national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

Public Sector Risk Management Framework

Executive Summary

NOTES TO THE READER

The Public Sector Risk Management Framework (Framework), including the accompanying guideline documents, templates and implementation tools were developed for the Public Service but remain the property of the National Treasury. The Framework, guideline documents, templates and implementation tools may be printed or downloaded but may not be used for commercial purposes.

PREFACE

The Framework has been developed in response to the requirements of the Public Finance Management Act and Municipal Finance Management Act for Institutions to implement and maintain effective, efficient and transparent systems of risk management and control.

A number of supplementary guidelines, templates and implementation tools have been developed to enhance the user's understanding of the Framework and to facilitate its implementation. In addition, a web based e-Learning module has been developed to provide a practical way for users to test their understanding of the Framework.

Seeing that risk management is an evolving profession, the Framework (including the guideline documents, templates, implementation tools and e-Learning module) will be reviewed and updated periodically to keep up with new developments and user needs. Users are encouraged to assist in improving the relevance and overall quality of the Framework by providing comments, critique and recommendations through the comments section of the Framework.

SECTION 1: INTERPRETATION AND BACKGROUND

CHAPTER 1 - DEFINITIONS

1. Definitions

In this Framework, unless the context indicates otherwise -

"Accounting Officer"

means:

a) In a Constitutional Institution: The Chief Executive Officer;

b) In a National Department: The Director-General;

c) In a Provincial Department: The Head of Department;

d) In a Municipality: The Municipal Manager; and

e) In a Municipal Entity: The Chief Executive Officer.

"Accounting Authority" means:

a) In a 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 Board of Directors / Council; and

b) In a Provincial Public Entity: The Board of Directors / Council appointed by the Premier or Member of the Executive Council, accountable to the Provincial Legislature and Executive Council for that public entity, or the Chief Executive Officer in the absence of the Board of Directors / Council.

"Audit Committee" means:

An independent committee constituted to review the control, governance and risk management within the Institution, established in terms of section 77 of the PFMA, or section 166 of the MFMA.

"Chief Audit Executive" means:

A senior official within the organisation responsible for internal audit activities (where internal audit activities are sourced from external service providers, the Chief Audit Executive is the person responsible for overseeing the service contract and the overall quality of the services provided).

"Chief Risk Officer" means:

A senior official who is the head of the risk management unit.

"Executive Authority" means:

a) In a Constitutional Institution: The Chairperson of the Constitutional Institution in relation to a Constitutional Institution with a body of persons, and in relation to a Constitutional Institution with a single office bearer, the incumbent of that office;

b) In a National Department: The Cabinet member who is accountable to Parliament for that department;

c) In a Provincial Department: The Member of the Executive Council of a province who is accountable to the Provincial Legislature for that department;

d) In a National Public Entity: The Cabinet member who is accountable to Parliament for that public entity or in whose portfolio it falls;

e) In a Provincial Public Entity: The Member of the Provincial Executive Council who is accountable to the Provincial Legislature for that public entity or in whose portfolio it falls;

f) In a Municipality: The Municipal Council; and

g) In a Municipal Entity: The Municipal Council of its parent municipality.

"Framework" means:

The Public Sector Risk Management Framework.

"Inherent Risk" means:

The exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such factors.

"Institution(s)" means:

National and provincial departments and public entities reporting to these departments, including their subsidiaries and trading entities; municipalities and municipal entities, and independent institutions established by the Constitution.

"Internal Auditing" means:

An independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

"King III" means:

The King Code of Corporate Governance for South Africa 2009.

"Management" means:

All officials of the Institution except for the Chief Risk Officer and officials reporting to him/her.

"MFMA" means:

Municipal Finance Management Act (Act No. 56 of 2003).

"Other Official" means:

An official other than the Accounting Officer / Authority, Management, Chief Risk Officer and his/her staff.

"PFMA" means:

Public Finance Management Act (Act No. 1 of 1999 as amended by Act No. 29 of 1999).

"Residual Risk" means:

The remaining exposure after the mitigating effects of deliberate management intervention(s) to control such exposure (the remaining risk after Management has put in place measures to control the inherent risk).

"Risk" means:

An unwanted outcome, actual or potential, to the Institution's service delivery and other performance objectives, caused by the presence of risk factor(s). Some risk factor(s) also present upside potential, which Management must be aware of and be prepared to exploit. This definition of "risk" also encompasses such opportunities.

"Risk Appetite" means:

The amount of residual risk that the Institution is willing to accept.

"Risk Champion" means:

A person who by virtue of his/her expertise or authority champions a particular aspect of the risk management process, but who is not the risk owner.

"Risk Factor" means:

Any threat or event which creates, or has the potential to create risk.

"Risk Management" means:

A systematic and formalised process to identify, assess, manage and monitor risks.

"Risk Management Committee" means:

A committee appointed by the Accounting Officer / Authority to review the Institution's system of risk management.

"Risk Management Unit" means:

A business unit responsible for coordinating and supporting the overall Institutional risk management process, but which does not assume the responsibilities of Management for identifying, assessing and managing risk.

"Risk Owner" means:

The person accountable for managing a particular risk.

"Risk Tolerance" means:

The amount of risk the Institution is capable of bearing (as opposed to the amount of risk it is willing to bear)

CHAPTER 2 - PURPOSE, APPLICABILITY AND BACKGROUND

2. Purpose

(1) The Framework has been developed in terms of the prescripts (a) and (b) below, read in conjunction with prescripts (c) and (d):

a) sections 38(1)(a)(i) and 51(1)(a)(i) of the PFMA, which require the Accounting Officers/Authorities to ensure that their Institutions have and maintain effective, efficient and transparent systems of risk management;

b) sections 62(1)(c)(i) and 95(c)(i) of the MFMA, which require the Accounting Officers to ensure that their municipalities and municipal entities have and maintain effective, efficient and transparent systems of risk management;

c) section 6(2)(a) of the PFMA, which empowers the National Treasury to prescribe uniform norms and standards in terms of this Act; and

d) section 20(1)(iv), (v) and (vi) of the MFMA, which empowers the Minister of Finance to prescribe uniform norms and standards in terms of this Act.

(2) The Framework also incorporates the requirements of the Batho-Pele principles and King III insofar as they concern risk management.

(3) The Framework aims to support Institutions to improve and sustain their performance by enhancing their systems of risk management to protect against adverse outcomes and optimise opportunities.

3. Applicability

(1) The Framework recognises that Institutions are not homogenous hence it is not possible to produce a blueprint that can be generically replicated across all Institutions.

(2) The Framework is thus "principles" rather than "prescriptive" based and adopts the approach of elucidating the principles, standards, models and practices proven to support and sustain effective risk management.

(3) Institutions are expected to develop their systems of risk management by adopting the said principles and standards, and adapting the models and operational practices to match their specific Institutional requirements.

4. Background

(1) Institutions are bound by their Constitutional mandates to provide services or products in the interest of the public good.

(2) No organisation has the luxury of functioning in a risk-free environment and public Institutions are especially vulnerable to risks associated with fulfilling their mandates.

(3) The public sector environment is fraught with unique challenges such as inadequate capacity, excessive bureaucracy and silo mentality, limited resources, competing priorities and infrastructure backlogs to mention a few.

(4) Such dynamics increase the risk profile of the public sector as a whole and place an extra duty of care on public sector managers to contain risks within acceptable limits.

(5) Risk management is a valuable management tool which increases an Institution's prospects of success through minimising negative outcomes and optimising opportunities.

(6) Local and international trends confirm that risk management is a strategic imperative rather than an option within high performing organisations.

(7) High performing organisations set clear and realistic objectives, develop appropriate strategies aligned to the objectives, understand the intrinsic risks associated therewith and direct resources towards managing such risks on the basis of cost-benefit principles.

(8) Institutions must, in accordance with the previously mentioned prescripts, implement and maintain effective, efficient and transparent systems of risk management and internal control.

(9) The underlying intention of 4(8) is that Institutions should through the risk management process achieve, among other things, the following outcomes needed to underpin and enhance performance:

a) more sustainable and reliable delivery of services;

b) informed decisions underpinned by appropriate rigour and analysis;

c) innovation;

d) reduced waste;

e) prevention of fraud and corruption;

f) better value for money through more efficient use of resources; and

g) better outputs and outcomes through improved project and programme management.

SECTION 2: PROCESS FRAMEWORK

CHAPTER 3 - CREATING AN ENABLING ENVIRONMENT

5. Creating an enabling environment for the management of risks

(1) The Accounting Officer / Authority is responsible for ensuring that the Institutional environment supports the effective functioning of risk management.

(2) The Institution's environment is the foundation of risk management, providing the underpinning culture, discipline andstructure that influence how strategy and objectives are established, how Institutional activities are planned and executed and how risks are identified, assessed and acted upon.

(3) To give effect to 5(1), the Accounting Officer / Authority should ensure that the Institution:

a) operates within its Constitutional mandate;

b) adopts a value system founded on a public service ethos;

c) possesses the inherent competencies required to execute its mandate;

d) adopts management practices that embrace the concepts of delegation of authority, personal responsibility, accountability and performance management; and

e) has an appropriate organisational structure supported by basic financial and management systems underpinned by risk management and internal controls.

6. Setting institutional objectives

(1) The Accounting Officer / Authority should establish objectives that are consistent with the Institution's Constitutional mandate and ensure that its services are appropriate, economical, efficient and equitable.

(2) The Accounting Officer / Authority must ensure that:

a) objectives are finalised through a rigorous analysis of the costs and benefits associated therewith;

b) the Institution has and maintains an effective process to identify the risks inherent in the chosen objectives; and

c) the Institution is able to manage such risks effectively, economically and efficiently.

7. Risk management policy

(1) The Institution should operate within the terms of a risk management policy approved by the Accounting Officer / Authority.

(2) The risk management policy should:

a) communicate the Institution's risk management philosophy in the context of how risk management is expected to support the Institution in achieving its objectives;

b) incorporate a statement committing the Institution to implementing and maintaining an effective, efficient and transparent system of risk management;

c) define risk and risk management as they apply within the Institution's particular context;

d) spell out the objectives of risk management;

e) outline the risk management approach; and

f) identify the key role players and their responsibilities.

(3) The risk management policy should be communicated to all incumbent officials and arrangements should be made for communicating the policy to all new recruits.

8. Risk management strategy

(1) The implementation of the Institution's risk management policy should be guided by a strategy approved by the Accounting Officer / Authority.

(2) The strategy should include:

a) a plan of action to improve the Institution's risk management maturity;

b) a focus on the prevention of fraud and corruption;

c) the Institution's risk management architecture and reporting lines;

d) a description of the risk management modality;

e) user guidelines; and

f) details of review and assurance of the risk management process.

(3) In terms of 8(2)(b), the Institution must have a fraud prevention policy approved by the Accounting Officer / Authority expressing the Institution's commitment to managing fraud and corruption.

(4) The Institution must develop a fraud prevention strategy (including a plan) to guide the implementation of the fraud prevention policy.

9. Organisational structure

(1) The Accounting Officer / Authority should delegate roles and responsibilities in a manner that ensures effective co-ordination and synergy of risk management activities.

(2) To give effect to 9(1), the work of business units, working groups and committees should be structured and co-ordinated in a way that provides a complete perspective of the Institution's risk exposures and opportunities.

10. Human resource capacity

(1) Adequate human resources capacity, represented by the requisite number of people with the right skills, is fundamental to implementing the risk management strategy.

(2) Internal processes should be established to sensitise all employees of the relevance of risk management to the achievement of their performance goals.

(3) Training and support should be provided to everyone involved in risk management activities to equip them to optimally execute their responsibilities for risk management as set out in Section 3, read together with Section 4.

(4) The Chief Risk Officer and his/her staff should possess the necessary skills, competencies and attitudes to execute the functions set out in Chapter 14 read together with 34(5).

11. Tools and technology

(1) Tools and technology can produce considerable efficiencies by simplifying complex processes and accelerating otherwise time consuming tasks in the risk management process.

(2) Where appropriate consideration should be given to the use of automated tools for capturing, organising, storing and interrogating data, as well as communicating and tracking information.

(3) Notwithstanding 11(1) and 11(2), all officials should be mindful of the fact that technology is not a substitute for the human endeavour and intellect required for effective risk management.

12. Funding the risk management activities

(1) Funding is required to cover the cost of implementing, maintaining and continuously improving the state of risk management and control.

(2) The Chief Risk Officer should control the operating and capital costs of the Risk Management Unit.

(3) The cost of implementing and improving controls should be the responsibility of the respective Risk Owners, who should provide for such costs in their capital or operational budgets as the case may be.

(4) Investments in risk management and control should be considered on the basis of cost versus benefit.

CHAPTER 4 - INTEGRATION OF RISK MANAGEMENT ACTIVITIES

13. Enterprise-wide risk management (ERM)

(1) ERM is a broad-based application of risk management in all major functions and activities of the Institution, rather than only in selected areas, to isolate the material risks.

(2) ERM represents a response to the dilemma that risks (including opportunities) are dynamic and often highly interdependent and need to be managed through a portfolio approach rather than as separate and static events, to achieve comprehensive and integrated attention.

(3) ERM also calls for the Institution to look beyond itself, requiring the consideration of risks on performance regardless of whether risk is internally or externally generated.

(4) To give effect to 13(3), the Institution should:

a) communicate timeously with other organs of state in instances where the identification, evaluation and management of risk to the Institution require the participation of these organs;

b) identify and communicate to other organs of state risks posed to them by the Institution's own actions or inaction; and

c) consider the material risks throughout the value chain responsible for producing and delivering particular services or goods, to appreciate the threats posed by the non-performance of the parties in the value chain.

(5) The Institution must be aware of and comply with various legislations that prescribe the specific treatment of risk within their ambit, for example, Occupational Health and Safety Act, Disaster Management Act, Prevention of Fraud and Corruption Act and others.

(6) Formal channels of communication and co-operation should exist within the Institution to facilitate synergy between the Risk Management Unit and Risk Management Committee, and internal formations concerned with risk mitigation, including but not limited to formations responsible for:

a) occupational health and safety;

b) business continuity management;

c) prevention of fraud and corruption; and

d) awarding of tenders.

CHAPTER 5 - RISK IDENTIFICATION

14. Risk identification

(1) Risk identification is a deliberate and systematic effort to identify and document the Institution's key risks.

(2) 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.

(3) The Institution should adopt a rigorous and ongoing process of risk identification that also includes mechanisms to identify new and emerging risks timeously.

(4) The risk identification process should cover all risks, regardless of whether or not such risks are within the direct control of the Institution.

(5) 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.

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

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

a) review of external and internal audit reports;

b) review of the reports of the Standing Committee on Public Accounts and the relevant Parliamentary Committee(s);

c) financial analyses;

d) historic data analyses;

e) actual loss data;

f) interrogation of trends in key performance indicators;

g) benchmarking against peer group or quasi peer group;

h) market and sector information;

i) scenario analyses; and

j) forecasting and stress testing.

15. Focus points of risk identification

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

a) (a) 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:

(i) strategic risk identification should precede the finalisation of strategic choices to ensure that potential risk issues are factored into the decision making process for selecting the strategic options;

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

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

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

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

(ii) 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

(iii) to the extent that 15(1)(b)(ii) is deemed inadequate to expose the full extent of risk introduced by significant environmental or Institutional changes, operational risk identification should be repeated when changes occur, or at least once a year, to identify new and emerging risks.

c) Project risk identification to identify risks inherent to particular projects:

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

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

CHAPTER 6 - RISK ASSESSMENT

16. Risk assessment

(1) 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.

(2) 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.

(3) 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.

(4) Risks should be expressed in the same unit of measure used for the key performance indicator(s) concerned.

(5) Risk assessment should be performed through a three stage process:

a) firstly, the inherent risk should be assessed to establish the level of exposure in the absence of deliberate management actions to influence the risk;

b) secondly, a residual risk assessment should follow the process described in 16(4)(a) to determine the actual remaining level of risk after the mitigating effects of management actions to influence the risk; and

c) thirdly, the residual risk should be benchmarked against the Institution's risk appetite to determine the need for further management intervention, if any.

(6) Risk assessment should be strengthened where possible by supplementing Management's perceptions with the methods referred to in 14(7).

(7) 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.

CHAPTER 7 - RISK RESPONSE

17. Responding to risks

(1) Risk response is concerned with developing strategies to reduce or eliminate the threats and events that create risks.

(2) Risk response should also make provision for the exploitation of opportunities to improve the performance of the Institution.

(3) Responding to risk involves identifying and evaluating the range of possible options to mitigate risks and implementing the chosen option.

(4) Management should develop response strategies for all material risks, whether or not the management thereof is within the direct control of the Institution, prioritising the risks exceeding or nearing the risk appetite level.

(5) Where the management of the risk is within the control of the Institution, the response strategies should consider:

a) avoiding the risk by, for example, choosing a different strategy or terminating the activity that produces the risk;

b) treating the risk by, for example, implementing or improving the internal control system;

c) transferring the risk to another party more competent to manage it by, for example, contracting out services, establishing strategic partnerships and buying insurance;

d) accepting the risk where cost and strategy considerations rule out alternative strategies; and

e) exploiting the risk factors by implementing strategies to take advantage of the opportunities presented by such risk factors.

(6) In instances where the management of risk is not within the control of the Institution, the response strategies should consider measures such as forward planning and lobbing.

(7) Response strategies should be documented and the responsibilities and timelines attached thereto should be communicated to the relevant persons.

18. Designing control activities to mitigate risks

(1) Management is responsible for designing, implementing and monitoring the effective functioning of system internal controls.

(2) Without derogating from the above, everyone in the Institution should also have responsibilities for maintaining effective systems of internal controls, consistent with their delegated authority.

(3) Management should develop the internal control architecture through:

a) preventative controls to prevent errors or irregularities from occurring e.g. physical security of assets to prevent theft;

b) detective controls to find errors or irregularities after they have occurred e.g. performance of reconciliation procedures to identify errors; and

c) corrective controls that operate together with detective controls to correct errors or irregularities.

(4) The internal control architecture should include:

a) management controls to ensure that the Institution's structure and systems support its policies, plans and objectives, and that it operates within laws and regulations;

b) administrative controls to ensure that policies and objectives are implemented in an efficient and effective manner;

c) accounting controls to ensure that resources are accounted for fully and transparently and are properly documented; and

d) information technology controls to ensure security, integrity and availability of information.

CHAPTER 8 - COMMUNICATION AND REPORTING

19. Communication and reporting

(1) Relevant information, properly and timeously communicated is essential to equip the relevant officials to identify, assess and respond to risks.

(2) The Institution's risk communication and reporting process should support enhanced decision making and accountability through:

a) dissemination of relevant, timely, accurate and complete information; and

b) communicating responsibilities and actions.

CHAPTER 9 - MONITORING

20. Risk monitoring

(1) Monitoring concerns checking on a regular basis to confirm the proper functioning of the entire risk management system.

(2) Monitoring should be effected through ongoing activities or separate evaluations to ascertain whether risk management is effectively practised at all levels and across the Institution in accordance with the risk management policy, strategy and plan.

(3) Monitoring activities should focus on evaluating whether:

a) allocated responsibilities are being executed effectively;

b) response strategies are producing the desired result of mitigating risks or exploiting opportunities; and

c) a positive correlation exists between improvements in the system of risk management and Institutional performance.

SECTION 3: ROLES AND RESPONSIBILITIES

CHAPTER 10 - RISK MANAGEMENT FUNCTIONS OF EXECUTIVE AUTHORITIES

21. Functions of Executive Authority with respect to risk management

(1) The Executive Authority should take an interest in risk management to the extent necessary to obtain comfort that properly established and functioning systems of risk management are in place to protect the Institution against significant risks.

(2) Responsibilities of the Executive Authority in risk management should include:

a) ensuring that the Institutional strategies are aligned to the government mandate;

b) obtaining assurance from management that the Institution's strategic choices were based on a rigorous assessment of risk;

c) obtaining assurance that key risks inherent in the Institution's strategies were identified and assessed, and are being properly managed;

d) assisting the Accounting Officer / Authority to deal with fiscal, intergovernmental, political and other risks beyond their direct control and influence; and

e) insisting on the achievement of objectives, effective performance management and value for money.

(3) In case of a municipality or municipal entity, in addition to the responsibilities outlined in 21(2), the Executive Authority should also:

a) approve the risk management policy, strategy, and implementation plan; and

b) approve the fraud prevention policy, strategy and implementation plan.

CHAPTER 11 - RISK MANAGEMENT FUNCTONS OF ACCOUNTING OFFICERS / AUTHORITIES

22. Functions of Accounting Officer / Authority with respect to risk management

(1) The Accounting Officer / Authority is the ultimate Chief Risk Officer of the Institution and is accountable for the Institution's overall governance of risk.

(2) High level responsibilities of the Accounting Officer / Authority should include:

a) setting an appropriate tone by supporting and being seen to be supporting the Institution's aspirations for effective management of risks;

b) delegating responsibilities for risk management to Management and internal formations such as the Risk Management Committee, Fraud Prevention Committee, Finance Committee, Information and Communication Technology Committee;

c) holding Management accountable for designing, implementing, monitoring and integrating risk management into their day-to-day activities;

d) holding the internal structures referred to in 22(2)(b) accountable for performance in terms of their responsibilities for risk management;

e) providing leadership and guidance to enable Management and internal structures responsible for various aspects of risk management to properly perform their functions;

f) ensuring that the control environment supports the effective functioning of risk management as discussed in Chapter 3;

g) approving the risk management policy, strategy, and implementation plan;

h) approving the fraud prevention policy, strategy and implementation plan;

i) approving the Institution's risk appetite and risk tolerance;

j) devoting personal attention to overseeing management of the significant risks;

k) leveraging the Audit Committee, Internal Audit, External Audit and Risk Management Committee for assurance on the effectiveness of risk management;

l) ensuring appropriate action in respect of the recommendations of the Audit Committee, Internal Audit, External Audit and Risk Management Committee to improve risk management; and

m) providing assurance to relevant stakeholders that key risks are properly identified, assessed and mitigated.

CHAPTER 12 - RISK MANAGEMENT FUNCTIONS OF AUDIT COMMITTEES

23. Functions of the Audit Committee with respect to risk management

(1) The Audit Committee is an independent committee responsible for oversight of the Institution's control, governance and risk management.

(2) The responsibilities of the Audit Committee with respect to risk management should be formally defined in its charter.

(3) The Audit Committee should provide an independent and objective view of the Institution's risk management effectiveness.

(4) Responsibilities of the Audit Committee, where there is a separate Risk Management Committee, should include:

a) reviewing and recommending disclosures on matters of risk in the annual financial statements;

b) reviewing and recommending disclosures on matters of risk and risk management in the annual report;

c) providing regular feedback to the Accounting Officer / Authority on the adequacy and effectiveness of risk management in the Institution, including recommendations for improvement;

d) ensuring that the internal and external audit plans are aligned to the risk profile of the Institution;

e) satisfying itself that it has appropriately addressed the following areas:

(i) financial reporting risks, including the risk of fraud;

(ii) internal financial controls; and

(iii) IT risks as they relate to financial reporting.

(5) Where there is no separate Risk Management Committee, the risk management responsibilities of the Audit Committee should be identical to those listed in 24(5).

(6) The Audit Committee should evaluate the effectiveness of Internal Audit in its responsibilities for risk management.

CHAPTER 13 - FUNCTIONS OF RISK MANAGEMENT COMMITTEES

24. Functions of the Risk Management Committee

(1) The Risk Management Committee is appointed by the Accounting Officer / Authority to assist them to discharge their responsibilities for risk management.

(2) The membership of the Risk Management Committee should comprise both management and external members with the necessary blend of skills, competencies and attributes, including the following critical aspects:

a) an intimate understanding of the Institution's mandate and operations;

b) the ability to act independently and objectively in the interest of the Institution; and

c) a thorough knowledge of risk management principles and their application.

(3) The chairperson of the Risk Management Committee should be an independent external person, appointed by the Accounting Officer / Authority.

(4) The responsibilities of the Risk Management Committee should be formally defined in a charter approved by the Accounting Officer / Authority.

(5) In discharging its governance responsibilities relating to risk management, the Risk Management Committee should:

a) review and recommend for the Approval of the Accounting Officer / Authority, the:

(i) risk management policy;

(ii) risk management strategy;

(iii) risk management implementation plan;

(iv) Institution's risk appetite, ensuring that limits are:

* supported by a rigorous analysis and expert judgement;

* expressed in the same values as the key performance indicators to which they apply;

* set for all material risks individually, as well as in aggregate for particular categorisations of risk; and

* consistent with the materiality and significance framework.

(v) Institution's risk tolerance, ensuring that limits are supported by a rigorous analysis and expert judgement of:

* the Institution's ability to withstand significant shocks; and

* the Institution's ability to recover financially and operationally from significant shocks.

(vi) Institution's risk identification and assessment methodologies, after satisfying itself of their effectiveness in timeously and accurately identifying and assessing the Institution's risks.

b) evaluate the extent and effectiveness of integration of risk management within the Institution;

c) assess implementation of the risk management policy and strategy (including plan);

d) evaluate the effectiveness of the mitigating strategies implemented to address the material risks of the Institution;

e) review the material findings and recommendations by assurance providers on the system of risk management and monitor the implementation of such recommendations;

f) develop its own key performance indicators for approval by the Accounting Officer / Authority;

g) interact with the Audit Committee to share information relating to material risks of the Institution; and

h) provide timely and useful reports to the Accounting Officer / Authority on the state of risk management, together with accompanying recommendations to address any deficiencies identified by the Committee.

(6) In instances where the scale, complexity and geographical dispersion of the Institution's activities dictate the need for the Risk Management Committee to work through sub-committees, the Risk Management Committee should ensure that:

a) approval is obtained from the Accounting Officer / Authority for the establishment of the sub-committees;

b) the terms of reference of the sub-committees are aligned to that of the Risk Management Committee; and

c) the Risk Management Committee exercises control over the functioning of the sub-committees.

CHAPTER 14 - FUNCTIONS OF CHIEF RISK OFFICERS

25. Functions of the Chief Risk Officer

(1) The primary responsibility of the Chief Risk Officer is to bring to bear his / her specialist expertise to assist the Institution to embed risk management and leverage its benefits to enhance performance.

(2) The high level responsibilities of the Chief Risk Officer should include:

a) working with senior management to develop the Institution's vision for risk management;

b) developing, in consultation with management, the Institution's risk management framework incorporating, ***inter alia***, the:

(i) risk management policy;

(ii) risk management strategy;

(iii) risk management implementation plan;

(iv) risk identification and assessment methodology;

(v) risk appetite and tolerance; and

(vi) risk classification.

c) communicating the Institution's risk management framework to all stakeholders in the Institution and monitoring its implementation;

d) facilitating orientation and training for the Risk Management Committee;

e) training all stakeholders in their risk management functions;

f) continuously driving risk management to higher levels of maturity;

g) assisting Management with risk identification, assessment and development of response strategies;

h) monitoring the implementation of the response strategies;

i) collating, aggregating, interpreting and analysing the results of risk assessments to extract risk intelligence;

j) reporting risk intelligence to the Accounting Officer / Authority, Management and the Risk Management Committee; and

k) participating with Internal Audit, Management and Auditor-General in developing the combined assurance plan for the Institution.

CHAPTER 15 - RISK MANAGEMENT FUNCTIONS OF MANAGEMENT

26. Functions of Management with respect to risk management

(1) Management is responsible for executing their responsibilities outlined in the risk management strategy and for integrating risk management into the operational routines.

(2) High level responsibilities of Management should include:

a) executing their responsibilities as set out in the risk management strategy;

b) empowering officials to perform effectively in their risk management responsibilities through proper communication of responsibilities, comprehensive orientation and ongoing opportunities for skills development;

c) aligning the functional risk management methodologies and processes with the Institutional process;

d) devoting personal attention to overseeing the management of key risks within their area of responsibility;

e) maintaining a co-operative relationship with the Risk Management Unit and Risk Champion;

f) providing risk management reports;

g) presenting to the Risk Management and Audit Committees as requested;

h) maintaining the proper functioning of the control environment within their area of responsibility;

i) monitoring risk management within their area of responsibility; and

j) holding officials accountable for their specific risk management responsibilities.

CHAPTER 16 - RISK MANAGEMENT FUNCTIONS OF OTHER OFFICIALS

27. Functions of other officials with respect to risk management

(1) Other officials are responsible for integrating risk management into their day-to-day activities.

(2) High level responsibilities of other officials should include:

a) applying the risk management processes in their respective functions;

b) implementing the delegated action plans to address the identified risks;

c) informing their supervisors and/or the Risk Management Unit of new risks and significant changes in known risks; and

d) co-operating with other role players in the risk management process and providing information as required.

CHAPTER 17 - FUNCTIONS OF RISK CHAMPIONS

28. Functions of the Risk Champion

(1) The Risk Champion is a person with the skills, knowledge, leadership qualities and power of office required to champion a particular aspect of risk management.

(2) A key part of the Risk Champion's responsibility should involve intervening in instances where the risk management efforts are being hampered, for example, by the lack of co-operation by Management and other officials and the lack of institutional skills and expertise.

(3) The Risk Champion should also add value to the risk management process by providing guidance and support to manage "problematic" risks and risks of a transversal nature that require a multiple participant approach.

(4) In order to fulfil his/her function, the Risk Champion should possess:

a) a good understanding of risk management concepts, principles and processes;

b) good analytical skills;

c) expert power;

d) leadership and motivational qualities; and

e) good communication skills.

(5) The Risk Champion should not assume the role of the Risk Owner but should assist the Risk Owner to resolve problems.

CHAPTER 18 - RISK MANAGEMENT FUNCTIONS OF INTERNAL AUDITING

29. Functions of Internal Auditing with respect to risk management

(1) The role of the Internal Auditing in risk management is to provide an independent, objective assurance on the effectiveness of the Institution’s system of risk management.

(2) Internal Auditing must evaluate the effectiveness of the entire system of risk management and provide recommendations for improvement where necessary.

(3) Internal Auditing must develop its internal audit plan on the basis of the key risk areas.

(4) In terms of the International Standards for the Professional Practice of Internal Audit, determining whether risk management processes are effective is a judgment resulting from the Internal Auditor's assessment that:

a) Institutional objectives support and align with the Institution's mission;

b) significant risks are identified and assessed;

c) risk responses are appropriate to limit risk to an acceptable level; and

d) relevant risk information is captured and communicated in a timely manner to enable the Accounting Officer / Authority, Management, the Risk Management Committee and other officials to carry out their responsibilities.

(5) In case where the Internal Auditor assumes the role of the Chief Risk Officer, his/her risk management responsibilities include:

a) assisting Management to develop the risk management policy, strategy and implementation plan;

b) co-ordinating risk management activities;

c) facilitating identification and assessment of risks;

d) recommending risk responses to Management; and

e) developing and disseminating risk reports.

(6) When assisting Management in establishing or improving risk management processes, Internal Auditing must refrain from assuming management responsibilities for risk management.

CHAPTER 19 - RISK MANAGEMENT FUNCTIONS OF EXTERNAL AUDIT

30. Functions of the External Audit with respect to risk management

(1) The external auditor (Auditor-General) provides an independent opinion on the effectiveness of risk management.

(2) In providing the audit opinion, the Auditor- General usually focuses on:

a) determining whether the risk management policy, strategy and implementation plan are in place and are appropriate;

b) assessing the implementation of the risk management policy, strategy and implementation plan;

c) reviewing the risk identification process to determine if it is sufficiently robust to facilitate the timely, correct and complete identification of significant risks, including new and emerging risks;

d) reviewing the risk assessment process to determine if it is sufficiently robust to facilitate timely and accurate risk rating and prioritisation; and

e) determining whether the management action plans to mitigate the key risks are appropriate, and are being effectively implemented.

CHAPTER 20 - RISK MANAGEMENT FUNCTIONS OF THE NATIONAL TREASURY

31. Functions of the National Treasury with respect to risk management

(1) The National Treasury has specific functions in terms of section 6(2) of the PFMA and sections 5(2) and 34 of the MFMA to:

a) prescribe uniform norms and standards;

b) monitor and assess the implementation of the PFMA and MFMA;

c) assist Institutions in building their capacity for efficient, effective and transparent financial management; and

d) enforce the PFMA and MFMA.

(2) To give effect to 31(1)(b), the National Treasury should monitor and assess, among other things, the implementation of risk management, including any prescribed norms and standards.

(3) With respect to capacity building, the National Treasury should assist national departments, national public entities, Constitutional institutions, municipalities and municipal entities in building their capacity for, among other things, efficient, effective and transparent risk management.

(4) With respect to enforcement, the National Treasury should enforce the legislation and any prescribed norms and standards for, among other things, risk management in national departments, national public entities, Constitutional institutions, municipalities and municipal entities.

(5) In addition, the National Treasury may do anything further that is necessary to fulfil its responsibilities effectively.

CHAPTER 21 - RISK MANAGEMENT FUNCTIONS OF THE PROVINCIAL TREASURIES

32. Functions of the Provincial Treasury with respect to risk management

(1) The Provincial Treasury has specific functions in terms of section 18(2) of the PFMA and sections 5(4) and 34 of the MFMA to:

a) prescribe uniform norms and standards;

b) monitor and assess the implementation of the PFMA and MFMA;

c) assist Institutions in building their capacity for efficient, effective and transparent financial management; and

d) enforce the PFMA and MFMA.

(2) To give effect to 32(1)(b), the Provincial Treasury should monitor and assess, among other things, the implementation of risk management, including any prescribed norms and standards.

(3) With respect to capacity building, the Provincial Treasury should assist provincial departments, provincial public entities, municipalities and municipal entities, in among other things, in building their capacity for efficient, effective and transparent risk management.

(4) With respect to enforcement, the Provincial Treasury should enforce the legislation and any prescribed norms and standards for, among other things, risk management in provincial departments, provincial public entities, municipalities and municipal entities.

(5) In addition, the Provincial Treasury may do anything further that is necessary to fulfil its responsibilities effectively.

SECTION 4: PERFORMANCE AND EVALUATION OF RISK MANAGEMENT

CHAPTER 22 - EVALUATION OF RISK MANAGEMENT EFFECTIVENESS

33. Evaluation of value add

(1) Evaluation of risk management effectiveness is vital to maximise the value created through risk management practices.

(2) Institutions should strive to incrementally and sustainably achieve a mature risk management regime in order to realise the outcomes referred to in 4(9).

(3) Institutions should periodically evaluate the value add of risk management by measuring outcomes against preset key performance indicators aligned to the overall goals and objectives of the Institution.

(4) Institutions should utilise the Financial Management Maturity Capability Model developed by the National Treasury to evaluate their current and progressive risk management maturity.

34. Performance Indicators

(1) Everyone in the Institution has a part to play in achieving and sustaining a vibrant system of risk management and to that extent must function within a framework of responsibilities and performance indicators.

(2) The Accounting Officer / Authority should evaluate its own performance in leading the risk management process in the Institution through the following and other relevant indicators:

a) the risk management maturity trend as measured in terms of an appropriate index such as the Financial Capability Maturity Model;

b) the Institution's performance against key indicators, including comparison of year-on-year performance;

c) the Institution’s “avoided risk” record when compared against the peer group or quasi-peer group;

d) percentage change in unauthorised expenditure, fruitless and wasteful expenditure and irregular expenditure based on year-on-year comparisons;

e) percentage change in incidents and quantum of fraud based on year-on-year comparisons; and

f) progress in securing improved audit outcomes in regularity and performance audits.

(3) Insofar as it concerns the responsibilities of the Audit Committee for risk management, the Accounting Officer / Authority should evaluate the performance of the Committee through the following and other relevant indicators:

a) the Auditor-General’s report on the effectiveness of the Audit Committee;

b) the results of the Audit Committee's own 360? assessment;

c) the Committee's co-ordination of the work of Internal Auditing, External Audit and other assurance providers in respect of risk management; and

d) the quality and timeliness of the Audit Committee's counsel and recommendations on matters concerning the system of risk management.

(4) The Accounting Officer / Authority should evaluate the performance of the Risk Management Committee through the following and other relevant indicators:

a) the results of the Risk Management Committee's own 360? assessment;

b) the pace and quality of the implementation of the risk management framework;

c) the Internal Audit report on the state of risk management;

d) the Auditor-General's report on the effectiveness of the Risk Management Committee; and

e) the quality and timeliness of the Risk Management Committee's counsel and recommendations.

(5) The Accounting Officer / Authority, in consultation with the Risk Management Committee, should evaluate the performance of the Chief Risk Officer through the following and other relevant indicators:

a) development and implementation of the risk management policy, strategy and implementation plan;

b) the Institution's collective awareness, skill and participation in risk management;

c) risk management maturity;

d) quality and timeliness of support to Management, other officials and the Risk Management Committee;

e) quality and timeliness of risk intelligence; and

f) absence of surprises.

(6) The Accounting Officer / Authority should evaluate the performance of Management through the following and other relevant indicators:

a) business unit performance against key indicators, including comparison of year-on year performance;

b) implementation of risk management action plans;

c) co-operation with the Risk Management Unit, Risk Management Committee, Risk Champion and relevant stakeholders involved in risk management;

d) quality and timeliness of risk identification, assessment and reporting;

e) proactive identification of new and emerging risks;

f) absence of surprises;

g) year-on-year reduction in adverse incidents and realised losses;

h) elimination of unauthorised expenditure, fruitless and wasteful expenditure and irregular expenditure;

i) reduction in fraud; and

j) progress in securing improved Internal Audit and Auditor-General outcomes in regularity and performance audits.

(7) The Accounting Officer / Authority should evaluate the performance of Risk Champions through the following and other relevant indicators:

a) resolution of delegated problems.

(8) Insofar as it concerns the responsibilities of Internal Auditing for risk management, the Accounting Officer / Authority should evaluate the performance of Internal Auditing through the following and other relevant indicators:

a) timeliness and quality of assurance on risk management;

b) timeliness and quality of recommendations to improve risk management; and

c) adoption of risk based auditing.

(9) Management should evaluate the performance of their staff through the following and other relevant indicators:

a) implementation of risk management action plans.

REFERENCES

1. Companies Act No. 71 of 2008.

2. COSO Enterprise Risk Management – Integrated Framework 2004.

3. COSO – Strengthening Enterprise Risk Management for Strategic Advantage, 2009.

4. Draft International Standards ISO/DIS 31000, 2008.

5. Framework for Managing Programme Performance Information 2007.

6. International Standards for the Professional Practice of Internal Audit.

7. King Code of Governance for South Africa 2009.

8. Municipal Finance Management Act no. 56 of 2003.

9. Public Finance Management Act no. 1 of 1999.

10. Public Service Regulations, 2001.

11. The Orange Book, Management of Risk – Principles and Concepts, October 2004.

12. Treasury Regulations (issued in terms of PFMA)