3.1 Risk identification

Risk generally is the uncertainty inherently related to consequences – either positive i.e. opportunity, or negative i.e. threat – of actions and events. It is measured through a combination of likelihood and impact, including perceived relevance. “Inherent risk” is the exposure arising from a specific risk before any action has been taken to manage it, while “residual risk” is the exposure arising from a specific risk after any action has been taken to manage it, and in case such an action has proved effective.

An organization defines the criteria to be used to evaluate risk significance. Such criteria should reflect both the stakeholders’ risk perception (based on a set of values/concerns), and the organization’s values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements. Risk criteria should be consistent with the organization’s risk management policy, defined in the risk management framework.

Defining risk criteria involves deciding on:
1. The nature and kind of consequences to be included, and how they will be measured;
2. The way probabilities are to be expressed;
3. How a level of risk is going to be determined;
4. The criteria for determining when a risk needs treatment;
5. The criteria for deciding when a risk is acceptable and/or tolerable;
6. Whether and how combinations of risks will be taken into account.

Risk identification requires analysing several issues:
- **Source/root cause event**: any activity having a potential to increase a specific risk, whether or not such an activity is under the control of the organization;
- **Areas of impact**: dealing with categorization/prioritization of consequences;
- **Enablers**: the organizational features helping a risk-event to occur;
- **Events**: occurrence of a particular set of circumstances; and
- **Their potential consequences**: potential outcome of an event. A wide range of risk consequences should be considered, including cascade and cumulative effects.

The above issues can create, enhance, prevent, degrade, accelerate or delay the ability of either the whole organization, or part of it, to achieve its own objectives.

I. Risk hierarchy and risk categorization

The risk management framework includes a hierarchy of risks, comprising a variety of risk levels together with priorities in risk treatment strategies.

- **Enterprise or so-called “corporate” risks** are strategic (i.e. can significantly impact on the organization). To manage them is fundamental to the long term viability of the organization and this must be done under the supervision of the risk committee;

- **Portfolio management risks** are inherently related to the portfolio of projects as a whole, and are managed by senior management. Some examples of portfolio risk are: affordability of the portfolio; lack of capability/capacity to implement the portfolio; lack of timely availability of skills and human resources;
- **Project risks** can impact on the projects’ objectives and outcomes, and are managed by the project risk manager; where appropriate, they will be addressed as part of the project management framework. Some examples of project risk are: project scope poorly defined, resources not available when required, quality requirements not clearly specified.

- **Operational risks** can impact on a program’s objectives and/or outcomes (i.e. unsuitable skills mix, resources reduced due to budget cuts, outputs not delivered on time, poor quality outputs) and are managed by the program directors.

While each risk captured may be important for management at the function and business unit levels, the corporate risk list requires prioritization to focus the attention of the board and senior management on key risks.

The management of risk at corporate, enterprise and operational levels needs to be integrated, so that the levels of activity support each other. In this way the organization’s risk management strategy will be led from the top, and be embedded in the normal working routines and activities.

Risk specialists on specific risks, directly referring to the related senior managers, are needed. Specific risk areas include, for example:

- Health and safety risks;
- Fraud risks (i.e., manipulation of any procedures for dishonest purposes; failure to comply with procedures and/or internal regulations; alteration of checks on execution of works or on delivery of supplies; etc.);
- ICT risks (i.e., security systems risks; business continuity; etc.)

An organization should therefore set and document its risk categories and risk consequence categories according to its size, purpose, nature, complexity and context. The risk categories, including those from stakeholders, should be communicated throughout the organization in order to share a common understanding.

Grouping similar kinds of risks into risk categories helps to:

1. Allow consistent assessment;
2. Profile and report the consequences of actual and potential events;
3. Facilitate comparison across the organization;
4. Aggregate and map similar kinds of risk across the organization;
5. Allocate risk management responsibilities;
6. Build internal skills, knowledge and expertise throughout the organization.

The table below shows risk categories and classes for a NSO, according to the allocation suggested by Co.S.O. enterprise risk management standard.

<table>
<thead>
<tr>
<th>Strategic</th>
<th>Statistical production, Statistical data dissemination, Management systems and processes, Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational</td>
<td>HR, Finance, ICT, Procurement</td>
</tr>
<tr>
<td>Compliance</td>
<td>Compliance to law, standards</td>
</tr>
</tbody>
</table>
**II. Risk identification techniques**

Risk identification may require a multidisciplinary approach, since risks may cover a wide range of causes and consequences.

Risk identification methods can include:

a) Evidence based methods, for example checklists and historical data reviews;

b) Systematic team approaches (a team of experts systematically identifies risks by means of a structured set of prompts or questions (i.e. structured or semi-structured interviews, Brainstorming[1], Delphi method[2]));

c) Inductive reasoning techniques (i.e. preliminary hazard analysis, HAZOP, HACCP);

d) Scenario analysis (i.e. root-cause analysis, scenario analysis as such, cause-consequence analysis);

e) Statistical methods (i.e. Monte-Carlo analysis, Bayesian analysis).

In implementing these techniques the maturity of a risk management system should always be taken into account. During the experimental phase of the risk management model, the experience analysis should always be combined with either structured or semi-structured interview, or a prompt /check list, in order to guide risk owners through the risk analysis.

The experience analysis needs to be based on actual information, through the examination of data from various systems (e.g. electronic document management systems, non-conformities and IT incidents registration system, time use recording system, as well as a specific system to record quality features of statistical surveys). Once the risk management culture is more established throughout the organization, brainstorming and the Delphi technique can replace the interview, the cause/consequence analysis, the check-list or any other simpler kind of scenario analysis.

Factors influencing selection of techniques are:

1. Problem complexity and the methods needed to analyse them;

2. The nature and degree of risk assessment uncertainty, that is based on the amount of information available and requirements to satisfy objectives;

3. The extent of resources needed in terms of time and level of expertise, data needs or cost;

4. Whether the method can provide a quantitative output.

[1] Brainstorming is a means of collecting a broad set of ideas and evaluation, ranking them by a team. It may be stimulated by prompts or by one-on-one and one-on-many interview techniques

[2] A means for combining expert opinions to support the source and influence identification, probability and consequence estimation and risk evaluation. It is a cooperative technique for building consensus among experts (ISO ISO31010 – risk Assessment Techniques)