Office of the Accountant General

Frequently Asked Questions (FAQ's)

Risk Management

1. What are the guidelines/methods for performing effective risk assessment processes?

1.1. The key steps in ensuring that risk assessments are effective and efficient should take into account at least the following:

1.1.1. Project planning (including prioritization, milestones, deliverables, etc)

1.1.2. Communication of the needs and the benefits both to internal and external stakeholders

1.1.3. Introducing RM to all senior management and obtain commitment

1.1.4. Starting the process where it adds value in solving critical problems(e.g. budget process plans)

1.1.5. Keeping it simple

1.1.6. Maintaining focus and have clear direction

1.2. National Treasury Risk Management Framework also includes steps for risk assessment which are:

Step 1: Quantifying the parameters (scoring system) of impact and likelihood before the actual assessment;

Step 2: Applying the parameters to the risk matrix to indicate what areas of the risk matrix would be regarded as high, medium or low risk;

Step 3: Determining the risk acceptance criteria by identifying what risks will not be tolerated;

Step 4: Determine risk acceptability and what action will be proposed to reduce the risk.

N.B. The RMF can be downloaded from (http://oag.treasury.gov.za/).

2. Does the Risk Officer (RO) sit in the audit committee meetings or what is the RO's involvement in the audit committee?

2.1. The RO is usually not a member of the Audit Committee; however, the terms of reference of the Audit Committee will assist in determining whether the RO should be present at its meetings.

2.2. Good practice suggests that the AC should receive briefing on risk management from appropriate personnel. The practice of having RO present at the meetings is therefore encouraged.

2.3. Where there is a functional Risk Management Committee, the chairperson of this committee should be present at meetings of the AC to report on the state of risk management. Where either one or both of the AC charter or RM charter does not give formal effect to this arrangement it is recommended that the charter be amended to formalize this.

3. What are the responsibilities of the Internal Audit unit as opposed to the Risk Management unit?

3.1. For the roles of the RO, please refer to question 6.

3.2. The Internal Audit(IA) unit is established in compliance with the PFMA and the MFMA to provide independent assurance and consultancy to the accounting officer and report to the audit committee on the institution's internal control, governance and risk management

3.3. The IA function is required to evaluate the efficiency, effectiveness and the economy of the risk management process and systems

3.4. Where the IA is satisfied with the integrity of the RM process, it is required to develop long and short term audit plans that take cognizance of the most important risks that they need to provide assurance or consultancy on.

3.5. Internal Auditors provide an independent and objective review of the adequacy and effectiveness of controls introduced to mitigate risks (including the adequacy & effectiveness of the systems of risk management).

3.6. Where there is no RO, the IA can perform the duties of the RO but then cannot audit the systems of RM (May have to outsource the audit of the RM systems and processes).

4. Under which Directorate should the Risk Management functions be placed?

It is not prescribed under which Directorate the functions of RM should be placed, however it is recommended that the functions rest within a unit where the head of the unit reports directly to the Accounting officer in order for the issues of RM to receive serious attention. (See Q 8).

5. What is the difference between a Risk Manager and a Risk Officer?

5.1. The term “risk manager” is often used interchangeably (and incorrectly) with “risk officer” when referring to the individual tasked with facilitating the risk management activity of an institution.

5.2. A distinction needs to be made between a “risk manager” and a “risk officer” (commonly referred to as the Chief Risk Officer).

5.3. A risk manager is an individual responsible and accountable for

i. identifying risks relating to certain objectives;

ii. assessing the seriousness of the identified risks; and

iii. putting into action measures to mitigate particular risk.

5.4. In other words a risk manager is somebody that actually manages risk in their area of responsibility on a day to day basis. A risk manager can therefore be anyone in an organisation, from a line manager to a junior official.

5.5. The Chief Risk Officer (CRO) is a professional that brings structure and formality to the way risk management is implemented and practiced in an organisation. The CRO is responsible for leading, coordinating and consolidating the entire risk management effort of an institution by providing expert support, guidance and advice. (See Q 6 for the duties of the CRO. You will notice that it does not include any responsibilities for actually managing risks. Actual management of risks, however, is explicitly of line management/risk manager.

6. What are the duties of a Chief Risk Officer?

6.1. The core functions of CRO include the following:

* Provide expect guidance and support to line management on risk management processes

* Coordinating, facilitating and guiding the process of identifying, assessing and monitoring risks at all business levels.

* Collating, analysing, interpreting and reporting on the outcomes of risk assessments.

* Maintaining the enterprise risk register.

* Reporting to various stakeholders on the status and progress of the organisation's risk management programme (e.g. Accounting Officer, EXCO, Audit Committee, Risk Management Committee)

* Developing the overall organizational risk management strategy for approval by the Accounting Officer.

* Developing appropriate tools and techniques for identifying, assessing and responding to risks.

* Develop an ERM maturity model.

* Provide training and promote advocacy of RM.

7. At what level should the CRO be appointed?

7.1. It is recommended that the position of a CRO should be informed by:

* The organisation's appreciation and embrace of risk management

(i.e. how seriously risk management is taken);

* The nature, scope and extent of responsibilities that the position entails; and

* An evaluation of the CRO job description (done through job evaluation processes)

8. Who should the Chief Risk Officer report to?

8.1. The accountability and reporting lines of the public sector CRO are not prescribed.

8.2. In an ideal situation, the CRO would report at a level that has sufficient authority and influence to ensure that risk management enjoys the necessary organisational support and profile. Accordingly, it is preferable that the CRO is accountable and reports to the Accounting Officer, however if this is not possible, it is recommended that the CRO reports to someone of sufficient influence to promote the organizational status of RM.

8.3. Alternatively it would be ideal for the CRO to report at an executive senior level (such as the Chief Operations Officer).

8.4. The reporting and accountability lines of the CRO will vary from institution to institution, given the operational dynamics, organizational structure, etc.

8.5. The CRO should attend the executive senior management meeting if she/he does not report directly to the accounting officer.

9. Is it a norm for each Province to have its own Enterprise Risk Management strategy from internal audit to which all departments need to comply/align?

9.1. In terms of section 18(2)(d) of the PMFA, Provincial Treasuries have the principal responsibility for monitoring and assessing the implementation of national and provincial norms and standards (and by implication, systems of risk management) in provincial departments and provincial public entities.

9.2. Provincial treasuries may develop risk management framework/guidelines aligned to the national framework to assist the departments and entities in implementing RM, which takes into account the unique dynamics of the province.

10. Control self assessment vs. risk based auditing?

10.1. Control self assessment

(a) Control self assessment (CSA) is a methodology that can be used by managers to assess the adequacy of their risk management and control processes.

(b) As such it is not independent and the results thereof might lack objectivity. The process allows management and/or work teams directly responsible for a business function to:

i. Participate in the assessment of internal control

ii. Evaluate risk

iii. Develop action plan to address identified weaknesses

iv. Assess the likelihood of achieving business objectives.

10.2. Risk based auditing

(a) Risk based auditing (RBA) is an approach that focuses internal audit priority and resource on providing assurance/consultancy on the most significant risks to the organization.

(b) RBA is an independent process performed by qualified auditors.