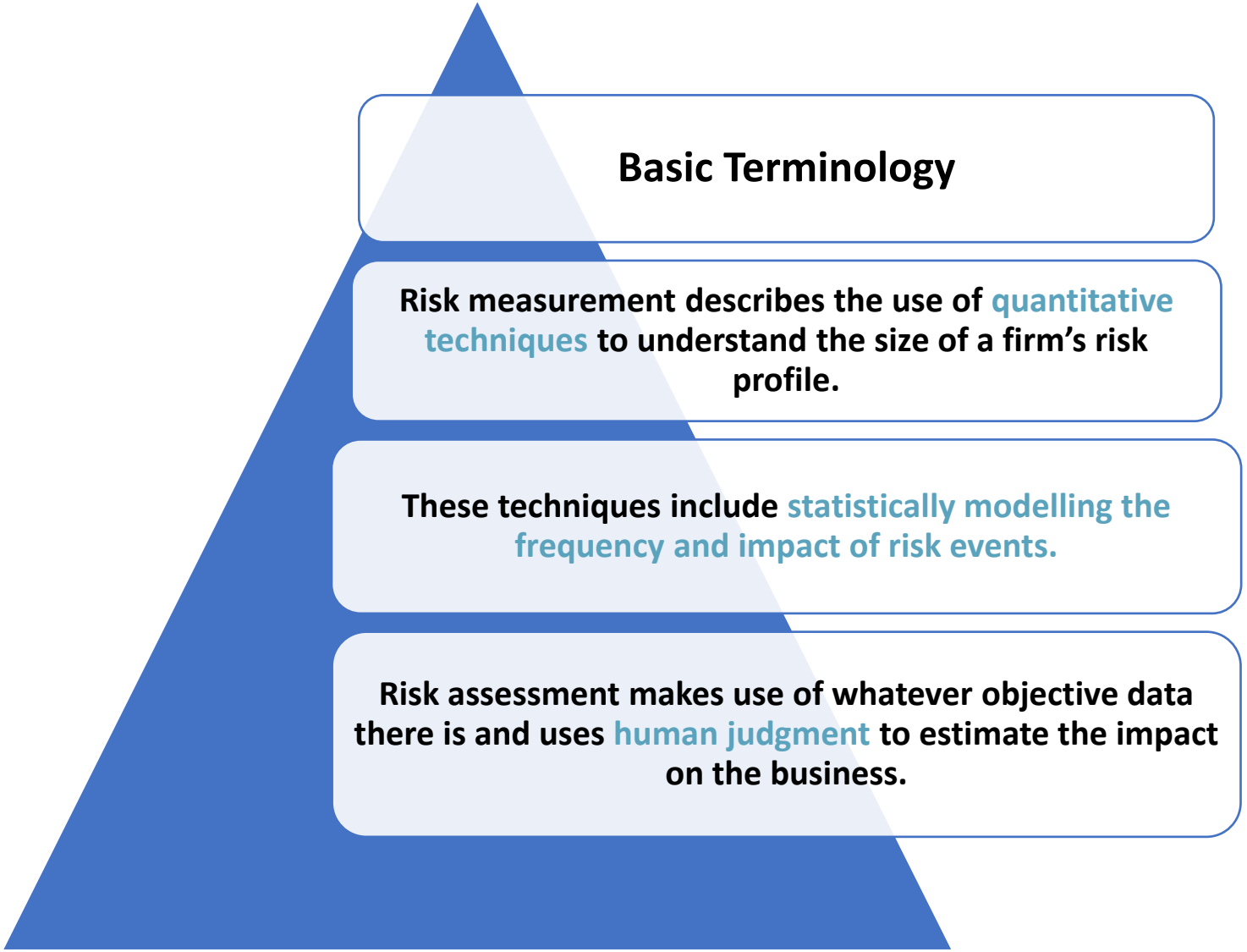
Operational Risk Assessment and Measurement

Risk assessment and risk measurement are both concerned with understanding the likelihood of risks occurring and their potential impact on the business.

The reasons for measuring and assessing operational risk are to:

- Establish a **quantitative baseline** for improving the control environment
- Provide an **incentive for risk management** and the development of a strong risk culture
- Improve **management decision-making**
- **Satisfy regulators and shareholders** that a firm is adopting a proactive and transparent approach to risk management
- Make an assessment of the **financial risk exposure** that can be used for capital allocation purposes

Operational Risk Assessment and Measurement



Methods of Assessment

Impact and Likelihood Assessment

Likelihood Probability Ratings

- Very low
  not likely to occur within the next ten years
  rating score = 1
- Low
  likely to occur within the next three to ten years
  rating score = 2
- Medium
  likely to occur within the next two to three years
  rating score = 3
- High
  likely to occur within the next year
  rating score = 4

Impact Loss Ratings

- Very low
  under £1,000
  rating score = 1
- Low
  £1,000 to £10,000
  rating score = 2
- Medium
  £10,000 to £50,000
  rating score = 3
- High
  above £50,000
  rating score = 4

The overall risk score is the product of the likelihood rating scores and the impact rating scores:

Risk score = likelihood score × impact score

Methods of Assessment

Typical Heat Map

Methods of Assessment

Advantages of an impact and likelihood assessment

- It provides a simple method for viewing the **range of risks** the business faces.
- It provides an evaluation of the effectiveness of the **control environment** if gross and net risk scores are plotted separately.
- It focuses **management attention** on the most important risks.
- It can be used with **minimal hard data**.
- It can capture a wide **range of risk possibilities** – from large, strategic risks to everyday, more detailed issues.
- It encourages a **risk-aware culture** and a more transparent risk environment.

Disadvantages of an impact and likelihood assessment

- It may present an over **simplified, subjective overview**

All subjective assessments should be validated by

- Real loss data
- An independent party, such as internal audit, a central risk function or peer review

Methods of Assessment

Scenario Analysis

- Scenario analysis is a **'top-down' method** of highlighting potential risk combinations in order to allow preventative action to be taken.
- It uses the experience of business professionals to capture possible scenarios that have occurred in the past or may result in loss in the future.

Bottom-Up Analysis

- The bottom-up measurement approach seeks to **analyse the individual risks** and adequacy of controls across business processes.
- It is called 'bottom-up' because it builds up a detailed profile of the risks that occur in each area.

Methods of Assessment

Advantages of bottom-up analysis

- It addresses risk and control issues at the process level.
- Accountability and responsibility for risk management can be clearly defined.
- It encourages a more transparent and risk aware culture.
- It encourages continuous improvement
- It can improve the quality of management information.

Disadvantages of bottom-up analysis

- It takes time to implement.
- It can be subjectively influenced by managers if not properly managed.
- Aggregating risks 'upwards' is not straight-forward.

Question time

Which of the following falls under People Risk ?

A. System unavailable during peak hours

B. Inadequately defined roles and responsibilities

C. Threat of terrorist action

D. Lack of written procedures

Key Risk Indicators (KRIs)

Factors will influence the likelihood of this risk occurring

- Example:
  Key Risk: Loss of Key Staff
- *General staff turnover as a proxy for key staff turnover.*
- *Percentage of undocumented processes*
- *Salary gaps identified by the annual salary benchmarking tests.*

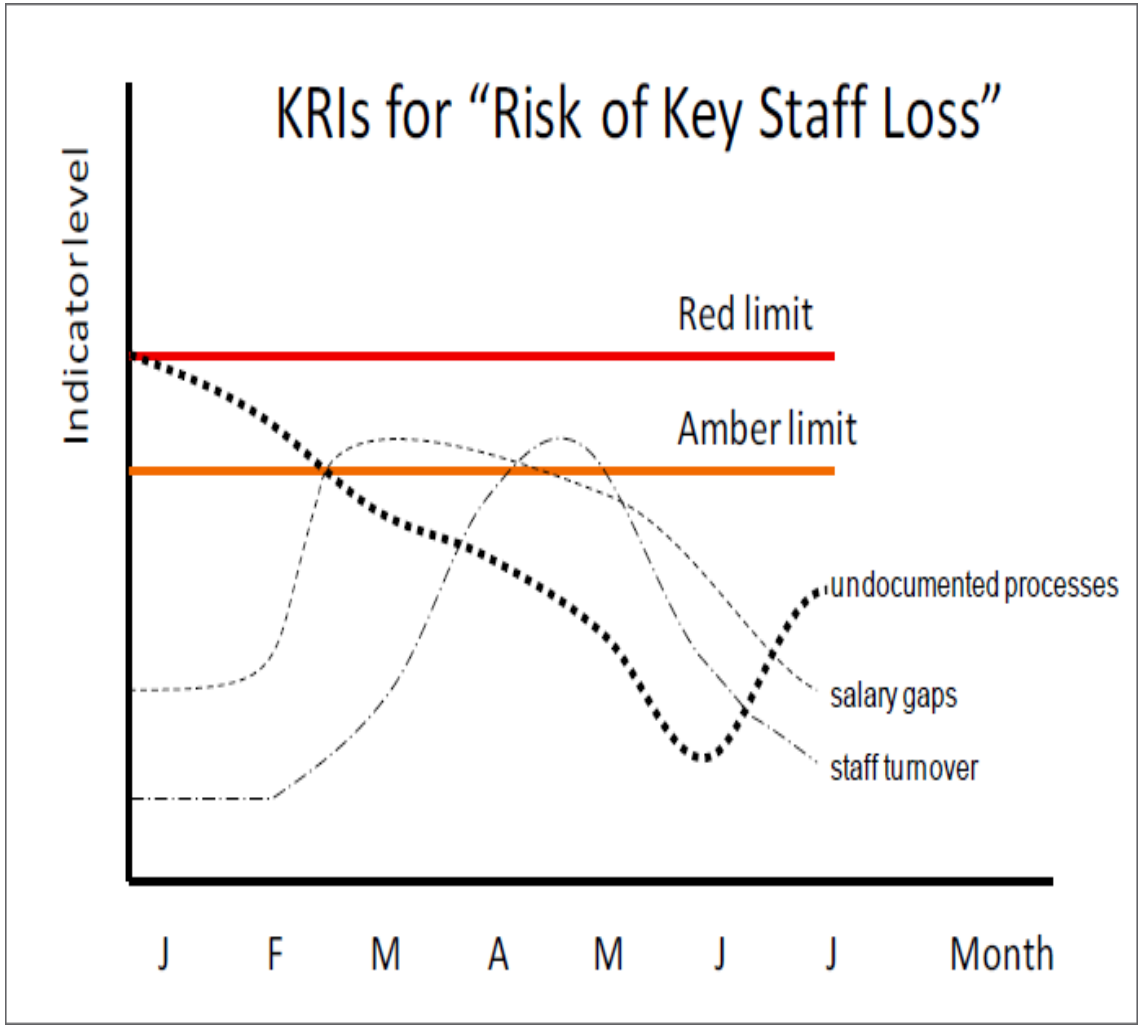
The firm can designate the top 'x' risks as its key risks.

It is possible to obtain data that describes the current status of those key risks, and to define upper and lower acceptable limits on the behaviour of this data.

This approach provides indicators on the firm's key risks, or it produces a series of key risk indicators (KRIs).

Key Risk Indicators (KRIs)

- *Good progress has been made in reducing the percentage of undocumented processes, although this is now starting to rise again. This increases the risk that key staff might leave without a proper hand-over being possible.*
- *In February, when the results of the annual salary benchmarking became available it became evident that some staff were being paid below market levels. This was followed a few months later by an increase in staff turnover. The salary gaps have since been closed, and turnover has declined to within tolerance.*
- *In summary, the three indicators together point to an overall reduction in the likelihood of key staff leaving.*



Key Risk Indicators (KRIs)

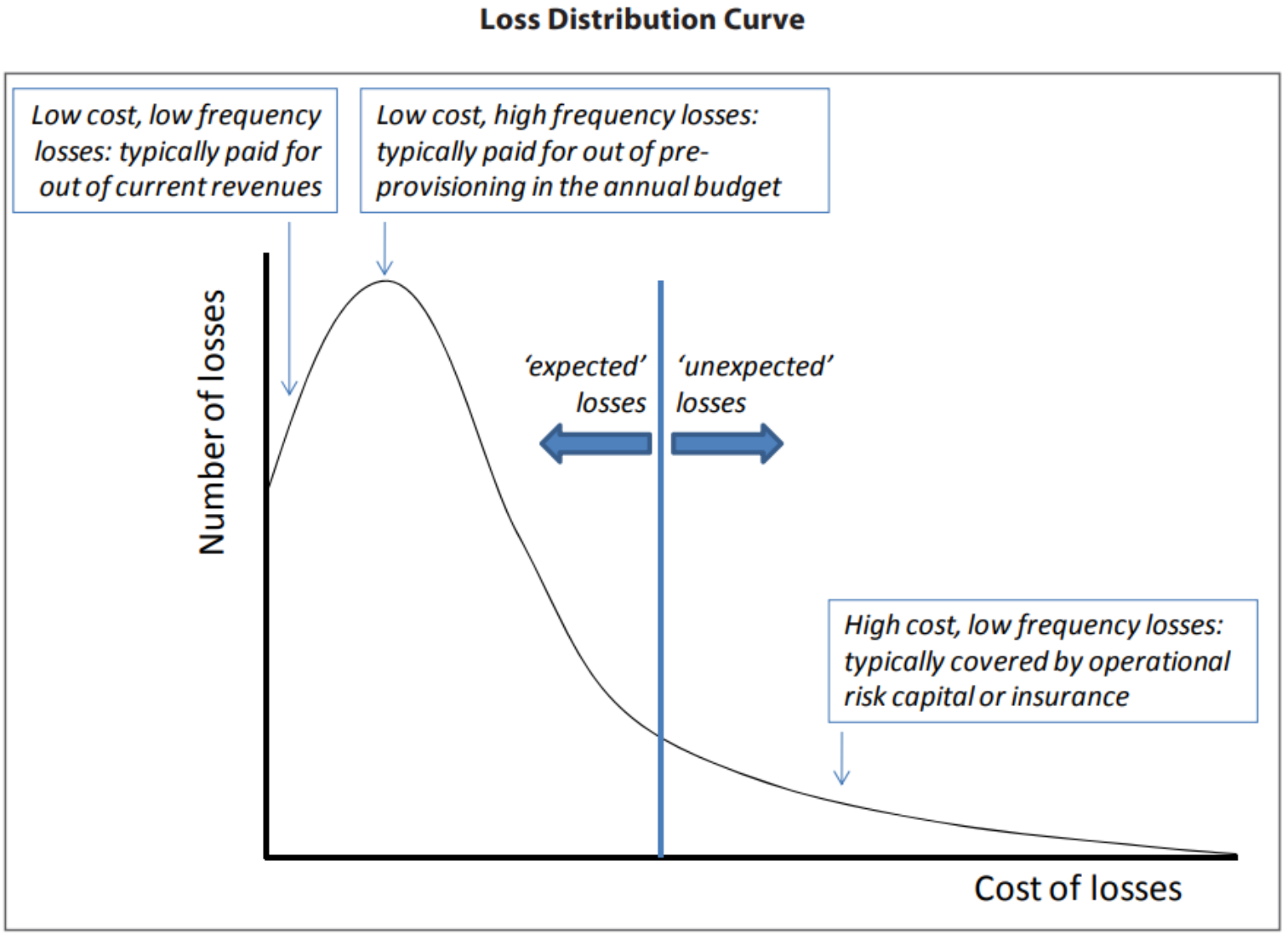
Advantages of using KRIs

- They allow trends to be **monitored** and can therefore be used to anticipate problems.
- They allow limits of **acceptability** to be established.
- They can provide a basis for **objective risk measurement.**

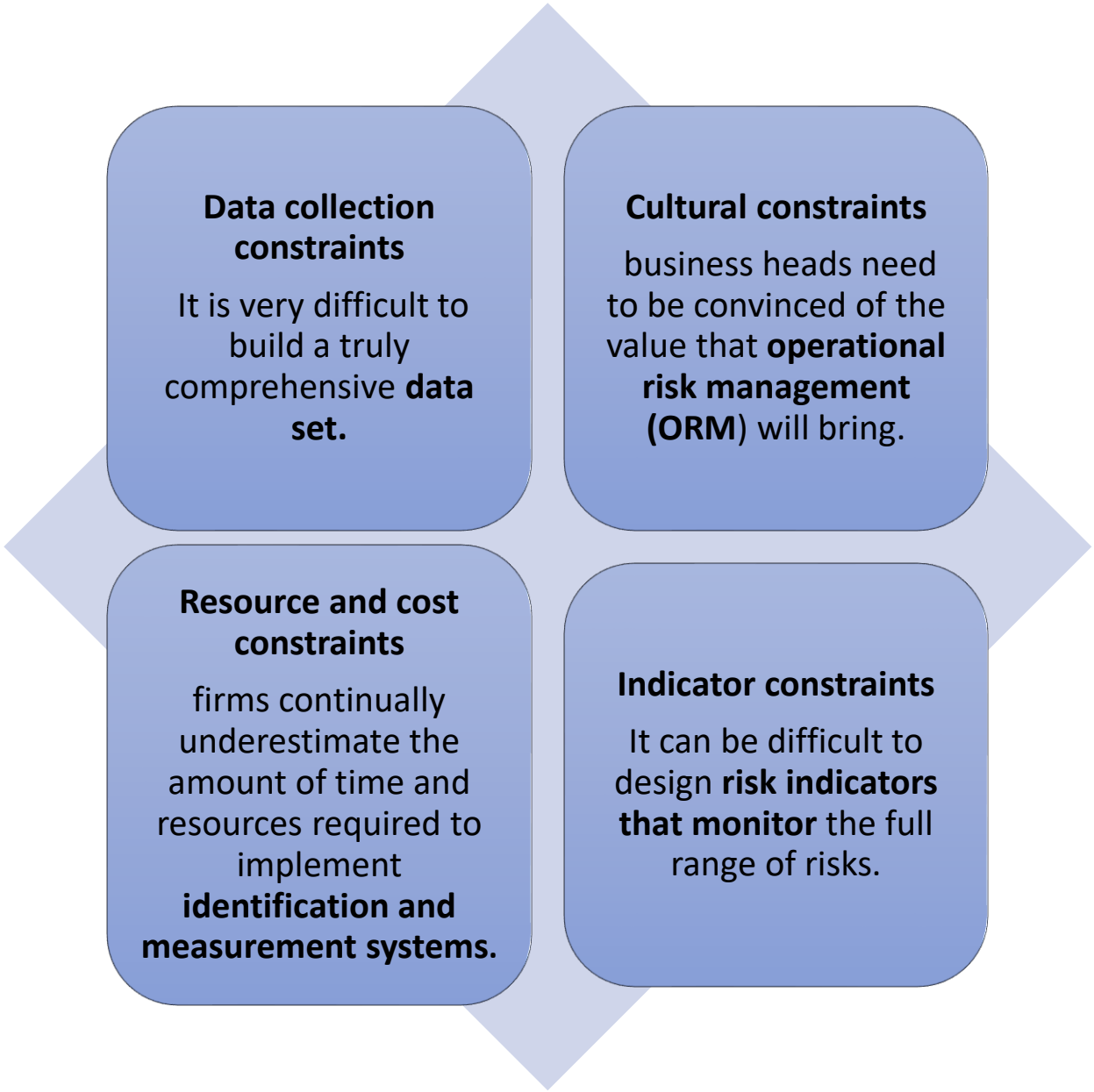
Disadvantage of using KRIs

- Any system of business measurement, is that they can cause skewed **business performance** if managers start 'managing to their KRIs' in an attempt to enhance their bonus ratings.

Historical Loss Data



Practical Constraints on Implementing a Framework



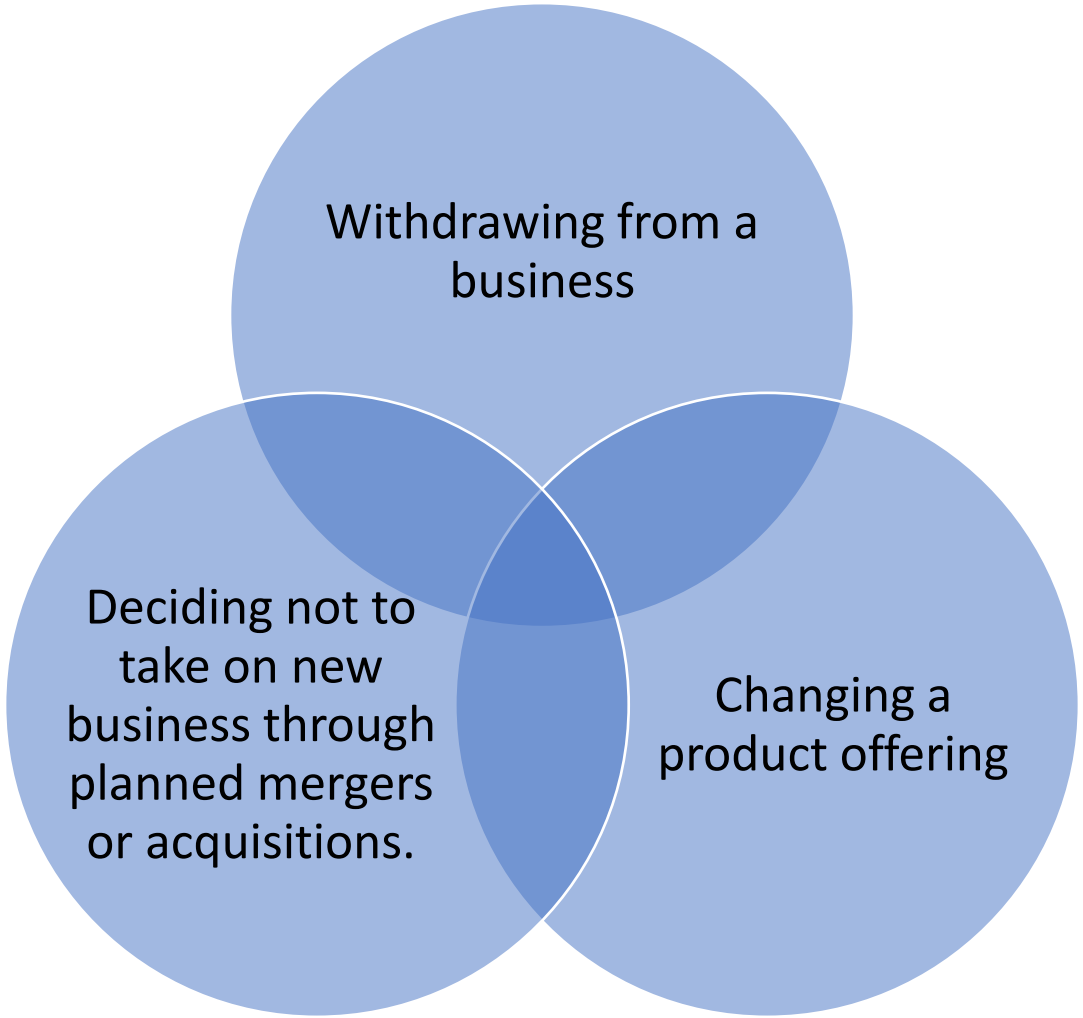
Managing Operational Risk

A Risk Register and its Core Features

The risk register's column headings

- Objectives, processes or products affected by this risk
- Description of risk
- Risk ranking
- Lead person or department
- Action plan
- Target and completion dates
- Sources of assurance and oversight (which may or may not be the lead person or department)
- Mitigating controls, their effectiveness and owner(s)

Methods for Managing Operational Risk Exposure



Operational Risk Mitigation

Controls	• All processes should have controls and check points designed into them to detect errors and prevent fraud and theft.
Business Continuity Planning (BCP) and Disaster Recovery (DR)	• A business continuity plan (BCP) - deals with the **premises and people aspects** • Disaster recovery (DR) - deal with the **IT and other infrastructure**
Outsourcing	• A firm may choose to outsource some aspects of its business to a third party with specific expertise in managing certain risks.
Insurance	• **Insurance policies** can be constructed to cover losses due to fire, theft and losses caused by human error.
Information and Cyber Security	• **Information and cyber security** continues to be high on most corporate agendas in response to the increasing threat from cyber criminals.

Information and Cyber Security -Information risk management regime

Secure IT systems	• Remove or disable unnecessary functionality from IT systems, and keep them patched against known vulnerabilities
Network security	• Connecting to untrusted networks (such as the internet) can expose your organisation to cyber attacks
Penetration testing	• Also called ‘pen testing’ or ‘ethical hacking’ is a systematic process of probing for vulnerabilities in networks and applications.
Managing user privileges	• Users of your IT systems should only be provided with the user privileges that they need to do their job.
User education and awareness	• Produce user security policies that describe acceptable and secure use of your organisation’s IT systems.

Question time

What is Penetration Testing?

A. Removing or disabling unnecessary functionality from IT systems.

B. Systematic process of probing for vulnerabilities in networks and applications.

C. Connecting to untrusted networks.

D. Continuously monitor inbound and outbound network traffic.

Information and Cyber Security - Information risk management regime

Incident management	• Establish an incident response and disaster recovery capability that addresses the full range of incidents that can occur.
Malware prevention	• Viruses and other malicious software are known as malware. Produce policies that directly address the business processes that are vulnerable to malware.
Monitoring	• Continuously monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate attacks and the compromise of data.
Removable media controls	• Where the use of removable media is unavoidable limit the types of media that can be used together with the users, systems, and types of information that can be transferred.
Home and mobile working	• Assess the risks to all types of mobile working where the device connects to the corporate network infrastructure

Operational Risk Mitigation

Physical Security	• The operational risks associated with physical security can be reduced by firms making often quite **simple arrangements**
Risk Awareness Training	• **Risk awareness training** for all relevant staff should be given by the firm to help staff understand the principle of reducing the likelihood of risk occurring.
Data Protection	• Firms are legally obliged to take the greatest care with **data relating** to their customers.

Operational Loss Data

Escalation thresholds	• These can be defined so that losses of various amounts are escalated to **pre-defined levels** within the organisation.
Loss causal analysis	• If the underlying cause(s) of a loss can be understood, then there is a greater chance of preventing a similar occurrence of the same issue elsewhere in the firm.