Introduction to risk, risk types and operational risk

Risk could be seen as an upside or downside event. A downside risk event could potentially cause a loss, while an upside risk event could potentially cause a profit or a loss.

Risk can be defined as the uncertainty of an event that could cause a loss or ensure a positive outcome if such an event occurs; the more uncertain the outcome of an event, the higher the risk, while the more certain the outcome of the event, the lower the risk.

Risk management: can be regarded as the process of managing risk exposures with the objective of preventing a loss event from occurring or minimising the effects should such an event occur.

Classification of risks

Risks of an enterprise can essentially be classified into two main categories

- Financial risks
  - Credit risk
  - Market risk
  - Liquidity risk
    - Risk Factors
      - Interest rates
      - Exchange rates
- Non-financial risks
  - Operational risks
  - Legal risk
  - Strategic risk
  - Reputational risk
    - Risk Factors
      - People
      - Technology
      - Regulations
      - External factors
      - Processes
Non-financial risks could be described as those risk exposures that could negatively influence the operations of an organisation and ultimately incur losses of quantitative nature, indirectly influencing the profitability of the business.

Financial risks could be seen as those risk exposures that will lead to a direct financial loss and negatively influence the profitability of the organisation.

**Enterprise risk management**

Enterprise risk management is the culture, processes and tools to identify strategic opportunities and reduce uncertainty. It is a comprehensive view of risk both from operational and strategic perspectives and is a process that supports the reduction of uncertainty and promotes the exploration of opportunities.

An enterprise risk management approach will ensure that risk exposures are managed in such a way that it will optimally protect and enhance the shareholder value of the organisation.

Enterprise risk management: a systematic process embedded in a company’s system of internal control to satisfy policies approved by its board of directors, aimed at fulfilling its business objectives and safeguarding both the shareholder’s investment and the company’s assets.

The purpose of the enterprise risk management process is to manage and effectively control risk appropriately within the company’s overall risk appetite.

An enterprise risk management approach can provide:

- Improved business performance
- Increased organisational effectiveness
- Better risk reporting

During the risk-reporting process, the board of directors can get an overview of all the risk exposures and information to make realistic decisions regarding the risk appetite of the organisation.

Factors that ensure an effective approach to enterprise risk management:

- Risk management culture
- Common risk language
- Risk reporting
- Benefits
A risk management culture can be regarded as the overall accepted and promulgated approach to risk management in the organisation. The culture should ensure that risks are managed based on clearly defined management principles that will ensure total involvement by all employees in the risk management processes as part of their daily responsibilities.

The common risk language for the organisation should support an enterprise risk management approach with the aim of aligning strategies, processes, people and technology. Furthermore, it will make sure that all employees understand the risk-related concepts, definitions and references for the organisation and ensure their cooperation during the risk management processes.

Internal risk management policies and procedures are an important method of promoting a common risk language for an organisation. These policies and procedures should incorporate detailed definitions of risk management concepts and responsibilities, which will guarantee a common understanding of the organisation's approach to risk management.

There are various benefits, which could add value to a successful enterprise risk management approach. These potential benefits ensure the following:

- The organisation has an overview of all the risks it's facing.
- There’s adequate information in order to formulate a realistic enterprise-wide risk appetite.
- There’s a common understanding of the risk management approach of the organisation.
- There’s total involvement of all employees at all management and operating levels, which could guarantee dedication towards cooperation between cross-functional departments.
- There’s sound decision making.
- There are effective risk management policies and procedures in place, promoting the responsibilities of employees with regard to risk management.
- There’s an integrated approach to risk management throughout the organisation, leading to proactive action to prevent risk events influencing all functions.
- There’s effective risk reporting. According to Deloach (2000: 8), one of the single most important benefits of enterprise risk management is that it provides greater confidence and relevant summary of information, to the board, chief executive offer (CEO) and management, that risk
opportunities are being systematically identified, rigorously analysed and effectively managed on a continuous and enterprise-wide basis.

- There’s increased organisational effectiveness. An enterprise risk management approach will provide the top-down coordination necessary to make various functions work efficiently and to address individual risk and interdependencies.

- There’s a coordination approach to risk management between key role players such as the board of directors, risk management, internal audit and business managers.

- There’s improved business performance in the organisation adopts a portfolio view of all risks; manages the interdependence between risk types, capital, and profitability; and rationalises the risk transfer strategies of the organisation. These efforts support key management decisions such as capital allocation, product development and pricing, merger and acquisitions and outsourcing, which, in turn, could lead to an improved business and an enhancement of shareholder value.

- The organisation has a competitive edge by being able to identify risks at an early stage (early warning), which enables it to position itself to exploit profitably the financial risks and control the non-financial risks also faced by competitors.

**Financial risk**

Financial risk is speculative in nature, which means it entails ventures that could result in a profit or loss.

Chapman (2000: 8) states that financial risk is the exposure of an organisation to adverse events that erode profitability and in extreme circumstances bring about business collapse.

The upside of a risk event can be regarded as the positive outcome.

According to Valsamakis, Vivian and Du Toit (2010: 302), it is generally accepted that speculative risk rarely insured for the following reasons:

- There are limited adequate statistics available to predict the probability of a loss.
- The probability of a loss may be too high to make insurance a practicable mechanism to cover a loss.
- The insurance premium might be too high, which will defeat the objective of a speculative risk, which is to make the highest possible profit.
Hedging: A hedge is an investment to reduce the risk of adverse price movements in an asset. Normally, a hedge consists of taking an offsetting position in a related security. Referred to as derivative risk.

A derivative is a security with a price that is dependent upon or derived from one or more underlying assets.

The function of derivatives is the redistribution of risk.

**Credit risk**

Credit is the risk that a counterparty to a financial transaction may fail to perform according to the terms and conditions of the contract. Credit can thus be described as a loss that an organisation could suffer as a result of a borrower of a loan who cannot comply with the agreement to repay the loan within a specific period. It is also known as default risk, because a customer defaults on the payment of invoices.

Chapman (2008: 207-208) states that credit risk may have three main components, namely default, exposure and recovery.

Default risk: This is regarded as the probability that a customer will fail to pay back a loan, meaning that the customer is in breach of contract and therefore “at fault”.

Exposure risk: this relates to the uncertainty surrounding the payment of agreed-upon future amounts. According to Chapman (2008:208), the source of this risk lies primarily in market environments. For examples, should interest rate increase, a borrower might not be able to afford the higher premiums and will therefore default.

Recovery risk: This relates to uncertainty over the possibility of recovering the outstanding amounts after a customer defaults on payments. Should a bank, for example, fail to recover any outstanding debt, that bank will suffer a loss due to a credit risk event.

A general approach to managing credit risk involves:

- 1st the establishment of credit policies guidelines to prescribe certain credit limits and a regular review of these limits.
- 2nd counterparty creditworthiness is evaluated and limits are set before credit is granted.
- 3rd loans are managed on an ongoing basis in customers have specialised credit departments to manage their credit risk.

**Market risk/price risk**

Market or price risk: is the risk of a decrease in the value of a financial portfolio as a result of adverse movement in market variable such as prices, currency exchange rates and interest rates.

Market risk can be measured according to two approaches:

- **Value-at-Risk (VaR)**, which is a measure of the risk involved in a portfolio of financial instruments. According to Olson and Wu (2008: 19), VaR can be characterised as a maximum expected loss, given a certain time horizon and within a given confidence interval, usually using a 99th percentile.

- **Scenario analysis**, which refers to varying a wider range of parameters at the same time. It examines the impact of catastrophic events on an organisation’s financial position. Stress testing typically refers to shifting the values of the individual parameters that affect the financial position of an organisation, and then determining the effect on the organisation’s business (Olson and Wu, 2008: 25)

Market risk is also regarded as the exposure of an organisation to a potential loss arising from diminishing sales or margins as a result of changes in market conditions, outside the control of the organisation.

The factors influencing market risk are, for example,

- Price variation
- Market growth
- Interest rates
- Foreign exchange rates
- Equity
- Commodity risks

Financial risks deals with the uncertainty of factors such as,

- Interest rates
- Exchange rates
- Share prices
- Commodity prices
- (and therefore it is clear that market risk falls within the scope of financial risk category)

Derivatives: are financial instruments the returns of which are derived from those of other financial instruments and who performance, therefore, depends on the performance of those instruments. “Derivatives serve a valuable purpose in providing a means of managing financial risk”.

Derivatives can transfer, at a price, any undesired risk to other parties who want either to assume risk or have other offsetting risks.

Derivatives are contracts between counterparties and aim to cover the following types of risks exposures:

- Interest rates
- Foreign currency exchange rates
- Commodities (such as energy, bullion, base metals and agriculture)
- Equities

Derivatives are divided into three main groups:

- **Forwards and futures**, which are used mainly as anticipatory hedges (in anticipation of having to buy and sell a specific asset in the future)
- **Options**, which are used to provide leverage or gearing (small amount of money enabling a similar return; or the same amount of money achieving an enhanced return)
- **Swaps**, which allow investors to transform current commitments in an attempt to match up with changing circumstances and expectations.

In summary, market risk is the exposure arising from adverse changes in the market values (the price) of a financial instrument or portfolio. Market risk also exists whenever a financial organisation, such as a bank, take trading, banking and investment positions. Major exposure to market risk occurs in formal financial and over-the-counter markets, both in South Africa and internationally.

**Interest rate risk**

The interest rate is part of a government’s monetary policy to control the money supply of a country.

Interest rate risk is the risk of a loss that an organisation could suffer as a result of adverse consequences due to fluctuations in interest rates.
Interest rate risk is known to fluctuate and is by nature speculative type of financial risk, since interest rate movements can result in profits or losses. It can thus be argued that interest rate depends on the state of the economy.

The interest is regarded as an important component of a bank’s rating, since it affects different areas of a bank’s finances, including net interest margins and the value of fixed-rate loan portfolios.

**Country risk**

Effective management of country risk requires an integration of assessments, policies and processes, as well as internal and external information. A bank, for example, is exposed to country risk through transactions with counterparties in foreign countries. Risk arises when conditions or events in a particular country reduce the ability of counterparties in that country to meet their obligations. These conditions could include things such as the imposition of exchange controls, a debt moratorium, insufficient foreign exchange, political instability and civil war.

**Liquidity risk**

Liquidity is an organisation’s ability to meet its financial obligations within a given time period.

Liquidity is the risk that an obligation may be unable to meet its financial obligations to counterparties. This risk will be reflected in insufficient funds or marketable assets being available.

The ultimate responsibility for drafting liquidity policies and reviewing liquidity decisions lies with the highest level of management.

Chapman (2008: 144) states that liquidity is an important measure of risk exposure. It is vital to a business that there are sufficient liquid resources available to meet maturing obligations.

Liquidity risk can occur when an organisation has more assets than liabilities, but at a certain given time, the organisation is unable to liquidate those assets in order to meet the immediate demands.

There are certain common factors that could influence an organisation’s financial risk. These financial risk factors such as interest rates and exchange rates could influence an organisation’s credit, market and/or liquidity risks.
**Exchange rate risk/Foreign exchange risk**

An exchange rate risk is also known as currency risk or foreign exchange risk (forex risk).

In order to mitigate this risk factor, investors will usually consider a hedging strategy.

**Non-financial risk**

Non-financial risk are those risks usually resulting in a loss to the organisation and where an amount is usually written off after processes to recover part of the loss by means of insurance or recovery procedures.

Non-financial risk is very difficult to quantify therefore making it very difficult to manage.

Typical risk types that fall under non-financial risks are:

- Strategic risk
- Reputational risk
- Legal risk
- Operational risk

**Strategic risk**
Strategic risk is how much risk can be taken to help achieve business objectives, while respecting the constraints within which the firm operates.

Factors for a sound business strategy:

- Determining the roles and responsibilities of all role players, including the board of directors, for the implementation of a sound risk management process to manage the risks proactively, and
- Ensuring the continuous monitoring of progress to achieve the business objectives.

The following strategic risks will influence the business strategy, once formulated:

- **Risk culture of the organisation.** If a strategy is aligned with the culture of the organisation, which includes the values and management principles, the chances of a successful strategy is high.
- **External risks.** There are various external risks an organisation faces during the implementation of a strategy. For example, the so-called triple bottom line such as the economic, environment and social aspects of the organisation’s activities.
- **Time factor.** A good business strategy is dependent on the correct timing. Should the strategy be implemented at the wrong time it could lead to the failure of the business.
- **Legislation.** It is important that the organisation have sound legislation processes, which will, for example, ensure accurate business contracts especially if the strategy is dependent on external contractors.
**Reputational risk**

Reputational risk is the negative exposure of an organisation’s business practices and/or internal controls that may cause a decline in the customer base and/or a reduction in revenue.

Possible effects of reputational risk include the following:

- A loss of customers and business
- A loss of income
- A loss of the company’s image and branding
- A negative influence on the employees in terms of morale and their confidence in the company
- A decline in the company’s share price and subsequent loss of investors
- A loss of the company’s market share regarding its products/services
- An increased focus on the company’s governance by regulators and external auditors, which could be costly in terms of employees’ time

Organisations should monitor the exposures to reputational risks closely in order to establish an adequate reputational risk strategy. Such a strategy will prepare an organisation to mitigate and deal effectively with these reputational risk events. The following are examples of reputational risk events:

- Fraud and bribery
- Key service interruptions by inadequate systems or viruses
- Poor quality of outsourced contractors
- Poor quality of services and/or products
- Poor customer service
- Joint ventures with other organisations with a bad reputation
- Breaches of law and regulations

**Legal risk**

Legal risk is regarded as the risk arising from violations of or non-conformance with laws, rules regulations, prescribed policies or ethical standards. The risk also arises when laws or rules governing certain products or activities of an organisation’s customers may be unclear or untested.
Non-compliance exposes the organisation to fines, financial penalties, payment of damages, and the voiding of contracts.

Legal claims against an organisation could be disastrous to an organisation and lead to liquidation. Therefore, it is important for an organisation to be prepared to deal successfully to such claims. This can be achieved by means of insurance policies for example.

**Operational risk**

**Defining operational risk**

Causes and effects of operational risk

<table>
<thead>
<tr>
<th>Risk factor/cause</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>People (loss of key staff)</td>
<td>Loss of revenue due to a shortage of experienced staff to do the work</td>
</tr>
<tr>
<td>Process (incorrect data input)</td>
<td>Loss due to a shortcoming in the process used to validate data</td>
</tr>
<tr>
<td>Systems (system downtime)</td>
<td>Loss of business due to the fact that new deals could be captured and processed in time</td>
</tr>
<tr>
<td>External factors (floods)</td>
<td>Loss of buildings due to floodwater</td>
</tr>
</tbody>
</table>

One way of being proactive in managing operational risk is to link potential events to their causes

Causes and events

<table>
<thead>
<tr>
<th>Risk factors/causes</th>
<th>Events</th>
</tr>
</thead>
</table>
| People/employees    | - Errors
                        | - Internal fraud
                        | - Employment law
                        | - Employers’ liability
                        | - Absence/loss of key staff |
                        | - Wrongful trading            |
| Systems (technology)| - Systems failure
                        | - Systems integrity
<pre><code>                    | - Outdated systems           |
</code></pre>
<table>
<thead>
<tr>
<th>System suitability</th>
<th>System support</th>
</tr>
</thead>
<tbody>
<tr>
<td>External environment/factors</td>
<td>Business interruption</td>
</tr>
<tr>
<td></td>
<td>Natural disasters</td>
</tr>
<tr>
<td></td>
<td>Third-party theft</td>
</tr>
<tr>
<td></td>
<td>External fraud</td>
</tr>
<tr>
<td>Legal/regulatory</td>
<td>Non-compliance with standards</td>
</tr>
<tr>
<td></td>
<td>Changes in regulatory standards</td>
</tr>
<tr>
<td></td>
<td>Contractual failures</td>
</tr>
</tbody>
</table>

Causes and effects can be classified further according to the frequency of the events and their potential impact, as is shown in the following examples:

- **High-frequency/low-impact events.** For example, there are likely to be several possible causes (such as human error and system failure), which can result in the late settlement of a financial transaction.
- **Low-frequency/high-impact events.** For example, wrongful trading (insider trading) can result from ineffective controls

Operational risk can be broken down into two main risk factors, namely internal factors and external factors. Internal factors should be reviewed according to a set of three key components: capacity, capability and availability. The following questions could be asked if operational risk arises from people risk as an internal factor:

- *does the business have enough employees (capacity) to accomplish its objectives?*
- *Do the employees have the right skills (capability) to perform their duties effectively?*
- *Will the employees be there when required (availability)?*

External factors are analysed in terms of the specific type of external interaction with the business of an organisation, for example, customers are external to an organisation, but they could influence the business.

It is important that these internal and external risk factors are viewed in unison. The degree of interconnected risk exposure across the main factors of operational risk needs to be examined in order to understand the full impact of the risk.
From the various definitions and views on operational risk, it is evident that the main risk factors of operational risk include the following:

- **Processes**: the processes operated by the organisation
- **People**: the people employed by the organisation to help operate and manage the processes
- **Systems**: the systems used to support the processes
- **Impact of business strategy**: the impact on the people, processes and systems that the business strategy may have
- **External factors**: the risk resulting from the external environment in which the organisation operates

Interrelationship between the business environment, external risk factors and internal risk factors. – Figure 1.5 page 19 son

The factors within the overall framework of the organisation’s business strategy are – figure 1.6 boy, don’t fuck it up

These factors can be explained further as:

- **Processes.** Large organisations typically execute a large number of processes in order to deliver their services. These include processes for making payments, manufacturing products and negotiating contracts. Risks can arise at all stages of these processes.
- **People.** Although many operational risk incidents are said to be the result of major internal control failures, they are often, in fact the failures of people.
- **Systems.** Almost all services depend on information technology systems. Problems can arise from the corruption of data stored on the system, whether accidental or deliberate, for example, programming errors and fraud.
- **Business strategy.** Business strategy, in the form of mergers, takeovers, new products and services, and re-engineering projects, can have an important effect on processes, systems and people. It is important that operational risk issues are considered when a business strategy is decided upon.
- **External environment.** The external environment in which an organisation operates could give rise to operational risks. The organisation itself tends to have little or no control over the source of such risks. The risks could arise from compliance, legal and litigation issues; unanticipated tax changes; physical threats such as robberies and cash heists; and the effects of natural disasters such as earthquakes, tsunamis and tornados.

A further grouping of operational risk exposures:

<table>
<thead>
<tr>
<th>Risk factor</th>
<th>Risk exposure</th>
</tr>
</thead>
</table>
| Processes and systems     | - The risk of errors arising from information systems  
                          - The risk of systems failure, leading either to error or loss of the business  
                          - The risk arising from systems infiltration, e.g. computer hacking  
                          - The risk arising from inadequate processes, leading to time delays and inefficiency, and resulting in financial losses and loss of business |
| People                    | - The risk arising from the possibility of incompetent, inexperienced, unsuitable and/or negligent staff  
                          - The risk of human error with specific regard to processing  
                          - The risk that a working culture may lead to low morale, high turnover of staff, low concentration, low productivity and industrial action  
                          - The risk of fraudulent and other criminal activity  
                          - The risks associated with unauthorised and/or ill-informed decision making at all levels, particularly with regard to business strategy, projects management, change management, liquidity and outsourcing. |
| External factors          | - Acts of god  
                          - External criminal activities  
                          - Political upheaval  
                          - The regulatory, legal, tax, and business environment and any changes in that environment  
                          - Risks associated with third parties, e.g. suppliers and contractors  
                          - Deterioration of an organisation’s reputation as perceived by the market |
**Operational risk:** is the exposure of an organisation to potential losses, resulting from shortcomings and/or failures in the execution of its operations. These losses may be caused by internal failures or shortcoming of people, processes and systems, as well as the inability of people, processes and systems to cope with the adverse effects of external factors.

**Key driver that expose organisations to more risk**

- **Globalisation**
  - Globalisation is regarded as the continuous integration of economic, financial, trade and communications amongst countries and different regions. Countries are in effect forced to move away from a narrow, nationalistic to broader view to facilitate trade.

- **Organisations are becoming more complex**
  - Each jurisdiction will have its own rules, regulations and practices, which differ from what the holding company deals with in a particular country.
  - Organisations place a significant reliance on computer technology. The system architecture design and IT operations are complex and in general a long term process, which can make it difficult for organisations to change direction due to technological challenges and cost factors.

- **Regulatory environment is becoming more vigilant and onerous**
  - Governments are promulgating more laws and regulations for example the environment and consumer rights.
  - Closely regulated industries such as the bank and insurance companies are required to have levels of capital.

- **Focus on governance**
  - Stakeholders are demanding more from organisations with regard to governance and transparency. Countries across the world have implemented code of governance. Organisations in South Africa are encouraged to implement the King III on Governance.

- **Consumer demands**
  - Consumers are becoming more sophisticated and therefore demand product and services of higher quality. Consumer rights are also protected by the Consumer Protection Act, No. 68 of 2008, which came into effect April 2011.
Underlying Operational Risk Factors

1- People
   - Operational failures caused by staff are driven by the following:
     o **Error**: this refers to errors made in dealing with transactions or failure to follow required processes.
     o **Fraud**: This refers to deliberate action by staff to falsify records, valuations or transactions, and is generally due to dishonest behaviour.
     o **Dependency on key person(s)**: This refers to situations in which there is too great a reliance on an individual, or group of individuals, to perform certain functions. Reliance on key staff may expose the organisation without a suitable replacement being in place.

People risk: People risk can be defined as the risk of loss caused intentionally or unintentionally by an employee.

2- Systems (technology)
   - System risk includes all technology risk, including external pressure such as the risk of not keeping up with the progress of changing or developing a technology. Technology risk could arise from maintenance contracts for existing infrastructure, application software, and the complete outsourcing of projects or the whole information technology service.
   - Proactive preventative measures against typical technology risk exposure:
     o **Physical protection**: security measure to prevent theft.
     o **Functional protection**: back-up systems to ensure the continued functionality of the systems.
     o **Data protection**: Firewalls to prevent viruses.

3- Processes
   - Process risk is the risk of business processes being insufficient and causing unexpected losses. A proactive risk operational risk function should be able to address the risk involved in the event of any changes to, or developments of, processes during, for example, joint ventures, mergers, and the implementation and changing of new systems, as well as the re-engineering of processes.
- Processes form and integral part of operational risk and can thus be seen as one of its main underlying risk factors