



**national treasury**

Department:  
National Treasury  
REPUBLIC OF SOUTH AFRICA

Public Sector Risk Management Framework

# Guidelines for the Accounting Authority / Officer

## 1. Purpose

The purpose of this guideline is to assist the Accounting Authority / Officer in discharging his/her responsibility for **risk management**.

An Accounting Authority / Officer is defined as:

- National Department: The Director-General
- Constitutional Institutions: The Chief Executive Officer
- Provincial Department: The Head of Department
- National Public Entity: The Board of Directors / Council appointed by the Minister, accountable to Parliament for that Public Entity or in whose portfolio it falls or the Chief Executive Officer in the absence of the controlling body
- Provincial Public Entity: The Board of Directors / Council appointed by the Premier or MEC, accountable to the Provincial Legislature and Executive Council for that Entity or the Chief Executive Officer in the absence of the controlling body
- Municipality: The Municipal Manager
- Municipal Entity: The Chief Executive Officer

## 2. Application

The guideline is designed to:

- Provide the Accounting Authority / Officer with information to enable him/her to fully understand the roles and responsibilities of his/her office in terms of risk management;
- Provide templates to assist the Accounting Authority / Officer to effectively discharge such roles and responsibilities.

### 3. How to navigate the guideline

The guideline has been structured according to the sections noted below. Each of the sections contains underlying information that can be accessed by clicking on the title.

- Legal mandate (Section 4)
- Strategic value of the Accounting Authority / Officer in risk management (Section 5)
- The Accounting Authority's / Officer's relationship with other stakeholders (Section 6)
- The role of Accounting Authority / Officer in the Risk Management Process (Section 7)
- ERM architecture and high level responsibilities of an Accounting Authority / Officer (Section 8)
- Evaluation criteria (Section 9)

### 4. Legal mandate and corporate governance

#### 4.1 Legal mandate

Legislating the implementation of risk management in public sector institutions is part of a macro strategy of Government towards ensuring the achievement of national goals and objectives. The following legislative instruments provide the legal foundation for the Accounting Authority / Officer's responsibility for risk management:

##### National Departments

- Section 38 (1)(a)(i) of the Public Finance Management Act (Act 1 of 1999 as amended by Act 29 of 1999) (PFMA);
- Treasury regulations TR3.2.1.

##### Constitutional Institutions

- Section 38 (1)(a)(i) of the Public Finance Management Act (Act 1 of 1999 as amended by Act 29 of 1999) (PFMA);
- Treasury regulations TR3.2.1.

##### Provincial Departments

- Section 38 (1)(a)(i) of the Public Finance Management Act (Act 1 of 1999 as amended by Act 29 of 1999) (PFMA);
- Treasury regulations TR3.2.1.

##### Public Entity

- Section 51 (1)(a)(i) of the Public Finance Management Act (Act 1 of 1999 as amended by Act 29 of 1999) (PFMA);
- Treasury regulations TR27.2.1.

##### Provincial Entity

- Section 51 (1)(a)(i) of the Public Finance Management Act (Act 1 of 1999 as amended by Act 29 of 1999) (PFMA);
- Treasury regulations TR27.2.1.

## Municipalities

- Section 62 (1)(c)(i) of the Municipal Finance Management Act (Act 56 of 2003) (MFMA).

## Municipal Entity

- Section 95 (c)(i) of the Municipal Finance Management Act (Act 56 of 2003) (MFMA).

### 4.2 Corporate Governance

The institution can draw guidance from the following:

- [King II Report on Corporate Governance](#);
- [Batho Pele principles](#).

### 5. Strategic value of the Accounting Authority / Officer in risk management

The Accounting Authority / Officer is the ultimate Chief Risk Officer of the institution and is accountable for the institution's risk management in terms of legislation.

It is important that the Accounting Authority / Officer set the right tone for risk management in the institution. Although all staff will be aware of the need to prevent loss and to safeguard stakeholders' interests, they may not be quite so clear about the institution's standpoint on risk.

It is therefore common for the Accounting Authority / Officer to develop and publish a risk management policy. This is a statement that declares the institution's commitment to risk management.

This will in turn ensure that the institution operates in a conducive control environment where the overall attitude, awareness, and actions of Heads of departments and management regarding internal controls and their importance to the institution is at par with the stated vision, values and culture of the institution.

### 6. The Accounting Authority's / Officer's relationship with other stakeholders

The Accounting Authority / Officer is responsible for putting systems in place to ensure that risk management is properly implemented. The key step in achieving this objective is to ensure that the risk management reporting lines are properly aligned to the concept of independence and sufficient authority is granted.

In ideal circumstances, the Chief Risk Officer (CRO) should report directly to the Accounting Authority / Officer (AA/AO) given the latter's legal responsibility for risk management. However, where this is not practical because of the AA/AO's large span of control and other operational factors, the AA/AO should delegate on the basis of the following principles:

- The CRO should enjoy sufficient "power of office" such that his/her influence does not become diluted, conscious of the fact that the CRO needs to work with and through top management;
- The person that the CRO reports to is at a sufficiently high level in the institution (preferably not more than 1 level below the AA/AO) and is able and willing to provide the necessary direction, support and guidance to the risk management function;
- Regardless of who the CRO reports to, it is clear throughout the institution that the risk management function is an institutional resource and not an extension of the function under which it is placed for reporting purposes;
- The CRO should have a dotted reporting line to the Risk Management Committee.

The reporting line of the CRO is not prescribed in the public sector risk management framework nor is there a common blue print for how this dilemma can be addressed. This creates flexibility for institutions to determine the appropriate placement of the CRO in the institutional hierarchy.

The Risk Management Committee is responsible for assisting the Accounting Authority / Officer in addressing its oversight requirements of risk management and evaluating and monitoring the institution's performance with regards to risk management.

The role of the Risk Management Committee is to formulate, promote and review the institution's ERM objectives, strategy and policy and monitor the process at strategic, management and operational levels.

The Risk Management Committee reviews the risk management policy and strategy and recommends for approval by the Accounting Officer;

The Risk Management Committee also reviews the risk tolerance and recommends for approval by the Accounting Officer and reports to the Accounting Officer any material changes to the risk profile of the Institution;

The Risk Management Committee develops goals, objectives and key performance indicators for the Committee for approval by the Accounting Officer.

The Audit Committee is responsible for providing the Accounting Authority / Officer with independent counsel, advice and direction in respect of risk management. The stakeholders rely on the Audit Committee for an independent and objective view of the institution's risks and effectiveness of the risk management processes.

The Executive Authority is accountable to the legislature \ parliament in terms of the achievement of the goals and objectives of the institution. The Executive Authority in a Municipality is the Executive Committee of Council.

High level responsibilities of the Executive Authority in risk management include:

- Providing oversight and direction to the Accounting Authority / Officer on the risk management related strategy and policies;
- Having knowledge of the extent to which the Accounting Authority / Officer and management has established effective risk management in their respective institutions;

The Risk Champion is a person with the skills, knowledge and leadership required to champion the risk management cause.

A key part of the Risk Champion's responsibility involves escalating instances where the risk management efforts are stifled, such as when individuals try to block ERM initiatives. Therefore the Risk Champion is ultimately accountable to the Accounting Authority / Officer to ensure application of risk management.

Management is accountable to the Accounting Authority / Officer for designing, implementing and monitoring risk management, and integrating it into the day-to-day activities of the institution. This needs to be done in such a manner as to ensure that risk management becomes a valuable strategic management tool for underpinning the efficacy of service delivery and value for money.

Internal Audit is accountable to the Accounting Authority / Officer for providing independent assurance regarding the risk management activities of an institution. Hence, Internal Audit is responsible for providing independent assurance that management has identified the institution's risks and has responded effectively. Internal audit may also play an advisory and consulting role to Management regarding risk management matters.

Although, best practice indicates that Internal Audit should not be in direct control of the risk management function, Internal Audit may perform advisory and consulting engagements on risk management in accordance with applicable standards (refer to the International Standards for the Professional Practice of Internal Auditing - Performance standard 2110).

Responsibilities of Internal Audit in risk management include:

- Reviewing the risk philosophy of the institution. This includes the risk management policy, risk management strategy, fraud prevention plan, risk management reporting lines, the values that have been developed for the institution;
- Reviewing the appropriateness of the risk tolerance levels set by the institution taking into consideration the risk profile of the institution;
- Providing assurance over the design and functioning of the control environment, information and communication systems and the monitoring systems;
- Providing assurance over the institution's risk identification and assessment processes;
- Utilising the results of the risk assessment to develop long term and current year internal audit plans;
- Providing independent assurance as to whether the risk management strategy, risk management implementation plan and fraud prevention plan have been effectively implemented within the institution;
- Providing independent assurance over the adequacy of the control environment. This includes providing assurance over the effectiveness of the internal controls implemented to mitigate the identified risks.

## **7. The role of Accounting Authority / Officer in the Risk Management Process:**

### **7.1 Role of the Accounting Authority / Officer in risk identification process**

The risk identification is defined as "the process of determining what, where, when, why, and how something could happen". Risk identification is a deliberate and systematic effort to understand and document all of the key risks facing the institution.

The objective of risk identification is to generate a comprehensive list of risks based on those events and circumstances that might enhance, prevent, degrade or delay the achievement of the objectives. This list of risks is then used to guide the analysis, evaluation, treatment and monitoring of key risks.

The Accounting Authority / Officer has a responsibility to participate in the risk identification process in order to add value and ensure that all factors (internal and external to the institution) that could hinder the institution's objectives are taken into account during the process. The risk identification process is normally performed through series of workshops, structured interviews etc. which the Accounting Authority / Officer might not be able to attend due to other work commitments. The Accounting Authority / Officer should therefore participate at strategic risk identification level with heads of divisions and management.

It is crucial for all stakeholders involved 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.

### **7.2 Role of the Accounting Authority / Officer in risk assessment**

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.

The Accounting Authority / Officer should review the risk profile as assessed for its accuracy and approve thereof. The Accounting Authority / Officer should focus his / her attention on whether the residual risks as assessed are below the risk tolerance levels. Where the risks have exceeded the tolerance levels, management should propose mitigation for approval by the Accounting Authority / Officer. There might be instances where the risks exceed tolerance levels, however cannot be avoided (e.g. Matter of national priority), in this case the Accounting Authority / Officer should approve and ensure the risks are being monitored regularly.

The Accounting Authority / Officer can utilise the Risk Management Committee to perform their function with regards to the Risk Assessment.

### **7.3 Role of the Accounting Authority / Officer in developing risk tolerance**

Risk appetite is developed at the institutional level by senior management and proposed to the Accounting Authority / Officer for approval

The Accounting Authority / Officer should regularly review all risks that have exceeded tolerance level.

### **7.4 Role of the Accounting Authority / Officer in developing risk response strategies**

A key outcome of the risk identification and evaluation process is a detailed list of all key risks including those that require treatment as determined by the overall level of the risk against the institution's risk tolerance levels. However, not all risks will require treatment as some may be accepted by the institution and only require occasional monitoring throughout the period.

All key risks identified should be responded to however not all these risks will require treatment. The risks that fall outside of the institution's risk tolerance levels are those which pose a significant potential impact on the ability of the institution to achieve set objectives and therefore require treatment.

All risks that have exceeded the tolerance levels should be responded to and treated to ensure that they are reduced to acceptable levels. Heads of divisions and Management should report all risks that exceeded tolerance levels and how the institution intends to respond to them to the Accounting Authority / Officer.

Risk owners nominated by executive management should assume responsibility for developing effective risk response plans. The risk owner should be a senior staff member or manager with sufficient technical knowledge about the risk and/or risk area for which a response is required.

### **7.5 Role of the Accounting Authority / Officer in developing Assurance plans**

The term 'Assurance' refers to the verification of risk mitigation and internal control. It embraces the tasks of internal audit, management reviews and specialised audits that test and validate the control environment.

An assurance plan is one of the primary means by which the Accounting Authority / Officer receives confirmation that internal controls and risk mitigations are appropriately designed and implemented. A risk-based assurance plan follows the outputs of the risk identification, assessment and control evaluation processes.

It is commonly accepted that assurance should be designed on an integrated basis. This means that there is a coordinated plan to provide a spread of assurance providers for the key controls. The principle of integration lies in the arranging of specialist assurance providers based on a rational allocation of resources.

Assurance providers usually have an existing assurance role such as internal auditors, insurance surveyors, safety auditors, environmental surveyors, quality auditors, stakeholder satisfaction surveys, credit auditors, etc. One of the main challenges with integrated assurance is to select assurance providers for strategic risk mitigations.

Another challenge is to secure agreement between existing assurance functions as to who will perform certain audits and reviews so that duplication is eliminated.

A risk-based assurance plan encourages an allocation of assurance resources based on risk priorities. Risk owners have a key role to play in selecting assurance activities for their respective risks.

## **8. ERM architecture and high level responsibilities of an Accounting Authority / Officer**

To derive optimal benefits, risk management ought to be conducted in a systematic manner, using proven methodologies, tools and techniques. For consistency in the way that risk management is handled in the public sector, all institutions are encouraged to adopt the ERM architecture.

The Accounting Authority / Officer must ensure that the responsibility for risk management vests at all levels of management and that it is not only limited to the Accounting Authority / Officer. The Accounting Authority / Officer must also ensure that a risk assessment is conducted regularly to identify emerging risks.

High level responsibilities of the Accounting Authority / Officer include:

- Setting the tone at the top by supporting ERM and allocating resources towards the implementation thereof;
- Establishing the necessary structures and reporting lines within the institution to support ERM;
- Approving the risk management strategy, risk management policy, risk management implementation plan and fraud risk management policy;
- Approving the institution's risk appetite and risk tolerance;
- Influencing an institutional "risk aware" culture;
- Approving the code of conduct for the institution and holding management and officials accountable for adherence;
- Place the key risks at the forefront of the management agenda and devote personal attention to overseeing their effective management;
- Hold management accountable for designing, implementing, monitoring and integrating risk management principles into their day-to-day activities;
- Holding the structures responsible for risk management activities accountable for adequate performance;
- Ensuring that a conducive control environment exists to ensure that identified risks are proactively managed;
- Leverage the Audit Committee, Internal Audit, Risk Management Committee and other appropriate structures for assurance on the effectiveness of risk management;
- Provide all relevant stakeholders with the necessary assurance that key risks are properly identified, assessed, mitigated and monitored;

- Consider and act on recommendations from the Audit Committee, Internal Audit, Risk Management Committee and other appropriate structures for improving the overall state of risk management;
- Provide appropriate leadership and guidance to senior management and structures responsible for various aspects of risk management.

## **9. Evaluation**

Clear objectives and key performance indicators should be set for the Accounting Authority / Officer in respect of risk management. These indicators should be able to measure the Accounting Authority / Officer's effectiveness in leading the institution's ERM in contributing to the institution's goals and objectives. Possible key performance indicators for the Accounting Authority / Officer could include:

- Maturity level of ERM as measured in terms of an appropriate index such as the Financial Capability Maturity Model;
- The institution's performance against key service delivery indicators, including comparison of year-on- year performance;
- Percentage change in unauthorised expenditure, fruitless and wasteful expenditure and irregular expenditure based on year-on-year comparisons;
- Percentage change in incidents of fraud based on year-on-year comparisons;
- Comparison of year-on-year Auditor-General regularity and performance report findings.

[Guidelines: Additional reading / reference](#)