3.2 Risk analysis and measurement

Risk analysis involves consideration of risk causes and sources, their positive and negative consequences and the likelihood of such consequences occurring.

It normally includes estimation of the range of potential consequences that might arise from an event, situation or circumstance, and their associated probabilities, in order to measure the level of risk. However, in some instances (such as where the consequences are likely to be insignificant, or probability is expected to be extremely low), a single parameter estimate can be enough to make a decision.

In any case, some framework for assessing risks should be developed. The assessment should draw as much as possible on unbiased independent evidence, should consider the perspectives of the whole range of those stakeholders affected by the risk, and avoid confusing a fair risk assessment with any judgment about the acceptability of particular risks.

There are three important principles in assessing risk:

1. Ensuring that there is a clearly structured process, through which both likelihood and impact are considered;
2. Recording risk assessment in such a way to facilitates monitoring and identification of risk priorities;
3. Distinguishing between “inherent” and “residual” risk. The level of risk will depend on the adequacy and effectiveness of existing controls.

Methods used in analysing risks can be:

- **Qualitative**: such methods define consequence, probability and level of risk, according to descriptive scales, may combine consequence and probability, and evaluate the resulting level of risk against qualitative criteria.
- **Semi-quantitative**: such methods use numerical rating scales for consequence and probability, and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic, or have some other relationship; the formulae used can also vary.
- **Quantitative**: this kind of analysis estimates practical values for consequences and their probabilities, and produces numerical values for impact, likelihood and level of risk, using data from a variety of sources. Full quantitative analysis may not always be possible or desirable due to poor information about the object being analysed, lack of data, influence of human factors, etc.

Both qualitative and quantitative techniques have advantages and disadvantages.

Qualitative analysis is relatively quick and easy, provides a lot of information about non-financial impacts and is easily understood by a large number of employees.

On the other hand, it doesn’t make much difference among levels of risk, cannot numerically aggregate or address risk interactions or correlations, and provides limited opportunity to perform cost-benefit analysis.

Quantitative analysis allows many qualitative methods weaknesses to be overcome, although it can be time-consuming and costly especially at first, during model development.

Cause-effect analysis is a semi-qualitative, structured method allowing a potential event to be traced back to its original causes. It organizes possible contributory factors into broad categories, so that all relevant hypotheses can be considered. It does not, however, by itself point to the actual causes, since these can only be determined by real evidence and empirical testing of hypotheses. Cause-and-effect analysis provides a structured pictorial display (diagram) of a list of causes for a specific effect (positive or negative depending on the context). It is used to build consensus on all possible scenarios, and the most likely causes identified by a team of experts; such causes can then be tested empirically or by evaluation of available data.

A cause-and-effect diagram can be made when there is need to:

- Identify the possible root-causes for a specific effect, problem or condition;
- Sort out and correlate some of the interactions among factors affecting a particular process;
- Analyse existing problems so that improvement action can be taken.
The input to a cause-and-effect analysis may come from expertise and experience from participants, or a previously developed model that has been used in the past.

The cause-and-effect analysis should be carried out by a team of experts who are aware of the problem requiring resolution.

The basic steps in performing a cause-and-effect analysis are as follows:

1. Establishing the effect to be analysed, and placing it in a box;
2. Determining the main categories of causes (chosen to fit the particular context), and representing them by boxes in the Fishbone diagram;
3. Filling in the possible causes for each major category with branches and sub-branches to describe the relationship among them;
4. To keep asking “why?” or “what caused that?” to connect the causes;
5. Reviewing all branches to verify consistency and completeness, and to ensure that the causes apply to the main effect;
6. Identifying the most likely causes, based on the opinion of the team and available evidence.

The results are normally displayed as either a Fishbone (or Ishikawa) diagram or tree diagram. The Fishbone diagram is structured by separating causes into major categories (represented by the lines off the fish backbone), with branches and sub-branches that describe more specific causes under the above-mentioned categories.

**Figure 3: Example of Ishikawa or Fishbone diagram**

![Fishbone Diagram Example](image)

**Source**: IEC/FDIS 31010:2009, Risk management – Risk assessment techniques

As mentioned above, the level of risk is a function of factors, in particular likelihood and impact.

**Impact** refers to the extent that a risk event may affect an organization. Impact assessment criteria may include financial, reputational, regulatory, health, safety, security, environmental, customer and operational consequences. Organizations typically define impact using a combination of such consequences, given that certain risks may impact the enterprise financially, while other risks may have a greater impact to reputation or health and safety.

**Likelihood** represents the weak/strong possibility that a given event will actually occur. Likelihood can be expressed through either qualitative, percent or frequency terms. Sometimes organizations describe likelihood in more personal and qualitative terms such as “event expected to occur several times (or not expected to occur) over the course of a career”.

The Appendix shows examples of risk indexes for impact and likelihood.

When using either qualitative or semi-qualitative methods – for example risk indexes – aimed at evaluating risk level whatever the event (statistical, organizational or specific ones), applying the same number of parameters for impact as well as likelihood is crucial. In order to balance subjectivity in evaluation, more than one evaluator for single risk is needed and evaluation should be supported through objective data as much as possible.

As for the roles and accountabilities, risk factors assessment is under the responsibility of the process owners. Risk measurement is a task for working groups supported by the risk management office, and participated in by the staff working on the processes in question, who submit their results for authorization/review at senior levels. Experts (e.g., IT, data protection/statistical confidentiality, etc.) are responsible for the measurement of specific risks. The results of assessment are always also reviewed and validated by the risk manager.
QUESTION MARK BOX

Q. With reference to the risk measurement phase, does your Organization use different techniques concerning risk classification (IT, financial, compliance, etc.)?

R. The risk assessment (in statistical areas) includes consideration of the range of issues in a statistical processing cycle that can affect data quality as well as managing stakeholder relationships.

Source: Australia Bureau of Statistics, In-depth survey on risk management practices

**Inherent risk:** the risk to an entity in the absence of any actions management might take to alter the risk’s likelihood or impact.

**Residual risk:** the portion of total risk remaining after risk treatment has been applied. Residual risk comprises acceptable risk and unidentified risk.