3.3 Risk weighting

Risk weighting involves comparing estimated levels of risk to assessment criteria, in order to identify the most significant risks, or to exclude minor risks from further analysis. The purpose is to ensure that use of resources will be focused on the most important risks. Care should be taken not to screen out low risks which occur frequently and can therefore have a significant increasing effect.

The preliminary analysis determines one or more of the following courses of action:

- Setting aside insignificant risks (so called acceptable risks) which would not justify treatment;
- Deciding to treat unacceptable risks;
- Setting priorities for risk response.

Risk weighting provides inputs to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Subsequently, the purpose of risk weighting is to assist in making decisions (based on the outcomes of risk analysis) about which risks need treatment and which priority must be assigned for their treatment. Risks are related to objectives, so can easily be prioritized for risk response in relation to such objectives. Unacceptable risks are ranked and prioritized in relation to other risks. Therefore, the decision about whether and how to treat the risk may depend on costs and benefits from taking the risk, and costs and benefits from implementing improved controls.

A common approach to prioritizing risks is to divide them into three bands:

- An upper band, where the level of risk is regarded as intolerable whatever benefits the activity may bring, and risk treatment is essential whatever its costs;
- A middle band, where costs and benefits are taken into account and opportunities balanced against potential consequences;
- A lower band, where the level of risk is regarded as negligible, or so small that no risk treatment measures are needed.

Some organizations represent this portfolio as a hierarchy, some as a collection of risks plotted on a heat map (also risk map or risk matrix).

First, the risks are ranked according to one, two, or more criteria, such as impact rating multiplied by likelihood rating.

Second, the ranked risk order is reviewed in light of additional considerations, such as impact alone, or the size of the gap between current and desired risk level (risk tolerance threshold).

If the initial ranking is done by multiplying financial loss by likelihood, then the final prioritization should also take into consideration other qualitative factors (for example loss of reputation).

The most common way to prioritize risks is by assigning a risk level for each area of the graph such as very high, high, medium, or low, where the higher the combined impact and likelihood ratings, the higher the overall risk level. The boundaries among levels vary from entity to entity, depending on risk appetite. For example, an organization with a greater risk appetite will have boundaries among risk levels shifted toward the upper right, and an organization with greater risk aversion will have boundaries among risk levels shifted toward the bottom left. Also, some organizations adopt asymmetric boundaries placing a somewhat greater emphasis on impact than on likelihood. For example, a risk having a “moderate” impact rating and a “frequent” likelihood rating has a “high” risk level assigned, whereas a risk having an “extreme” impact rating and a “possible” likelihood rating has a “very high” risk level assigned.