1.1 Definition of risk and risk management

Risk management is an organizational model aimed at developing the quality of management processes; it stands out by analysing the events that have never materialized within the organization.

Unlike most managerial systems, risk management doesn’t overlap with other internal controls because it represents a different perspective that cuts across planning and control, performance evaluation system, audit, quality and so on.

Therefore, risk management helps the organizations bring about a higher level of quality of services and products because it supports the decision-making processes, preparing for the difficulties that could hinder the achievement of the strategic goals.

In a few words, the main objective of risk management concerns protecting and strengthening:

- Values, ethics and sense of belonging
- The entity’s tangible and intangible assets
- Growth of organizational culture
- Leadership and relationship
- Effectiveness and efficiency of processes
- Resources for strategic priorities
- Stakeholder’s satisfaction

That means that risk management could be considered to be a tool to effectively manage an organization; in fact, it deals with risks and opportunities affecting the creation or the preservation of an entity’s value. Risk management is defined by the CoSO Model[1] as: “a process, effected by an entity’s board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives”.

The definition reflects certain fundamental concepts; in particular, risk management is:

- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in strategy setting
- Applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity’s management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories

This definition is purposefully broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries, and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness.

Risk management examines the events that have negative impact; they represent the risks which can prevent value creation or erode existing value.

There are many risk definitions in the literature and in the standards most recognized at the international level; the standard ISO 31000:2009 defines risk as: “the effect of uncertainty on objectives”, where “an effect is a deviation from what is expected (positive and/or negative), often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence” and the uncertainty is “the lack of information about the understanding or knowledge of an event, its consequences and likelihood”.

In fact, the concept of risk is more complex than the combination of likelihood and effect; it comprises some issues considered by the cognitive analysis relating to the organization, including:

- Risk Profile: set of risks that may affect all or part of an organization;
- Risk Appetite: total amount and type of risks that an organization decides to pursue, maintain or adopt
- Risk Attitude. (Existing Risk Profile). If an organization is particularly effective in managing certain types of risks, it may be willing to take on more risk in that category, conversely, it may not have any appetite in that area.
- Risk Acceptance, which refers to the maximum potential impact of a risk event that an organization could withstand. Often, appetite will be well below acceptance.
- Risk Capacity, which is the maximum level of risk that an organization can assume without violating the regulatory burden;
- Risk Retention, which considers stakeholders’ conservative return expectations and a very low appetite for risk-taking.
- Risk Tolerance, which is the level of variation that the entity is willing to accept around specific objectives.

All of these issues should be considered to assess the overall risk level of the organization.

Therefore, the identification of the “enabling factors” and the “causes” related to a risk, could contribute significantly to specifying the context in which the risk can occur, allowing risk owners, to adopt the necessary preventive measures.

While the enabling factor represents an organizational/social/environmental circumstance which facilitates a behaviour that could result in a risk, the cause is the reason why the action has been undertaken. Therefore, the root-cause analysis can help organizations distinguish risks that could be effectively tackled from those which can only be partially dealt with.

Regarding the definition of a risk, some issues should be taken into consideration[2]:

- A risk statement should be a clear, meaningful and concise statement that describes the risk. Example: Increased difficulties in reaching household survey respondents could adversely impact the quality of our data.
The statement should describe the event, and the potential impact of that event on the achievement of the organization’s objectives. Example: There is a risk that (event)....and the consequences are (impact)...

A good risk statement should also include the possible causes (drivers). Examples: There is a risk that (event)...because of (cause)...and the consequences would be (impact)....; Given that...there is a risk that...with the potential impact of....

Before any risk treatment is put in place, the event involves an "inherent risk", ontologically related to the activity that could determine the event itself; once the mitigating action has been put in action, all that’s left is the "residual risk", whose value can be equal to, greater or less than the "inherent risk".