Risk management

Risk management is the identification, evaluation, and prioritisation of risks (defined in ISO 31000 as the effect of uncertainty on objectives) followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate event or to maximize the realization of opportunities.

Risks can come from various sources including uncertainty in financial markets, threats from project failures (at any phase in design, development, production, or sustainment life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters, deliberate attack from an adversary, or events of uncertain or unpredictable root-cause. There are two types of events; negative events can be classified as risks while positive events are classified as opportunities.

In ideal risk management, a prioritisation process is followed whereby the risks with the greatest loss (or impact) and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled in descending order. In practice the process of assessing overall risk can be difficult, and balancing resources used to mitigate between risks with a high probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled.

BeResilient is a programme fully funded by CITB

NFB BeResilient Business & Skills

Risk management

How to use it.

According to the definition to the risk, the risk is the possibility that an event will occur and adversely affect the achievement of an objective. Therefore, risk itself has the uncertainty.

For the most part, risk management consist of the following elements, performed, more or less, in the following order.

1. identify, characterize threats
2. assess the vulnerability of critical assets to specific threats
3. determine the risk (i.e. the expected likelihood and consequences of specific types of attacks on specific assets)
4. identify ways to reduce those risks
5. prioritise risk reduction measures

Tip! Risks don't go away:

- **Even if you have mitigated, transferred or accepted**
- **Risks are always present, just less likely or somewhere else**
- **Review them regularly, at least annually**
- **What has changed? Likelihood, ease or exploitation**
- **Even company's risk appetite can change**

citb BeResilient is a programme fully funded by CITB

Principles.

The International Organization for Standardization (ISO) identifies the following principles of risk management:

Risk management should:

- create value – resources expended to mitigate risk should be less than the consequence of inaction
- be an integral part of organizational processes
- be part of decision making process
- explicitly address uncertainty and assumptions
- be a systematic and structured process
- be based on the best available information
- be tailorable
- take human factors into account
- be transparent and inclusive
- be dynamic, iterative and responsive to change
- be capable of continual improvement and enhancement

Process.

According to the standard ISO 31000 "Risk management – Principles and guidelines on implementation," the process of risk management consists of several steps as follows:

Establishing the context

This involves:

1. the social scope of risk management; the identity and objectives of stakeholders; the basis upon which risks will be evaluated, constraints.
2. defining a framework for the activity and an agenda for identification.
3. developing an analysis of risks involved in the process.
4. mitigation or solution of risks using available technological, human and organizational resources.

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 or benefits. Hence, risk identification can start with the source of our problems and those of our competitors (benefit), or with the problem itself.

Assessment

Once risks have been identified, they must then be assessed as to their potential severity of impact (generally a negative impact, such as damage or 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 an unlikely event, the probability of occurrence of which is unknown. Therefore, in the assessment process it is critical to make the best educated decisions in order to properly prioritize the implementation of the **risk management plan**.

Risk matrix.

A risk matrix is a matrix that is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity. This is a simple mechanism to increase visibility of risks and assist management decision making.

Risk is the lack of certainty about the outcome of making a particular choice. Statistically, the level of downside risk can be calculated as the product of the probability that harm occurs (e.g., that an accident happens) multiplied by the severity of that harm (i.e., the average amount of harm or more conservatively the maximum credible amount of harm). In practice, the risk matrix is a useful approach where either the probability or the harm severity cannot be estimated with accuracy and precision.

Although standard risk matrices exist in certain contexts, individual projects and organisations may need to create their own or tailor an existing risk matrix.

The resulting risk matrix could be:

Consequence

Likelihood	Negligible	Marginal	Critical	Catastrophic
Certain	High	High	Extreme	Extreme
Likely	Moderate	High	High	Extreme
Possible	Low	Moderate	High	Extreme
Unlikely	Low	Low	Moderate	Extreme
Rare	Low	Low	Moderate	High