Risk Identification

1. Introduction

Risk identification is a deliberate and systematic effort to identify and document the Institution's key risks. The objective of risk identification is to understand what is at risk within the context of the Institution's explicit and implicit objectives and to generate a comprehensive inventory of risks based on the threats and events that might prevent, degrade, delay or enhance the achievement of the objectives. This necessitated the development of risk identification guidelines to ensure that Institutions manage risk effectively and efficiently.

2. The risk identification process

Comprehensive identification and recording of risks is critical, because a risk that is not identified at this stage may be excluded from further analysis. In order to manage risks effectively, Institutions have to know what risks they are faced with. The risk identification process should cover all risks, regardless of whether or not such risks are within the direct control of the Institution. Institutions should adopt a rigorous and on-going process of risk identification that also includes mechanisms to identify new and emerging risks timeously.

Risk identification should be inclusive, not overly rely on the inputs of a few senior officials and should also draw as much as possible on unbiased independent sources, including the perspectives of important stakeholders.

2.1 Risk workshops and interviews

Risk workshops and interviews are useful for identifying, filtering and screening risks but it is important that these judgment based techniques be supplemented by more robust and sophisticated methods where possible, including quantitative techniques.

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

- review of external and internal audit reports;
- 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.

2.2 Focus points of risk identification

To ensure comprehensiveness of risk identification the Institution should identify risk factors through considering both internal and external factors, through appropriate processes of:

2.2.1 Strategic risk identification

Strategic risk identification to identify risks emanating from the strategic choices made by the Institution, specifically with regard to whether such choices weaken or strengthen the Institution's ability to execute its Constitutional mandate:

- strategic risk identification should precede the finalization of strategic choices to ensure that potential risk issues are factored into the decision making process for selecting the strategic options;

- risks inherent to the selected strategic choices should be documented, assessed and managed through the normal functioning of the system of risk management; and

- strategic risks should be formally reviewed concurrently with changes in strategy, or at least once a year to consider new and emerging risks.

2.2.2 Operational risk identification

Operational risk identification to identify risks concerned with the Institution’s operations:

- operational risk identification should seek to establish vulnerabilities introduced by employees, internal processes and systems, contractors, regulatory authorities and external events;

- operational risk identification should be an embedded continuous process to identify new and emerging risks and consider shifts in known risks through mechanisms such as management and committee meetings, environmental scanning, process reviews and the like; and

- operational risk identification should be repeated when changes occur, or at least once a year, to identify new and emerging risks.

2.2.3 Project risk identification

Project risk identification to identify risks inherent to particular projects:

- project risks should be identified for all major projects, covering the whole lifecycle; and

- for long term projects, the project risk register should be reviewed at least once a year to identify new and emerging risks.

3. How to perform risk identification

It is crucial to have knowledge of the business before commencing with risk identification process. It is also important to learn from both past experience and experience of others when considering the risks to which an Institution may be exposed and the best strategy available for responding to those risks.

Risk identification starts with understanding the Institutional objectives, both implicit and explicit. The risk identification process must identify unwanted events, undesirable outcomes, emerging threats, as well as existing and emerging opportunities. By virtue of an Institution's existence, risks will always prevail, whether the Institution has controls or not.

When identifying risks, it is also important to bear in mind that "risk" also has an opportunity component. This means that there should also be a deliberate attention to identifying potential opportunities that could be exploited to improve Institutional performance. In identifying risks, consideration should be given to risks associated with not pursuing an opportunity, e.g. failure to implement an IT system to collect municipal rates.

Risk identification exercise should not get bogged down in conceptual or theoretical detail. It should also not limit itself to a fixed list of risk categories, although such a list may be helpful.

The following are key steps necessary to effectively identify risks from across the Institution:

- Understand what to consider when identifying risks;
- Gather information from different sources to identify risks;
- Apply risk identification tools and techniques;
- Document the risks;
- Document the risk identification process; and
- Assess the effectiveness of the risk identification process.

3.1 Understand what to consider when identifying risks

In order to develop a comprehensive list of risks, a systematic process should be used that starts with defining objectives and key success factors for their achievement. This can help provide confidence that the process of risk identification is complete and major issues have not been missed.

3.2 Gather information from different sources to identify risks

Good quality information is important in identifying risks. The starting point for risk identification may be historical information about this or similar Institutions and then discussions with a wide range of stakeholders about historical, current and evolving issues, data analysis, review of performance indicators, economic information, loss data, scenario planning and the like can produce important risk information.

Furthermore, processes used during strategic planning like Strength Weakness Opportunity and

Threat SWOT Analysis, Political Economic Social Technological Environment & Legal. PEST (EL) Analysis and benchmarking will have revealed important risks and opportunities that should not be ignored, i.e. they should be included in the risk register.

Certain disciplines like IT, Strategic Management, Health and Safety etc. already have in place established risk identification methodologies as informed by their professional norms and standards. The risk identification process should recognize and utilize the outputs of these techniques in order not to "re-invent the wheel".

3.3 Apply risk identification tools and techniques

An Institution should apply a set of risk identification tools and techniques that are suited to its objectives and capabilities, and to the risk the Institution faces. Relevant and up-to-date information is important in identifying risks. This should include suitable background information where possible. People with appropriate knowledge should be involved in identifying risks.

Approaches used to identify risks could include the use of checklists, judgments based on experience and records, flow charts, brainstorming, systems analysis, scenario analysis, and system engineering techniques.

- The approach used will depend on the nature of the activities under review, types of risks, the Institutional context, and the purpose of the risk management exercise.

- Team-based brainstorming for example, where facilitated workshops is a preferred approach as it encourages commitment, considers different perspectives and incorporates differing experiences.

- Structured techniques such as flow charting, system design review, systems analysis, Hazard and Operability (HAZOP) studies and operational modeling should be used where the potential consequences are catastrophic and the use of such intensive techniques are cost effective.

- Since risk workshops are useful only for filtering and screening of possible risks, it is important that the workshops are supplemented by more sophisticated or structured techniques described above.

- For less clearly defined situations, such as the identification of strategic risks, processes with a more general structure, such as 'what-if' and scenario analysis could be used.

- Where resources available for risk identification and analysis are constrained, the structure and approach may have to be adapted to achieve efficient outcomes within budget limitations. For example, where less time is available, a smaller number of key elements may be considered at a higher level, or a checklist may be used.

3.4 Document the risks identified

The risks identified during the risk identification are typically documented in a risk register that, includes (at this stage):

- risk description;

- how and why the risk can happen (i.e. causes and consequences); and
- the existing internal controls that may reduce the likelihood or consequences of the risks.
- It is essential when identifying a risk to consider the following three elements:
- description/event - an occurrence or a particular set of circumstances;
- causes - the factors that may contribute to a risk occurring or increase;
- the likelihood of a risk occurring; and
- consequences - the outcome(s) or impact(s) of an event.

It is the combination of these elements that make up a risk and this level of detail will enable an Institution to better understand its risks.

3.5 Document your risk identification process

In addition to documenting identified risks, it is also necessary to document the risk identification process to help guide future risk identification exercises and to ensure good practices are maintained by drawing on lessons learned through previous exercises. Documentation of this step should include:

- the approach or method used for identifying risks;
- the scope covered by the identification; and
- the participants in the risk identification and the information sources consulted.

Experience has shown that management often disregards well controlled risks when documenting the risk profile of the Institution. It is stressed that a well-controlled risk must still be recorded in the risk profile of the Institution. The reason for this logic is that the processes for identifying risks should ignore at that point any mitigating factors (these will be considered when the risk is being assessed).

4. The outputs of risk identification

The document in which the risks are recorded is known as the "risk register" and it is the main output of a risk identification exercise.

A risk register is a comprehensive record of all risks across the Institution or project depending on the purpose/context of the register. There is no single blueprint for the format of a risk register and Institutions have a great degree of flexibility regarding how they lay out their documents.

The risk register serves three main purposes

- It is a source of information to report the key risks throughout the Institution, as well as to key stakeholders.

- Management uses the risk register to focus their priorities risks.
- It is to help the auditors to focus their plans on the Institution's top risks.

As a minimum, the risks register records:

- the risk;
- risk category;
- how and why the risk can happen "cause of risk";
- how will the risk impact the Institution if it materializes "impact on Institution";
- the qualitative and / or quantitative cost should the risk materialize;
- the likelihood and consequences of the risk to the Institution;
- the existing internal controls that may minimize the likelihood of the risk occurring;
- a risk level rating based on pre-established criteria;
- framework, including an assessment of whether the risk is acceptable or whether it needs to be treated;
- a clear prioritization of risks (risk profile);
- accountability for risk treatment (may be part of the risk treatment plan); and
- timeframe for risk treatment.

Once the risks have been identified and existing control have been assessed and it is has been established that controls are inadequate, an assessment of whether the risk is acceptable or whether it needs to be treated needs to be performed.