

Risk Management Principles Simple & Precise Explanation

Risk management as understood by its name is process of managing the risks, that involves first identify, assess and prioritize the risks and then implement the coordinated measures and/or resources to eliminate, minimize and monitor the probability and impact of the unwanted events or situations.

Risk management is the identification, evaluation, and prioritization 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 events or to maximize the realization of opportunities.

The risk that we need to manage can be of any type i.e. credit risk, uncertainty in financial markets, project failure at any stage of the project, natural disaster, IT infrastructure failure, bankruptcy of creditors, hacking of servers and an accident or attack from enemies etc.

Organizations adopt various approaches for managing the risks some may prefer to transfer the risk to other parties i.e. through insurance of plants and machinery and even complete projects (although there is still risk of bankruptcy of insurer).

Some may decide to avoid it by altering the processes and or by denying the orders from a fragile client.

Also some organizations manage the creditors' risks by increasing their profit margins etc. Risk sharing is another approach in which you share the benefit of gain or burden of loss from a risk and from measures taken to mitigate the risk.

There are some strategies to manage threats (uncertainties with negative consequences) which typically include avoiding the threat, reducing the negative effect or probability of the threat, transferring all or part of the threat to another party, and even retaining some or all of the potential or actual consequences of a particular threat, and the opposites for opportunities (uncertain future states with benefits).

There are several risk management standards available globally and that consider varying aspects of the risk management depending upon the target business areas i.e. engineering, project management and IT etc.

Certain risk management standards have been criticized for having no measurable improvement on risk, whereas the confidence in estimates and decisions seems to increase. For example, one study found that one

in six IT projects were “black swans” with gigantic overruns (cost overruns averaged 200%, and schedule overruns 70%).

There are risk management standards by PMI, NIST and ISO.

Risk Management 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
- To be dynamic, iterative and responsive to change
- Be capable of continual improvement and enhancement
- Be continually or periodically re-assessed

Risk management methods are adopted mostly in the following sequence:

1. To identify, characterize, and assess the potential threats to company assets or operations
2. To assess the vulnerability of critical assets and processes to specific threats
3. To determine the risk through risk assessment approach
4. Identify the practical ways to reduce the risks
5. Prioritize risk reduction measures based on a business strategy