national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

Public Sector Risk Management Framework

Risk Assessment

1. Introduction

Risk assessment is a systematic process to quantify or qualify the level of risk associated with a specific threat or event, to enrich the risk intelligence available to the Institution. The main purpose of risk assessment is to help the Institution to prioritise the most important risks as the Institution is not expected to have the capacity to deal with all risks in an equal manner.

2. The risk assessment process

Risks should be assessed on the basis of the likelihood of the risk occurring and the impact of its occurrence on the particular Institutional objective(s) it is likely to affect. Risks should be expressed in the same unit of measure used for the key performance indicator(s) concerned.

Risk assessment should be performed through a three stage process:

- Firstly, the inherent risk should be assessed to establish the level of exposure in the absence of deliberate management actions to influence the risk;
- Secondly, a residual risk assessment should be performed to determine the actual remaining level of risk after the mitigating effects of management actions to influence the risk; and
- Thirdly, the residual risk should be benchmarked against the Institution's risk appetite to determine the need for further management intervention, if any.

Risk assessment should be strengthened by supplementing Management's perceptions of risks, inter alia, with:

- review of the reports of the Standing Committee on Public Accounts and the relevant Parliamentary Committee(s);
- financial analyses;
- historic data analyses;
- actual loss data;
- interrogation of trends in key performance indicators;

- benchmarking against peer group or quasi peer group;
- market and sector information;
- scenario analyses; and
- forecasting and stress testing.

Risk assessments should be re-performed for the key risks in response to significant environmental and/or organisational changes, but at least once a year, to ascertain the shift in the magnitude of risk and the need for further management action as a result thereof.

3. The approach

Risk assessment is a fundamental component of the risk management process. It helps to guide the evaluation of risks by defining the key parameters of the risk and how these may impact on the achievement of Institution's objectives.

One of the key outcomes of the risk assessment process is determining levels of risk exposure for the Institution. In addition, the data and related information collected during the risk assessment process can be used to assist in guiding risk response decisions.

Risk assessment involves interrogating risks at two levels, namely at the inherent risk level and the residual risk level, using the same rating criteria for each assessment.

- Inherent risk considers the "worst case" scenario. This involves considering the likelihood and impact of the risk in the absence of any management control interventions. This level of assessment provides a perspective of the consequences of the risk to the Institution in its unmanaged state.
- The second tier of assessment concerns establishing the residual risk. Residual risk is the level of risk remaining after the mitigating influence of the existing control interventions is considered. Normally, management would introduce sufficient control to reduce the risk to within a pre-determined level, as informed by the optimal risk level.. The residual risk is a critical indicator of whether the existing controls are effective in reducing the risk to an acceptable level.

Risks can be assessed on a quantitative basis or a qualitative basis. Quantitative assessment works best for risks that involve numeric functions. A good example would be the risk of financial losses as this can be numerically quantified.

Quantitative techniques typically bring more precision and are used in more complex and sophisticated activities.

Qualitative assessment is applied when the risk in question does not lend itself to numeric quantification. In such cases more subjective means are utilised, the most important of which is the expert judgement of management.

3.1 Risk assessment involves the following key steps:

- Identify and evaluate existing control effectiveness;
- Determine risk likelihood (probability or frequency of risk occurrence);
- Determine risk consequence (outcome or impact of an event);
- Determine the overall risk rating level; and
- Document risk assessment process

Both the risk likelihood and consequence rating should be performed prior and post controls to determine level of risk rating (inherent vs. residual rating); and

3.1.1 Identify and evaluate existing control effectiveness

Controls may reduce the likelihood of occurrence of a potential risk, the impact of such a risk, or both. Management then needs to assess the control effectiveness based on their understanding of the control environment currently in place. Residual risk will therefore inform management of the actual level of control effectiveness.

Controls should be considered on the basis of:

- design effectiveness - is the control "fit for purpose" in theory i.e. is the control designed appropriately for the function for which it is intended; and
- operational effectiveness - does the control work as practically intended. It is useful to involve staff with an understanding of the controls when rating them. Internal audit, business analysts and operational/ financial management can all provide input into control identification and assessment.

A well-designed and implemented control can often mitigate or reduce more than one risk or type of risk.

3.1.2 Determine risk likelihood and consequence

Risks are assessed on the basis of the likelihood of the risk occurring and the impact of its occurrence (Risk = Likelihood x Impact).

The magnitude of the consequences of an event, should it occur, and the likelihood of the event and its associated consequences, should be assessed in the context of the effectiveness of the existing strategies and controls.

Consequences and likelihood may be estimated using statistical assessment and calculations. Where no reliable or relevant past data is available, subjective estimates may be made which reflect an individual's or Institution's degree of belief that a particular event or outcome will occur.

The most relevant sources of information and techniques should be used when analysing consequences and likelihood.

Sources of information:

- Past records;
- Practice and relevant experience;
- Relevant published literature;
- Market research;
- The results of public consultation;
- Experiments and prototypes;
- Economic, engineering or other models; and
- Specialist and expert judgments.

Techniques:

- Structured interviews with experts in the area of interest;

- Use of multi-disciplinary groups of experts;
- Individual evaluations using questionnaires; and
- Use of models and simulations.

Risk assessment should be performed in accordance with approved rating criteria for both likelihood and impact.

Click here to view a typical rating table for assessing risks.

3.1.3 Determine the overall risk rating

Once you have rated the likelihood and consequence, combine the two to determine the overall risk rating.

Based on the risk assessment, risks are classified by level to determine the appropriate level of response to those risks. Specific responses are defined at the "Risk Response" phase (See guideline on risk response strategy)

3.1.4 Document risk assessment process

Documentation of the risk assessment process provides a record of how risks were analyzed in previous periods, thereby informing future risk assessment exercises. A key outcome of documenting the risk assessment process is enabling accurate tracking of risks over time using historical reference data.

Documentation should include:

- key assumptions and limitations;
- sources of information used;
- explanation of the assessment method, and the definitions of the terms used to specify the likelihood and consequences of each risk;
- existing controls and their effectiveness;
- description and severity of consequences;
- the likelihood of these specific occurrences; and
- resulting level of risk.

Detailed documentation may not be required for very low risks; however a record should be kept of the rationale for initial screening of very low risks.

4. Risk assessment considerations

There are a number of other issues that must be considered in the context of risk assessment, which are noted below:

- The risk assessment tables need to be consistently applied for all key risks in the Institution.
- Certain disciplines, for example, IT and Health and Safety, may utilise assessment methodologies that are informed by their professional norms and standards. In such circumstances, it would be prudent for the sake of the operational efficiency of these disciplines to allow them to use their preferred methodology. However, in order to maintain

consistency at the Institutional level the same risks should be re-assessed in terms of the Institution-wide risk assessment methods.

- The results of risk assessment could be represented in 'heat maps'. These are a simple graphical representation of each risk according to the two scales.
- Assessment of likelihood more often than not imposes a challenge to management. Guidance in this respect can be obtained from the historical experience of the Institution, as well as the experience of similar Institutions.
- The assessments must be considered together with the Institution's risk appetite to determine whether the risk is acceptable or not. This in turn will inform whether additional interventions will be required.

5. Outputs

The output of risk assessment is a more sophisticated risk register which is enriched by the addition of ratings for each risk. This allows management to separate the more important risks from the less important ones and direct management attention accordingly.