**LECTURER NINE: CRITICAL RISKS IN AN ENTERPRISE**

I welcome you to the study of critical risks in an enterprise. In this topic we shall study the following: definition of terms e.g. risk, risk management and risk management process ; benefits of managing risk, processes of assessing business risks, the critical risk areas of in an enterprise, types of business risks, risk management strategies, and case study on business risk.

Kindly, make sure that:

You complete this lecture before proceeding to the next one.

* Refer to the suggested additional resources to get further information on each topic
* Make notes as to simplify your study
* Complete all activities and questions as you progress
* Spend at least 2 (two) hours to complete this topic for you to understand and apply the knowledge and skills acquired

|  |
| --- |
| By the end of the lecture, you should be able to:  i. Define the term risk, risk management and Risk Management Process  ii. Explain the benefits of managing risk.  iii. Demonstrate processes of assessing business risks  iv. Discuss the critical risk areas of in an enterprise.  v. Discuss the types of business risks strategies  vi Analyse a case study |

## What is a risk

Risk, in insurance terms, is the possibility of a loss or other adverse event that has the potential to interfere with an organization’s ability to fulfil its mandate, and for which an insurance claim may be submitted.

## What is risk management?

Risk management ensures that an organization identifies and understands the risks to which it is exposed. Risk management also guarantees that the organization creates and implements an effective plan to prevent losses or reduce the impact if a loss occurs.

## Benefits to managing risk

Risk management provides a clear and structured approach to identifying risks. Having a clear understanding of all risks allows an organization to measure and prioritize them and take the appropriate actions to reduce losses. Risk management has other benefits for an organization, including:

* Saving resources: Time, assets, income, property and people are all valuable resources that can be saved if fewer claims occur.
* Protecting the reputation and public image of the organization.
* Preventing or reducing legal liability and increasing the stability of operations.
* Protecting people from harm.
* Protecting the environment.
* Enhancing the ability to prepare for various circumstances.
* Reducing liabilities.
* Assisting in clearly defining insurance needs.

## CRITICAL RISK AREAS IN AN ENTERPRISE

Most risks in enterprise can be grouped into three general categories i.e. financial risks, operational risks and strategic risks. Enterprise risks may be broadly categorized into the following:

**1. Financial Risks**

This risk concerns the continuous financial position of an enterprise. Any kind of predisposition to activities that could result to possible loss of funds by the business is a financial risk. Financial risks may include credit risks, liquidity risks, interest rate risks, foreign exchange risks and investment portfolio risks.

**2. Operational risks**

These risks have to day with the enterprises internal day-to-day operations. An operational risk is, therefore, a function of internal controls, information systems, employee integrity, and operating processes. Examples of operational risks include:

**a) Transaction risk**

This is a risk that arises on a dailybasis in the business as transactions are processed. This risk is particularlyhigh for enterprises that handle a high volume of small transactions daily.

Common operational risks in the management of an enterprise include:

Inconsistencies between the inventory management system data and the accounting system data.

Inconsistent implementation of programs and strategies in the organization.

Poor record keeping that results in loss of finances

**b) Fraud risk:** Also referred to as integrity risk, fraud risk is the risk of loss of earningsor capital as a result of intentional deception by an employee or client. The mostcommon type of fraud in an enterprise is the direct theft of funds by employees. Other forms of fraudulent activities include the creation of misleadingfinancial statements, bribes and kickbacks.

**3. Strategic Risks**

Strategic risks include internal risks like those from adverse business decisions or improper implementation of those decisions, poor leadership, or ineffective governance and oversight, as well as external risks, such as changes in the business or competitive environment. These may include:

**a) Governance risk:** One of the most understated and underestimated risks within any organization arethe risk associated with inadequate governance or a poor governance structure.Direction and accountability come from the board of directors, who increasingly include representatives of various stakeholders in the business (investors, customers, institutional partners, etc). To protect against the risks associated with poor governance structure, businesses should ensure that their boards comprise the right mix of individuals who collectively represent the technical and personal skills and backgrounds needed by the institution.

**b) Reputation Risk:** This refers to the risk to earnings or capital arising from negative publicopinion, which may affect an enterprise’s ability to sell products and services or its accessto capital or cash funds. Reputations are much easier to lose than to rebuild, and should be valued as an intangible asset for any organization.Most successful enterprises cultivate their reputations carefully with specific audiences,such as with customers (their market), their funders and investors (sources of capital), and regulators or officials.

**c) External business environment risk:**  This refers to the inherent risks of the business’ activityand the external business environment. To minimize business risk, the enterprise must react to changes in the external business environment to take advantage of opportunities, to respond to competition, and to maintain a good public reputation. As in most businesses, it is often easier to focus on internal risks than to recognize shifts in the external marketplace that can potentially affect the enterprise. Businesses need to check the validity of their assumptions against the reality on a periodic basis, and respond accordingly. Anticipating and preparing for possible risks is the manager’s responsibility. Clients face the risk of loss of life, poor health, and risk on property through natural calamities. While external business risks are out of an enterprise’s direct control, the enterprise can still anticipate them and prepare for their impact.

**d) Regulatory and legal compliance risk:** Compliance risk arises out of violations of or non-conformance with laws, rules,regulations, prescribed practices, or ethical standards, which vary from country tocountry. The costs of non-conformance to norms, rules, regulations or laws rangefrom fines and lawsuits to the voiding of contracts, loss of reputation or businessopportunities, or shut-down by the regulatory authorities.

## DEVELOPING RISK MITIGATION STRATEGIES

Effective risk management requires an organization to take four key steps:

1. Identify the risks facing the institution and assess their severity (either frequency or potential negative consequences)
2. Measure the risks appropriately and evaluate the acceptable limits for that risk;
3. Monitor the risks on a routine basis, ensuring that the right people receive accurate and relevant information; and
4. Manage the risks through close oversight and evaluation of performance.

**RISK MANAGEMENT TECHNIQUES**

1. Risk avoidance
2. Risk reduction
3. Risk retention
4. Risk transfer

**Risk Management in Small Business**

Risk is defined as *the effect of uncertainty on objectives* (whether positive or negative). Risk management can therefore be considered the identification, assessment, and prioritization of [risks](http://en.wikipedia.org/wiki/Risk) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Risks can come from uncertainty in financial markets, project failures, legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attacks from an adversary. The strategies to manage risk include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk.

### Principles of risk management

The [International Organization for Standardization](http://en.wikipedia.org/wiki/International_Organization_for_Standardization) identifies the following principles of risk management:

Risk management should:

* Create value.
* Be an integral part of organizational processes.
* Be part of decision making.
* Explicitly address uncertainty.
* Be systematic and structured.
* Be based on the best available information.
* Be tailored.
* Take into account human factors.
* Be transparent and inclusive.
* Be dynamic, iterative and responsive to change.
* Be capable of continual improvement and enhancement.

## Risk Management Process

According to the standard [ISO 31000](http://en.wikipedia.org/wiki/ISO_31000) "Risk management -- Principles and guidelines on implementation," the process of risk management consists of several steps as follows:

### Establishing the context

Establishing the context involves:

1. **Identification** of risk in a selected domain of interest
2. **Planning** the remainder of the process.
3. **Mapping out** the following:
   * the social scope of risk management
   * the identity and objectives of stakeholders
   * the basis upon which risks will be evaluated, constraints.
4. **Defining a framework** for the activity and an agenda for identification.
5. **Developing an analysis** of risks involved in the process.
6. **Mitigation or Solution** of risks using available technological, human and organizational resources.

### Risk Identification

After establishing the context, the next step in the process of managing risk is to identify potential risks. Risks are about events that, when triggered, cause problems. Hence, risk identification can start with the source of problems, or with the problem itself.

### Risk Assessment

Once risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of the probability of an unlikely event occurring. Therefore, in the assessment process it is critical to make the best educated guesses possible in order to properly prioritize the implementation of the [risk management plan](http://en.wikipedia.org/wiki/Risk_management_plan).

The fundamental difficulty in [risk assessment](http://en.wikipedia.org/wiki/Risk_assessment) is determining the rate of occurrence since statistical information is not available on all kinds of past incidents. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for immaterial assets. Asset valuation is another question that needs to be addressed. Thus, best educated opinions and available statistics are the primary sources of information. Nevertheless, risk assessment should produce such information for the management of the organization that the primary risks are easy to understand and that the risk management decisions may be prioritized. Thus, there have been several theories and attempts to quantify risks. Numerous different risk formulae exist, but perhaps the most widely accepted formula for risk quantification is:

## Risk Options

Risk mitigation measures are usually formulated according to one or more of the following major risk options, which are:

1. Design a new business process with adequate built-in risk control and containment measures from the start.
2. Periodically re-assess risks that are accepted in ongoing processes as a normal feature of business operations and modify mitigation measures.
3. Transfer risks to an external agency (e.g. an insurance company)
4. Avoid risks altogether (e.g. by closing down a particular high-risk business area)

**Potential risk treatments**

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories:

* **Avoidance** (eliminate, withdraw from or not become involved)
* **Reduction** (optimise - mitigate)
* **Sharing** (transfer - outsource or insure)
* **Retention** (accept and budget)

#### Risk avoidance

This includes not performing an activity that could carry risk. An example would be not buying a [property](http://en.wikipedia.org/wiki/Real_property) or business in order to not take on the [Legal liability] that comes with it. Another would be not be flying in order to not take the risk that the [airplane](http://en.wikipedia.org/wiki/Fixed-wing_aircraft) were to be [hijacked](http://en.wikipedia.org/wiki/Aircraft_hijacking). Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits.

#### Risk reduction

Risk reduction or "optimisation" involves reducing the severity of the loss or the likelihood of the loss from occurring. For example, [sprinklers](http://en.wikipedia.org/wiki/Sprinkler) are designed to put out a [fire](http://en.wikipedia.org/wiki/Fire) to reduce the risk of loss by fire. This method may cause a greater loss by water damage and therefore may not be suitable.

#### Risk sharing

Briefly defined as "sharing with another party the burden of loss or the benefit of gain, from a risk, and the measures to reduce a risk." The term of 'risk transfer' is often used in place of risk sharing in the mistaken belief that you can transfer a risk to a third party through insurance or outsourcing. In practice if the insurance company or contractor go bankrupt or end up in court, the original risk is likely to still revert to the first party. As such in the terminology of practitioners and scholars alike, the purchase of an insurance contract is often described as a "transfer of risk." However, technically speaking, the buyer of the contract generally retains [legal responsibility](http://en.wikipedia.org/wiki/Legal_risk) for the losses "transferred", meaning that insurance may be described more accurately as a post-event compensatory mechanism. For example, a personal injuries insurance policy does not transfer the risk of a car accident to the insurance company. The risk still lies with the policy holder namely the person who has been in the accident. The insurance policy simply provides that if an accident (the event) occurs involving the policy holder then some compensation may be payable to the policy holder that is commensurate to the suffering/damage.

Some ways of managing risk fall into multiple categories. Risk retention pools are technically retaining the risk for the group, but spreading it over the whole group involves transfer among individual members of the group. This is different from traditional [insurance](http://en.wikipedia.org/wiki/Insurance), in that no premium is exchanged between members of the group up front, but instead losses are assessed to all members of the group.

#### Risk retention

Involves accepting the loss, or benefit of gain, from a risk when it occurs. True [self insurance](http://en.wikipedia.org/wiki/Self_insurance) falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. [War](http://en.wikipedia.org/wiki/War) is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

### Create a risk management plan

Select appropriate controls or countermeasures to measure each risk. Risk mitigation needs to be approved by the appropriate level of management. For instance, a risk concerning the image of the organization should have top management decision behind it whereas IT management would have the authority to decide on computer virus risks. The [risk management plan](http://en.wikipedia.org/wiki/Risk_management_plan) should propose applicable and effective security controls for managing the risks. For example, an observed high risk of computer viruses could be mitigated by acquiring and implementing antivirus software. A good risk management plan should contain a schedule for control implementation and responsible persons for those actions.

### Implementation

Implementation follows all of the planned methods for mitigating the effect of the risks. Purchase insurance policies for the risks that have been decided to be transferred to an insurer, avoid all risks that can be avoided without sacrificing the entity's goals, reduce others, and retain the rest.

### Review and evaluation of the plan

Initial [risk management plans](http://en.wikipedia.org/wiki/Risk_management_plan) will never be perfect. Practice, experience, and actual loss results will necessitate changes in the plan and contribute information to allow possible different decisions to be made in dealing with the risks being faced.

[Risk analysis](http://en.wikipedia.org/wiki/Risk_analysis_%28business%29) results and management plans should be updated periodically. There are two primary reasons for this:

1. To evaluate whether the previously selected security controls are still applicable and effective, and
2. To evaluate the possible risk level changes in the business environment. For example, information risks are a good example of rapidly changing business environment.

## Limitations

If risks are improperly assessed and prioritized, time can be wasted in dealing with risk of losses that are not likely to occur. Spending too much time assessing and managing unlikely risks can divert resources that could be used more profitably. Unlikely events do occur but if the risk is unlikely enough to occur it may be better to simply retain the risk and deal with the result if the loss does in fact occur. Qualitative risk assessment is subjective and lacks consistency. The primary justification for a formal risk assessment process is legal and bureaucratic.

Prioritizing the *risk management processes* too highly could keep an organization from ever completing a project or even getting started. This is especially true if other work is suspended until the risk management process is considered complete.

It is also important to keep in mind the distinction between risk and [uncertainty](http://en.wikipedia.org/wiki/Uncertainty). Risk can be measured by impacts x probability.