KWAZULU NATAL PROVINCIAL TREASURY

PROVINCIAL RISK MANAGEMENT FRAMEWORK

CONTENTS

1. Foreword by the MEC of Finance 3
2. Background 4
2.2. Definitions 5
3. The purpose of the Enterprise Risk Management (ERM) Framework 5
3.1 Benefits of the ERM policy and framework 6
3.2 Legal mandate 6
3.2.1 Enterprise Risk Management Framework Guidelines 7
4 Risk Management Structures 7
4.1. Provincial Risk Management Oversight structure 7
4.2 Departmental Risk Management Structure 8
4.3 Public Entities Risk Management Structures 8
4.4. Provincial Risk Reporting 9
5 Roles, responsibilities and governance 9
5.1 Members of the Executive Committee (MECs) 9
5.2 MEC Finance 10
5.3 Heads of institutions (Accounting Officers / Accounting Authorities) 10
5.4 Provincial Risk Management Committee (HODs) 11
5.5 KwaZulu Natal Provincial Treasury 12
5.6 Audit Committee 12
5.7 Focused/Internal Risk Management Committee/ MANCO 13
5.8 Fraud Prevention Committee 13
5.9 Business Unit/Programme Heads 14
5.10 Chief Risk Officer (CRO) 14
5.11 Internal Audit 15
5.12 Provincial Chief Risk Officers' Forum 15
6 Enterprise Risk Management (ERM) Approach 15
6.1 Risk Profiles 16
6.2 Fraud Risk Assessment 17
6.3 Developing risk profiles 17
6.3.1 Risk Identification 17
6.3.2 Risk Categories 18
6.3.3 Risk Assessment 20
7 Reporting 26
8 Combined Assurance 27
9 Monitoring 28
10 Embedding Risk Management 29

1. Foreword by the MEC of Finance

In the past, management of risk in the public service has not received adequate attention. With the introduction of the Public Finance Management Act (PFMA), Act 1 of 1999, the foundation has been laid for a more effective corporate governance framework as well as an accountable financial management system for the public sector. The Act has also established the legal framework for risk management in the public sector.

Today, more than ever, those in the public sector should be taking a long, hard look at risk – the threats to success and the possible consequences if they materialize. The importance of looking at risk comes in the wake of a more demanding society, bold initiatives and more challenge when things go wrong.

Public sector ***risk management and control*** should be firmly on the ***agenda*** for everyone involved in the public sector. Effective risk management processes will ultimately help achieve:

- **Greater organizational clarity of purpose** by clearly identifying policy needs and actions required to meet strategic objectives,
- **More cohesiveness of effort** through organizational consistency and clear role definition, **better decisions** through consideration of issues,
- **Faster reactions** through concentration on key performance trends, and
- **Accountability** by recording decisions in context and allocating responsibility for action.

Risk management processes and responsibilities are incorporated in the list of responsibilities allocated to Accounting Officers, Accounting Authorities and Audit Committees. However, these responsibilities are extended to all Managers in terms of the provisions of the PFMA. The PFMA establish responsibility for ***Risk Management at all levels of management*** and thus becomes everybody's responsibility. This should be seen as a medium term vision and to be successful it must assist in organizational and individual ***behavioural change*** and be seen to be of benefit to the individual as well as the organization.

We endorse the adoption of this risk management framework by institutions as a fundamental step towards an outward looking, accountable and innovative Public Sector.

Yours sincerely

_____
DR Z. L. MKHIZE, MP
MEC FOR FINANCE AND ECONOMIC DEVELOPMENT
DATE: _____

2. Background

Enterprise Risk Management (ERM) forms a critical part of any institution's strategic management. It is the process whereby an institution both methodically and intuitively addresses the risk attached to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of activities. ERM is therefore recognized as an integral part of sound organizational management and is being promoted internationally and in South Africa as good practice applicable to the public and private sectors.

The underlying premise of risk management is that every governmental body exists to provide value for its stakeholders. Such value is based on the quality of service delivery to the citizens. All institutions face uncertainty, and the challenge for management is to determine how much **uncertainty** the institution is prepared to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance **value**. The framework provides a basis for management to effectively deal with uncertainty of associated risk and opportunity, thereby enhancing its capacity to build value. Value is maximized when management sets objectives to strike an optimal balance between growth and related risks, and effectively deploys resources in pursuit of the institution's objectives. It is accordingly accepted by all stakeholders that Kwa Zulu Natal Provincial Government (KZNPG) will manage the risks faced in its various institutions in an appropriate manner.

2.1 Uncertainty

Institutions operate in environments where factors such as technology, regulation, restructuring, changing service requirements and political influence create uncertainty. Uncertainty emanates from an inability to precisely determine the likelihood that potential events will occur and the associated outcomes.

The ***Enterprise Risk Management Policy*** provides a framework within which management can operate to enforce the pro-active ERM process and to inculcate the risk management culture throughout KZNPG and its institutions and to further ensure that the risk management efforts of KZNPG and its institutions are optimised. It describes KZNPG's and its institutions' ERM processes and sets out the requirements for management in generating risk management action, together with furthering risk management assurance. This document further sets out KZNPG's policy on the management of risk at all levels of the organisation.

The ***Enterprise Risk Management Framework*** specifically addresses the structures, processes and standards implemented to manage risks on an enterprise-wide basis in a consistent manner. The ***Enterprise Risk Management Standards*** further address the specific responsibilities and accountabilities for the ERM process and the reporting of risks and incidences at various levels within KZNPG and its institutions. As the field of risk management is dynamic, this framework document is expected to change from time to time.

KZNPG and its institutions are obliged to adhere to the Treasury Regulations in terms of the Public Finance and Management Act, 1999 (PFMA).

Current trends in good corporate governance have given special prominence to the process of ERM and reputable organisations are required to demonstrate that they comply with expected risk management standards. This means that KZNPG must ensure that the process of risk management receives special attention throughout the organisations and that ***all levels of management know, understand and comply with framework document.***

2.2. Definitions

Risk

The Institute of Risk Management defines **risk** as "…***the uncertainty of an event occurring that could have an impact on the achievement of objectives.*** Risk is measured in terms of consequences of impact and likelihood."

This definition applies to each and every level of the enterprise and is KZNPG's overriding policy and philosophy that the management of risk is the responsibility of management at each and every level in KZNPG and its institutions. The management of risk is no more or less important than the management of organisational resources and opportunities and it simply forms an integral part of the process of managing those resources and opportunities.

Enterprise Risk Management

ERM deals with risks and opportunities affecting value creation or preservation and is defined as follows with reference to COSO (The Committee of Sponsoring Organisations of the Treadway Commission):

" a continuous, proactive and systematic process, effected by an institution's executive authority, executive council, accounting authority, accounting officer, management and other personnel, applied in strategic planning and across the institution, designed to identify potential events that may affect the institution, and manage risks to be within its risk tolerance, to provide reasonable assurance regarding the achievement of institution objectives."

3. The purpose of the Enterprise Risk Management (ERM) Framework

The purpose of the ERM framework is to provide a comprehensive approach to better integrate risk management into strategic decision-making; and

- Provide guidance for accounting officers, accounting authorities, managers and staff when overseeing or implementing the development of processes, systems and techniques for managing risk, which are appropriate to the context of the department or public entity.
- Advance the development and implementation of modern management practices and to support innovation throughout the Public Sector;
- Contribute to building a risk-smart workforce and environment that allows for innovation and responsible risk-taking while ensuring legitimate precautions are taken to protect the public interest, maintain public trust, and ensure due diligence;

It is anticipated that the implementation of the Enterprise Risk Management Framework will:

- Support KZNPG's governance responsibilities by ensuring that significant risk areas associated with policies, plans, programs and operations are identified and assessed, and that appropriate measures are in place to address unfavourable impacts;
- Improve results through more informed decision-making, by ensuring that values, competencies, tools and the supportive environment form the foundation for innovation and responsible risk-taking, and by encouraging learning from experience;
- Strengthen accountability by demonstrating that levels of risk associated with policies, plans, programs and operations are explicitly understood and that investment in risk management measures and stakeholder interests are optimally balanced; and
- Enhance stewardship and transparency by strengthening public sector capacity to safeguard human resources, property and interests.

3.1 Benefits of the ERM policy and framework

The benefits of the Enterprise Risk Management Policy and Framework are as follows:

- **Aligning risk appetite and strategy** – KZNPG's management considers their risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- **Pursuing institutional objectives through transparent identification and management of acceptable risk** – There is a direct relationship between objectives, which are what an entity strives to achieve and the ERM components, which represent what is needed to achieve the objectives.
- **Providing an ability to prioritise the risk management activity –** Risk quantification techniques assist management in prioritising risks to ensure that resources and capital are focused on high priority risks faced by KZNPG's.
- **Enhancing risk response decisions** – ERM provides the rigor for management to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.
- **Reducing operational surprises and losses** - KZNPG gains enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- **Identifying and managing multiple and cross-enterprise risks** - KZNPG faces a myriad of risks affecting different parts of KZNPG and ERM facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.
- **Seizing opportunities** - By considering a full range of potential events, KZNPG management is positioned to identify and proactively realize opportunities.
- **Improving deployment of capital** - Obtaining robust risk information allows KZNPG management to effectively assess overall capital needs and enhance capital allocation.
- **Ensuring compliance with laws and regulations** – ERM helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to KZNPG's reputation and associated consequences.
- **Increasing probability of achieving objectives** – ERM assists management in achieving KZNPG's performance and profitability targets and prevents loss of resources. Controls and risk interventions will be chosen on the basis that they increase the likelihood that KZNPG will fulfill its intentions to stakeholders.

3.2 Legal mandate

The Public Finance Management Act, 1999 supplemented by the relevant Treasury Regulations has legislated key governance best practices.

Section 38 (a) of the Public Finance Management Act, 1999 requires that:

"The accounting officer has and maintains:

1. *Effective, efficient and transparent systems of financial and risk management and internal control."*

Section 51 (1) (a) (i) of the PFMA requires that:

"An Accounting Authority for a public entity" –
(a) must ensure that the public entity has and maintains -

- *(i) effective, efficient and transparent systems of financial and risk management and internal control."*

The extension of general responsibilities in terms of section 45 and 57 of the Public Finance Management Act, 1999 to all managers within the public sector implies that responsibility for risk management vests at all levels of management and that it is not limited to only the accounting officer and internal audit.

The roles and responsibilities for the implementation of the ERM strategy is contained in the Treasury Regulations published in terms of the Public Finance Management Act, 1999. Section 3.2 and 27.2.1 of the regulations addresses risk management summarized as follows:

- *The accounting officer must ensure that a risk assessment is conducted regularly to identify emerging risks for the institution.*
- *The risk management strategy, which must include a fraud prevention plan, must be used to direct internal audit effort and priority and to determine the skills required of managers and staff to improve controls and to manage these risks.*
- *The risk management strategy must be clearly communicated to all officials to ensure that it is incorporated into the language and culture of the institution and embedded in the behaviour and mindset of its people.*

3.2.1 Enterprise Risk Management Framework Guidelines

The Enterprise Risk Management Framework adopted by KZNPG ensures that key risks are identified, measured and managed. The Enterprise Risk Management Framework provides management with proven risk management tools that support their decision-making responsibilities and processes, together with managing risks (threats and opportunities), which impact on the objectives and key value drivers of KZNPG.

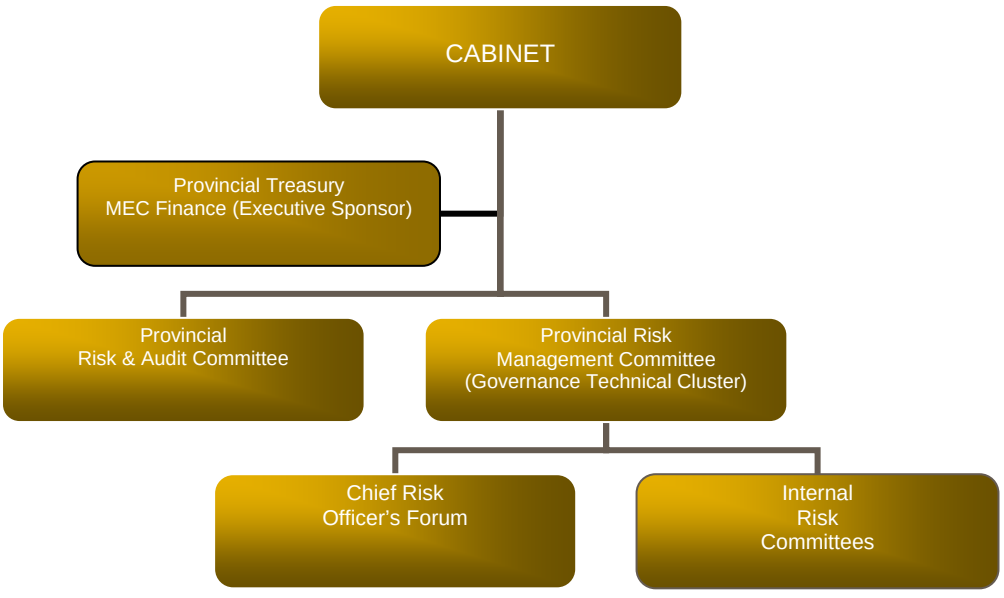
KZNPG has determined that ERM is everyone's responsibility and that it must be embedded into the everyday activities of all the institutions. This implies that ERM must be part of every decision that is made, every objective that is set and every process that is designed. Detailed ERM responsibilities for key risk management role players are listed below.

3.3. Applicability of the framework

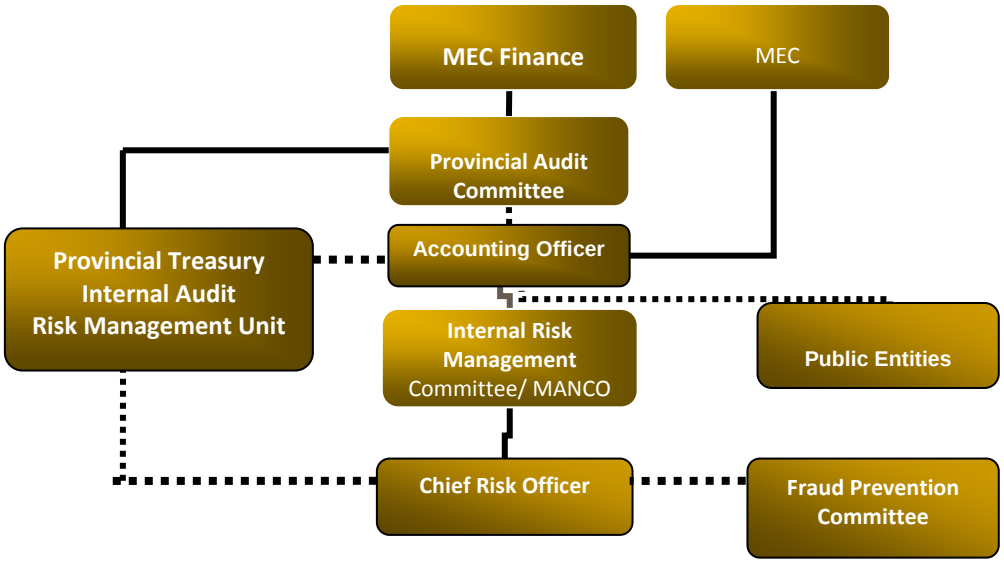
The Provincial Risk Management framework shall be applicable to all provincial departments including provincial parliament and the provincial public entities. Each department and public entity shall have a policy statement which makes reference to this framework. The sample policy statement is attached as Annexure 1 of the framework.

4 Risk Management Structures

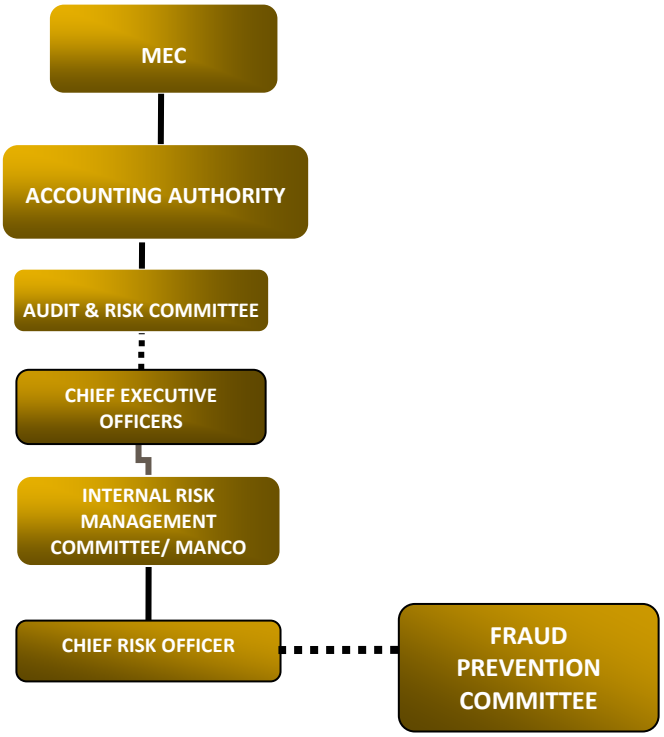
4.1. Provincial Risk Management Oversight structure



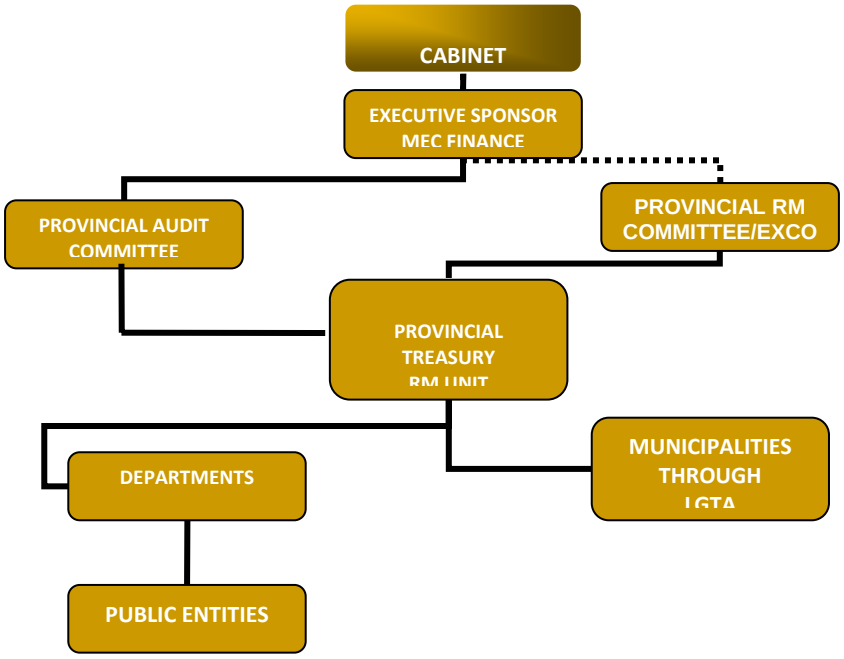
4.2 Departmental Risk Management Structure



4.3 Public Entities Risk Management Structures



4.4. Provincial Risk Reporting



5 Roles, responsibilities and governance

- The Accounting Officer/Accounting Authority of each institution is ultimately responsible for ERM and should assume overall ownership.
- All employees, managers, directors and members of Manco in KZNPG have some responsibility for ERM.
- The other managers support the risk management philosophy, promote compliance with the risk appetite and manage risks within their spheres of responsibility consistent with risk tolerances.
- Other personnel are responsible for executing ERM in accordance with established directives and protocols.
- A number of external parties often provide information useful in effecting ERM, but they are not responsible for the effectiveness of KZNPG's ERM processes and activities.

5.1 Members of the Executive Committee (MECs)

The MECs are collectively accountable to parliament in terms of the achievement of the goals and objectives of the province, and individually accountable for their respective institutions. As risk management is an important tool to support the achievement of this goal, it is important that the MECs should provide leadership to governance and risk management.

High level responsibilities of the MECs for their respective institutions for risk management include:

- Providing ***oversight and direction*** to the institution on the risk management related strategy and policies;
- Having knowledge of the extent to which the institution and management has established effective risk management in their respective institutions and ***assign responsibility and authority***;
- Awareness of and concurring with the institution's ***risk appetite and tolerance levels;***
- Reviewing the institution's ***portfolio view of risks*** and considering it against the risk tolerance;

- ***Influencing*** how ***strategy and objectives*** are established, institutional activities are structured, and risks are identified, assessed and acted upon;
- Requiring that management should have an established set of ***values by which every employee should abide by;***
- Insist on the ***achievement of objectives***, effective performance management, accountability and value for money.
- Consideration of
    - The design and functioning of ***control activities***, information and communication systems, and monitoring activities;
    - The quality and frequency of ***reporting;***
    - The ***way the institution is managed*** including the type of risks accepted;
    - The appropriateness of the **reporting lines**.

5.2 MEC Finance

The MEC Finance is the executive sponsor for the risk management process in the Province. This is an additional responsibility to the role the MEC is expected to take for Provincial Treasury as the institution for which he/she has executive accountability. The key responsibilities are:

- Ensuring that a ***risk management framework*** has been developed that is accepted by the Provincial Parliament and conforms to the National Treasury risk management framework.
- Ensuring that the ***risk management framework is effectively applied*** in the province and that Provincial Treasury has the capacity to facilitate its application.
- Providing the ***authority for Provincial Treasury*** to facilitate the application of the framework throughout the province.
- ***Periodic reporting to Cabinet*** on the effectiveness of the risk management framework in practice.
- Facilitating the ***annual reporting*** of the institutional risk profiles to Cabinet.
- Coordinating and presenting the ***Provincial consolidated risk profile*** to Cabinet and Parliament.
- Considering the reports from the ***Provincial Audit Committee***.

5.3 Heads of institutions (Accounting Officers / Accounting Authorities)

Each AO/AA is responsible for:

- the ***identification of key risks*** facing their respective institution;
- the total process of risk management, which includes a related system of internal control;
- for forming its own opinion on the effectiveness of the process;
- providing ***monitoring, guidance and direction*** in respect of ERM;
- ascertaining the status of ERM within their respective institution, by discussion with senior management and providing ***oversight*** with regard to ERM by:

    - Knowing the extent to which management has established effective ERM;
    - Being aware of and concurring with the set risk appetite;
    - Reviewing KZNPG and the institution's portfolios view of risk and considering it against it respective risk appetite; and
    - Considering the most significant risks and whether management is responding appropriately

- Identifying and ***fully appreciating the risk issues and key risk indicators*** affecting the ability of KZNPG and the institution to achieve its strategic purpose and objectives;
- ensuring that ***appropriate systems are implemented to manage the identified risks***, by measuring the risks in terms of impact and probability, together with proactively managing the mitigating actions to ensure that KZNPG and the institutions assets and reputation are suitably protected;
- ensuring that KZNPG's and the institutions ERM mechanisms provide it with an ***assessment of the most significant risks*** relative to strategy and objectives;

- considering input from the internal auditors, external auditors, auditor general and subject matter advisors regarding ERM;
- utilizing resources as needed to conduct special investigations and having open and unrestricted communications with internal auditors, external auditors, the auditor general and legal council;
- for ***disclosures in the annual report*** regarding ERM;

Provide stakeholder's with assurance that key risks are properly identified, assessed, mitigated and monitored through receiving credible and accurate information regarding the risk management processes. The reports must provide an evaluation of the performance of risk management and internal control;

5.4 Provincial Risk Management Committee (HODs)

Provincial Risk Management Committee must ensure that all Departments have complied with their risk management responsibilities. In addition they are responsible for ensuring the aggregate response to risk for the province meets the requirements as set out for the Accounting Officers.
Provincial Risk Management Committee must ensure that the various processes of Enterprise Risk Management cover the entire spectrum of risks faced by KZNPG.
Management is accountable to the **Provincial Risk Management Committee (HODs)**
for ***designing, implementing and monitoring*** the process of risk management and ***integrating it into the day-to-day activities*** of KZNPG.

More specifically management is responsible for:

- designing an ERM programme in conjunction with the Chief Risk Officer;
- deciding on the manner in which risk mitigation will be embedded into management processes;
- ***inculcating a culture of risk management*** in the KZNPG ;
- providing risk registers and risk management reports to the Chief Risk Officer pertaining to risk and control;
- identifying positive aspects of risk that could evolve into potential opportunities for KZNPG by viewing risk as an opportunity by applying the risk/reward principle in all decisions impacting upon KZNPG;
- assigning a manager to every key risk for appropriate mitigating action and to determining an action date;
- utilising available resources to compile, develop and implement plans, procedures and controls within the framework of the KZNPG 's Enterprise Risk Management Policy to effectively manage the risks within KZNPG;
- ensuring that adequate and cost effective risk management structures are in place;
- identifying, evaluating and measuring risks and where possible quantifying and linking each identified risk to key risk indicators;
- developing and implementing risk management plans including:
- actions to optimise risk/ reward profile, maximise reward with risk contained within the approved risk appetite and tolerance limits;
- implementation of cost effective preventative and contingent control measures and
- implementation of procedures to ensure adherence to legal and regulatory requirements.
- monitoring of the ERM processes on both a detailed and macro basis by evaluating changes, or potential changes to risk profiles;
- implementing and maintaining adequate internal controls and monitoring the continued effectiveness thereof;
- implementing those measures as recommended by the internal auditors, external auditors and other assurance providers which, in their opinion, will enhance controls at a reasonable cost;
- reporting to the Audit Committee on the risk process and resultant risk/ reward profiles;
- defining the roles, responsibilities and accountabilities at senior management level.

5.5 KwaZulu Natal Provincial Treasury

Treasury's responsibilities include ***ensuring that all components of ERM are in place at all institutions.*** Treasury generally fulfils this duty by:

- providing leadership and direction to the Accounting Officers. Together with the senior managers, Treasury shapes the values, principles and major operating policies that form the foundation of KZNPG's ERM processes. Key senior managers in the various institutions set strategic objectives, strategy and related high-level objectives.
- setting broad-based policies and developing KZNPG's ERM philosophy, risk appetite and culture. MANCO takes actions concerning KZNPG's organisational structure, content and communication of key policies and the type of planning and reporting systems that KZNPG will use.
- meeting periodically with senior managers responsible for major organisational units and functional areas to review their responsibilities, including how they manage risk.
- gaining knowledge of risks inherent in institution's operations, risk responses and control improvements required and the status of efforts underway. To discharge this responsibility, Treasury must clearly define the information it requires from the various institutions.
- providing technical advice to the accounting officer/accounting authority, senior management on risk management strategies.
- reviewing and facilitating risk management training conducted at appropriate levels within the institutions to inculcate a risk management culture;
- consolidating the provincial risk profile and escalate critical risks to the Provincial Audit Committee, Provincial Risk Committee and Cabinet.
- summarising cross cutting risks for consideration by the Provincial Risk Committee and ensuring that uniform risk mitigation strategies are implemented.
- analysing risk reports from various institutions and provide technical advice on the risk mitigation strategies.
- communicate transversal risks for inclusion in the assurance providers' operational plans
- reporting of risk with particular emphasis on significant risks or exposures and the appropriateness of the steps management has taken to reduce the risk to an acceptable level
- reviewing reports of significant incidents and major frauds (both potential and actual) including the evaluation of the effectiveness of the response in investigating any loss and preventing future occurrences
- Assist institutions in facilitating risk assessments and developing risk mitigation strategies

Treasury has been appointed to provide direction, guidance, support, build capacity and to monitor institutions in effecting ERM.

5.6 Audit Committee

The Audit Committee oversees the roles and responsibilities of the Internal Audit team, specifically relating to providing assurance in respect of ERM.
The Audit Committee will be responsible for ***addressing the governance requirements*** of ERM and ***monitoring the KZNPG institution's performance with ERM activities***. The Audit Committee will meet quarterly and has a defined mandate and terms of reference, which covers the following aspects:

- constitution;
- membership;
- authority;
- terms of reference; and
- meetings.

The Audit Committee further:

- Reviews written reports furnished by the **Provincial Risk Management Committee (HODs)/** detailing the adequacy and overall effectiveness of the institutional Risk Committee's function and its implementation by management.
- Review risk philosophy, strategy, policies and processes recommended by the **Provincial Risk Management Committee (HODs)** and consider reports by the **Provincial Risk Management Committee (HODs)** on implementation and communication to ensure incorporation into the culture of the institutions.
- Ensure that risk definitions and contributing factors, together with risk policies, are formally reviewed on an annual basis.
- Review the acceptability of the risk profile in conjunction with the overall risk appetite of the institutions, taking into account all risk mitigation factors, including, but not limited to, internal controls, business continuity and disaster recovery planning, etc.
- Ensure compliance with the Provincial risk policies and framework.
- Oversee the Fraud Prevention Committees of the institutions to ensure they are operating effectively and to receive periodic reports (quarterly) on their respective activities.

5.7 Focused/Internal Risk Management Committee/ MANCO

The Focused/Internal Risk Management Committees/ MANCO assume the following responsibilities:

- Review and assess the integrity of the risk control systems and ensure that the risk policies and strategies are effectively managed.
- Set out the nature, role, responsibility and authority of the risk management / risk officer function within the institution and outline the scope of risk management work.
- Monitor the management of significant risks to the institution, including emerging and prospective impacts.
- Review any legal matters, together with the legal advisor, that could have a significant impact on the institution.
- Review management and internal audit reports detailing the adequacy and overall effectiveness of the institution's risk management function and its implementation by management, and reports on internal control and any recommendations, and confirm that appropriate action has been taken.
- Review risk identification and assessment methodologies.
- Review and approve the risk tolerance for the institution.
- Review and approve any risk disclosures in the Annual Financial Statements.
- Monitor the reporting of risk by management with particular emphasis on significant risks or exposures and the appropriateness of the steps management has taken to reduce the risk to an acceptable level.
- Monitor progress on action plans developed as part of the risk management process.
- Review reports of significant incidents and major frauds (both potential and actual) including the evaluation of the effectiveness of the response in investigating any loss and preventing future occurrences:
- Significant incidents are defined as any event which results in, or has the potential to result in serious personal injury (to the public, staff or third parties) or serious physical damage to property, plant, equipment, fixtures or stock.
- Significant frauds are defined as any fraud which results in, or has the potential to result in the loss of assets with a value exceeding 10% of the institution' budget allocation.
- Providing feedback to the audit committee and Provincial Treasury on the effectiveness of risk management:

5.8 Fraud Prevention Committee

All institutions are obliged to appoint a Fraud Prevention Committee, to consist of members of staff drawn from a variety of levels of the institution. The Fraud Prevention Committee must ensure the implementation of the fraud and misconduct strategy, creating fraud awareness amongst all

stakeholders and accepting responsibility for considering any reports of fraud or misconduct and for taking appropriate action in consultation with the Head of institution.

The Head of institution establishes the right tone for the prevention and management of fraud and misconduct in the institution. This is achieved through developing and publishing a fraud and misconduct risk management policy.

The Fraud Prevention Committee, in fulfilling its role, is responsible for ensuring that the following is achieved.

- Monitoring of the ***application of the policy*** and ensuring adequate supervision and dynamism of the controls and procedures.
- The ***planned and required activities are undertaken*** such as the policy inclusion in the letter of appointment for staff, communication and training campaigns.
- An appropriate ***fraud risk assessment*** is completed.
- The reports of fraud and misconduct are ***effectively handled***.
- Consistent and ***appropriate action*** is taken on known incidents of fraud and misconduct.
- ***Quarterly reports*** to the Provincial Audit Committee/Audit Committee that summarises the institution's fraud prevention, detection and action for the period.

5.9 Business Unit/Programme Heads

Senior managers in charge of institutional business units/programmes have overall responsibility for managing risks related to their unit's objectives and are responsible for:

- identifying, assessing and responding to risk relative to meeting the unit's objectives;
- ensuring that the processes utilised are in compliance with KZNPG's Enterprise Risk Management policies and that their activities are within the established risk tolerance limits;
- reporting on progress and issues to the institutional Chief Risk Officer and to the Internal Risk Management Committee;
- complying with Enterprise Risk Management policies and developing techniques tailored to the unit's activities;
- applying ERM techniques and methodologies to ensure risks are appropriately identified, assessed, responded to, reported on and monitored;
- ensuring risks are managed on a daily basis; and
- providing leadership with complete and accurate reports regarding the nature and extent of risks in the unit's activities.

Institutions may have technical committees in place that deal with specialised areas of risk such as environmental management, quality management and technical compliance matters. These are expected to be continued as deemed appropriate for the risk profile of the institution.

5.10 Chief Risk Officer (CRO)

The Chief Risk Officer assisted by the institutional Risk Officers:

- undertakes a Gap Analysis of the institution's ERM process at regular intervals;
- performs reviews of the risk management process to improve the existing process;
- facilitates annual risk management assessments and risk assessments for all major changes and incidents, such as accidents, purchases of capital equipment, restructuring of operational processes etc.;
- develops systems to facilitate risk monitoring and risk improvement;
- ensures that all risk categories are included in the assessment;
- ensures that key risk indicators are included in the risk register;
- aligns the risk identification process with KZNPG's targets and objectives;
- agrees on a system of risk quantification;
- identifies relevant legal and regulatory compliance requirements;
- compiles a consolidated risk register on an annual basis;

- costs and quantifies actual non-compliance incidences and losses incurred and formally reports thereon;
- formally reviews the occupational health, safety and environmental policies and practices;
- consolidates all information pertaining to all risk related functions, processes and activities;
- reviews the Business Continuity Management Plans;
- liaises closely with the Internal Audit to develop a risk based audit plan and management assurance plans,
- benchmarks the performance of the risk management process to the risk management processes adopted by other entities both within South Africa and abroad;
- assists in compiling risk registers for all functional areas at strategic, tactical and operational levels;
- communicates the risk strategy to all management levels and to employees;
- ensures that the necessary risk management documentation is developed in respect of the risk management process;
- communicates with the Provincial Treasury, Audit Committee and the Risk Committee regarding the status of ERM;
- regularly visits functional areas and meets with senior managers to promote embedding risk management into the culture and daily activities of KZNPG;
- works with institutional leaders to ensure institutional plans and budgets include risk identification and management;

5.11 Internal Audit

The role of Internal Audit in governance is defined by the South African Institute of Internal Auditors as follows: "To support the Board and Management in identifying and managing risks and thereby enabling them to manage the organisation effectively". This is achieved by:

- enhancing their understanding of risk management and the underlying concepts;
- assisting them to implement an effective risk management process, and
- providing objective feedback on the quality of organisational controls and performance."

Internal Audit is responsible for:

- providing assurance that management processes are adequate to identify and monitor significant risks;
- using the outputs of risk assessments to direct internal audit plans;
- providing ongoing evaluation of the risk management processes;
- providing objective confirmations that the Provincial Risk Management Committee and Audit Committee receive the right quality of assurance and reliable information from management regarding risk;
- providing assurance regarding the effectives and efficiency of risk responses and related control activities and
- further providing assurance as to the completeness and accuracy of ERM reporting.

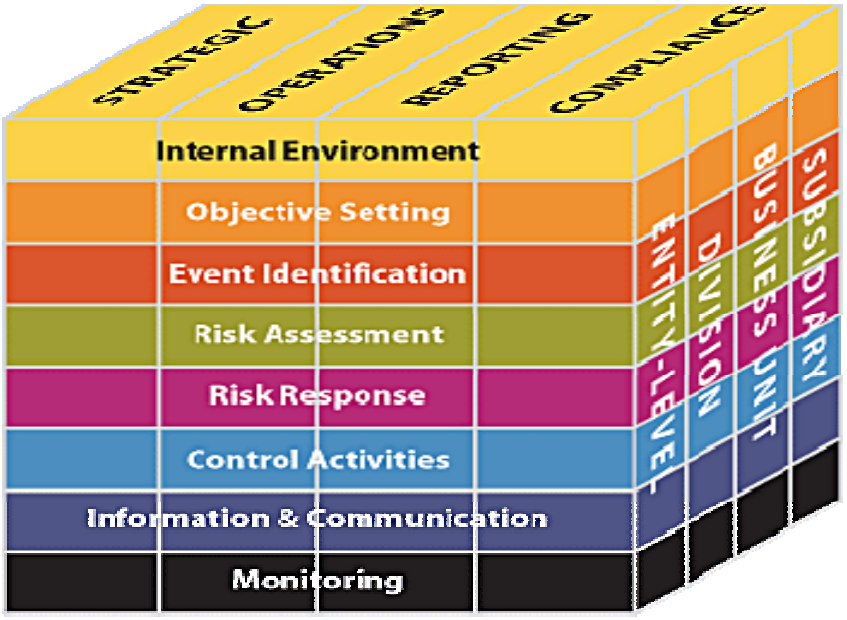
5.12 Provincial Chief Risk Officers' Forum

The risk Management Forum is responsible for

- Promotion of sound enterprise wide risk management practices in the province through knowledge sharing, and development of enterprise wide risk management tools and guidelines.
- Identification and development of strategies to deal with risk cutting across the province

6 Enterprise Risk Management (ERM) Approach

The provincial ERM approach is based on the COSO Risk Management Framework depicted in the diagram below.

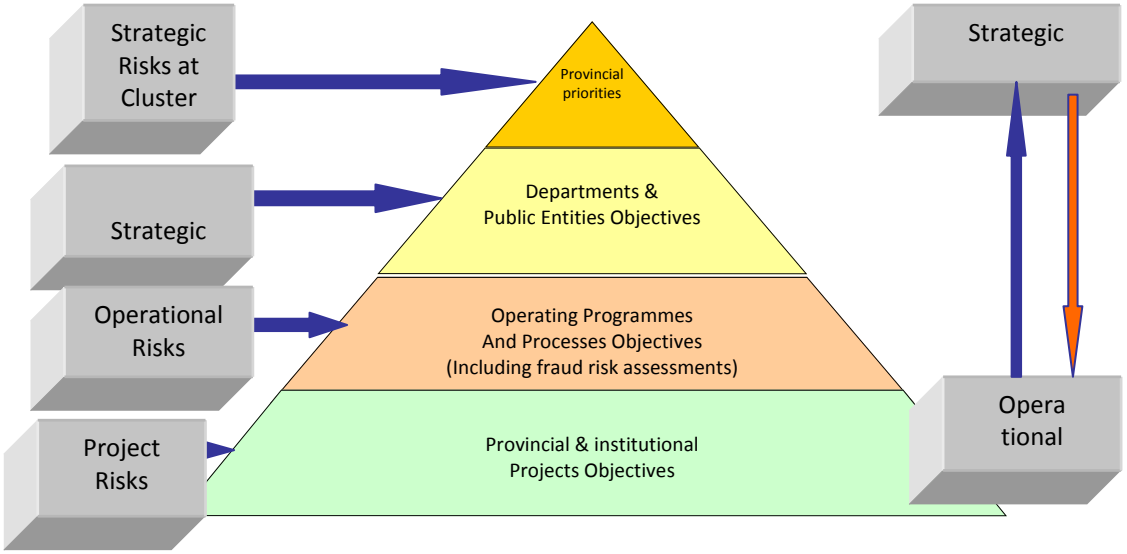


The implementation of enterprise-wide risk management is guided by the methodology outlined in this document. The methodology allows for a consistent approach to be applied throughout KZNPG and facilitates the interaction, on risk management matters, between the various institutions and functional areas within the institutions.

6.1 Risk Profiles

Risk profiles plans shall be developed and reviewed on an annual basis. Three levels of risk profiles need to be developed and maintained at the institutions. These are:

- Strategic,
- Operational and
- Project.



The development and maintenance of the profiles should be a continuous process but management should formally assess and agree the profiles annually. This is usually achieved through facilitated workshops where management collectively agrees on the risk identification, assessment and actions.

Strategic level

- top-down risk assessment at strategic level as part of corporate development and strategy setting;
- assess the internal control environment and verify on a risk based approach the compliance with internal policies, procedures and guidelines;
- facilitate risk owners in ensuring effectiveness of current management controls and strategies; and
- align risk management activities at strategic level within the different units of the institution and day-to-day business

Operational level

- assess the internal control environment and verify on a risk based approach the compliance with internal policies, procedures and guidelines;
- review the adequacy, effectiveness and adherence to existing policies, procedures and guidelines;
- conduct operational risk assessments focusing on identifying key (inherent) risk;
- financial risk control, focusing on assessment of key financial reporting controls to identify any gaps and to facilitate and monitor follow up actions;
- identify where government institutions could benefit from supporting guidance on policies, procedures and guidelines; and facilitate sharing of the best practices.

6.2 Fraud Risk Assessment

A key element of the fraud and misconduct policy is the development of a fraud prevention plan. This plan is underpinned by a fraud risk assessment. The fraud risk assessment is completed according to the same process as the other risk assessments. However, an institution may wish to integrate the fraud risk evaluation together with the other risk profiles or to separately complete a fraud risk assessment. The fraud risk information will need to be extracted in order to develop and maintain the fraud prevention plan.

6.3 Developing risk profiles

6.3.1 Risk Identification

Risks emanate from internal or external sources which affects implementation of strategy or achievement of objectives.

As part of risk identification, management recognises that uncertainties exist, but does not know when a risk may occur, or its outcome should it occur. Management initially considers a range of potential risks − affected by both internal and external factors − without necessarily focusing on whether the potential impact is positive or negative.

Potential risks range from the obvious to the obscure, and the potential effects from the significant to the insignificant. But even potential risks with relatively remote possibility of occurrence should not be ignored at the risk identification stage if the potential impact on achieving an important objective is great.

External Factors	**Economic and Business**	Related risks might include emerging or movements in the international, national, provincial markets and globalisations
	Natural environment	Risks might include such natural disasters as flood, fire or earthquake, and sustainable development.
	Political	Risks might include newly elected government officials, political agendas and new legislation and regulations. The influence of international governments and other governing bodies
	Social	Risks might include changing demographics, shifting of family structures, work/life priorities, social trends and the level of citizen engagement
	Technological	Risks might include evolving electronic commerce, expanded availability of data and reductions in infrastructure costs.

Internal Factors	**Infrastructure**	Risks might include unexpected repair costs, or equipment incapable of supporting production demand.
	Human resource	Risks might include increase in number of on-the-job accidents, increased human error or propensity for fraudulent behaviour.
	Process	Risks might include product quality deficiencies, unexpected downtime, or service delays.
	Technology	Risks might include inability to maintain adequate uptime, handle increased volumes, deliver requisite data integrity, or incorporate needed system modifications.
	Governance and accountability frameworks	Values and ethics, transparency, Policies, procedures and processes

6.3.2 Risk Categories

Potential risks are grouped into categories. By aggregating risks horizontally across an organisation and vertically within operating units, management develops an understanding of the interrelationships between risks, gaining enhanced information as a basis for risk assessment.

RISK CATEGORIES	DEFINITION OF RISK CATEGORIES
1. Strategic and service delivery risks	Risks arising from policy decisions or major decisions affecting provincial and organisational priorities; Risks arising from senior-level decisions on priorities. Strategy and Business Intelligence failures. Risks that have an effect of hindering service delivery due to inefficient, ineffective and uneconomical use of resources
2. Intergovernmental and Interdepartmental Co-ordination Risks	Risks emanating from the relationship between the spheres of government in National, Provincial and Local levels as well as between provincial departmental, and are having the effect of impeding the attaining of objectives
3. Governance, Compliance/ Regulatory and Reputational Risks	Values and ethics, transparency, policies, procedures and processes as well organisational structures. Compliance with legal requirements such as legislation, regulations, standards, codes of conduct/practice, contractual requirements and internal policies and procedures. This category also extends to compliance with additional 'rules' such as policies, procedures or expectations, which may be set by contracts or

	customers. The reputation risks exposures due to the conduct of the entity as a whole, the viability of product or service, or the conduct of employees or other individuals associated with the business.
4. Political Risks	Risks relating to newly elected government officials, political agendas and new legislation and regulations or amendments thereof. The influence of international governments and other governing bodies on the institutional strategy.
5. Economic Risks	Related risks relating emerging or movements in the international, national, provincial markets and globalisations Factors to consider include: • Inflation; • Foreign exchange fluctuations; and • Interest rates • Pricing
6. Environmental Risks	Risks relating to natural disasters as flood, fire or earthquake, and sustainable development.
7. Social Risks	Risks relating to poverty alleviation, changing demographics, shifting of family structures, work/life priorities, social trends and the level of citizen engagement
8.Infrastructure Risks	Risks relating to infrastructure e.g. roads, buildings, etc.
9. Financial Risks	Risks arising from spending on capital projects Risks from failed resource bids and insufficient resources. Risks encompassing the entire scope of general financial management. Potential factors to consider include: • Cash flow adequacy and management thereof; • Financial losses; • Wasteful expenditure; • Budget allocations; • Financial statement integrity; • Revenue collection; and Increasing operational expenditure.
10. Health and Safety/Security Risks	Risks arising from outbreak of diseases and pandemic. Risks that are associated with the safety and security of the communities as well as the execution of institutional mandate Security of networks , systems and information
11.Shareholder Risks	Risks associated with shareholding interests that the institution has with its stakeholders. Risks that could have a systemic impact on the sector within the public entity operates and or on the economy and service delivery.
12.Human Resources	Risks associated with staff capacity in relation • Integrity and honesty; • Recruitment; • Skills and competence; • Employee wellness; • Employee relations; • Retention; Non-familiarity of staff with the set guidelines and procedures
13.Technological and System Risks	Risks associated with evolving electronic commerce, expanded availability of data and reductions in infrastructure costs. Failure of application system to meet user requirements. Absence of in-built control measures in the application system.

14. Process/operational	Ineffective and inefficient processes. Inadequate controls in the operational processes.
15. Project risks	Risks associated with not meeting project scope, costs, duration and deliverables
16. Fraud and Corruption Risks	These risks relate to illegal or improper acts by employees resulting in a loss of the institution's assets or resources.
17. Cultural	Risks relating to an institution's overall culture and control environment. The various factors related to organisational culture include: • Communication channels and the effectiveness; • Cultural integration; • Entrenchment of ethics and values; • Goal alignment; and • Management style.
18. Disaster Recovery/Business Continuity	Risks related to an institution's preparedness or absence thereto to disasters that could impact the normal functioning of the institution e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include: • Disaster management procedures; and • Contingency planning.

6.3.3 Risk Assessment

Identified risks are analyzed in order to form a basis for determining how they should be managed. Risks are associated with related objectives that may be affected. Risks are assessed on both an inherent and a residual basis, and the assessment considers both risk likelihood and impact. A range of possible results may be associated with a potential event, and management needs to consider them together.

Risk assessment allows consideration of the extent to which potential events might have an impact on achievement of objectives. It is about analyzing and assigning ratings to the potential likelihood (frequency or probability) of an event occurring, and the potential consequence (impact or magnitude of effect), if the event does occur. The level of risk is determined by considering the combined effect of the likelihood and impact.

External and internal factors influence which events may occur and to what extent the events will affect the achievement of objectives. In risk assessment, management considers the mix of potential future events relevant to the organisation and its activities. There are three important principles for assessing risk:

- ensure that there is a clearly structured process in place;
- record the assessment of risk in a way which facilitates monitoring and the identification of risk priorities; and
- be clear about the difference between, inherent and residual risk.

Inherent and Residual Risk

Inherent risk is the risk in the absence of any actions management might take or has taken to reduce either the risk's likelihood or impact. Should there be existing controls, these must not be taken into account when estimating the inherent risk value. Inherent risks are rated, assuming that there are no controls in place to mitigate the risk.

The existence of controls, depending on how adequate and effective they are, may influence the likelihood or impact of the risk. This means that risk likelihood or impact may be reduced. Residual

risk is the risk that remains after taking into account the effect of any existing controls. Example: The risk of theft of a car may be rated high. But having an immobilizer may reduce the likelihood of the risk occurring. The risk of theft may therefore be reduced.

In assessing risk, management considers the impact of expected and unexpected potential events. Many events are routine and recurring, and they are already addressed in management programs and operating budgets. Others are unexpected, often having a low likelihood of occurrence but may have a significant potential impact. Unexpected events usually are responded to separately. However, uncertainty exists with respect to both expected and unexpected potential events, and each has the potential to affect strategy implementation and achievement of objectives. Accordingly, management assesses the risk of all potential events that are likely to have a significant impact on the achievement of objectives.

Risk assessment is applied first to inherent risks. Once risk controls and responses have been identified and/or developed, the residual risk is then determined.

Likelihood and Impact

Likelihood represents the probability that a given event or risk will occur while impact represents the effect of the risk should it occur.

Control

A control could be policies, procedures, laws, regulations or any action that would reduce the likelihood or impact of a risk. For example: have an insurance policy or an alarm system will reduce the likelihood or impact of the risk of theft. Therefore the insurance policy and alarm system are referred to as controls.

There are different categories of controls and these are explained later in this document.

Step 1: Estimating likelihood and impact

Risk assessment is tricky because the process involves subjective thinking. The identification of risks is generally based on an individual's experience and knowledge of the business and operations. Since experience and knowledge are unique to each individual, it is important to get a wide range of individuals on the risk management team. Each identified risk must be rated in terms of likelihood and impact.

Some types of risk lend themselves to a numerical diagnosis – particularly financial risk. For other risks - for example reputational risk - a much more subjective view is all that is possible. In this sense risk assessment is more of an art than a science. The assessment should draw as much as possible on unbiased independent evidence; consider the perspectives of the whole range of stakeholders affected by the risk.

Likelihood measures the probability that the identified risk / threat will occur within a specified period of time (between 1 and 3 years) on the basis that management have no specific / focused controls in place to address the risk / threat. The likelihood of occurrence must be assessed for every identified risk. Estimates of risk likelihood often are determined using data from past observable events, which may provide a more objective basis than entirely subjective estimates. Internally generated data based on the institution’s own experience may reflect less subjective personal bias and provide better results than data from external sources.

There are also more scientific and objective methods of determining the likelihood and impact of a risk.
The following rating scales have been established for KZNPG.

Measures of likelihood of occurrence

Table of likelihood parameters

Likelihood category	Category definition	Factor
Certain	The risk is already occurring, or is likely to occur more than once within the next 12 months	100
Likely	The risk could easily occur, and is likely to occur at least once within the next 12 months	0.80
Moderate	There is an above average chance that the risk will occur at least once in the next three years	0.60
Unlikely	The risk occurs infrequently and is unlikely to occur within the next three years	0.40
Rare	The risk is conceivable but is only likely to occur in extreme circumstances	0.20

Measures of Impact

The following table is to be used to assist management in quantifying the potential impact that a risk exposure may have on the institution.

Severity ranking	Continuity of service delivery	Safety & Environmental	Technical complexity	Financial	Achievement of objectives	Factor
Critical	Risk event will result in widespread and lengthy reduction in continuity of service delivery to stakeholders of greater than 48 hours	Major environmental damage Serious injury (permanent disability) or death of personnel or members of the public Major negative media coverage	Use of unproven technology for critical system / project components High level of technical interdependencies between system / project components	Significant cost overruns of >20% over budget (higher of income or expenditure budget)	Negative outcomes or missed opportunities that are of critical importance to the achievement of objectives	100
Major	Reduction in supply or disruption for a period ranging between 24 & 48 hours over a significant area	Significant injury of personnel or public Significant environmental damage Significant negative media coverage	Use of new technology not previously utilised by the institution for critical systems / project components	Major cost overruns of between 10 % & 20 % over budget (higher of income or expenditure budget)	Negative outcomes or missed opportunities that are likely to have a relatively substantial impact on the ability to meet objectives	60
Moderate	Reduction in supply or disruption for a period between 8 & 47 hours over a regional area	Lower level environmental, safety or health impacts Negative media coverage	Use of unproven or emerging technology for critical systems / project components	Moderate impact on budget (higher of income or expenditure budget)	Negative outcomes or missed opportunities that are likely to have a relatively moderate impact on the ability to meet objectives	35
Minor	Brief local inconvenience (work around possibly) Loss of an asset with minor impact on operations	Little environmental, safety or health impacts Limited negative media coverage	Use of unproven or emerging technology for systems / project components	Minor impact on budget (higher of income or expenditure budget)	Negative outcomes or missed opportunities that are likely to have a relatively low impact on the ability to meet objectives	20

Severity ranking	Continuity of service delivery	Safety & Environmental	Technical complexity	Financial	Achievement of objectives	Factor
Insignifi cant	No impact on business or core systems	No environmental, safety or health impacts and / or negative media coverage	Use of unproven or emerging technology for non-critical systems / project components	Insignificant financial loss	Negative outcomes or missed opportunities that are likely to have a relatively negligible impact on the ability to meet objectives	10

Step 2: Risk Matrix

Inherent risk exposure is the risk to the institution in the absence of any actions management might take to alter either the risk's impact or likelihood. Inherent risk is the product of the impact of a risk and the probability of that risk occurring before the implementation of any direct controls. The score for inherent risk assists management and internal audit alike to establish relativity between all the risks / threats identified.

The ranking of risks in terms of inherent risk provides management with some perspective of priorities. This should assist in the allocation of capital and resources in the operations. Although the scales of quantification will produce an automated ranking of risks, management may choose to raise the profile of certain risks for other reasons.

The table below is to be used to assist management in quantifying the inherent risk of a particular risk (i.e. pre controls)

Inherent risk exposure	Factor
Critical	**> 60**
Major	**> 35 ≤ 60**
Moderate	**> 20 ≤ 35**
Minor	**> 10 ≤ 20**
Insignificant	**≤ 10**

For example: A likelihood of 0.20 and impact of 100 would result in a risk index of 20 and this correlates to a minor risk. In this way each combination of likelihood and impact can be mapped to a risk index. The risk index indicates the severity of the risk.

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

Risk appetite

Risk appetite is the amount of risk that is accepted in pursuit of achieving objectives. KZNPG has adopted a quantitative approach in determining risk appetite, reflecting and balancing goals for growth, return and risk. Risk appetite is directly related to strategy. It is considered in strategy setting, where the desired return from a strategy should be aligned with the risk appetite. Different strategies will expose different risks. Enterprise risk management, applied in strategy setting, helps management select a strategy consistent with risk appetite.

Defining a risk as acceptable does not imply that the risk is insignificant. The assessment should take into account of the degree of control over each risk; the cost impact, benefits and opportunities presented by the risk and the importance of the policy, project, function or activity.

Reasons for classifying a risk to be acceptable could include:

- the likelihood and impact of the risk could be so low that specific treatment is inappropriate
- the risk being such that no treatment is available
- the cost of the treatment being so excessive compared to the benefit that acceptance is the only option.

Step 4. Considering the Risk Response

Management selects an approach or set of actions to align assessed risks with risk appetite, in the context of the strategy and objectives. Personnel identify and evaluate possible responses to risks, including avoiding, accepting, reducing and sharing risk.

Risk responses fall within the following categories:

- **Avoidance-** Action is taken to exit the activities giving rise to risk. Risk avoidance may involve exiting a project, avoiding high risk investments, or not accepting a pioneering technical solution.

- **Reduction –** Action is taken to reduce the risk likelihood or impact, or both. This may involve any of a myriad of everyday business decisions. e.g. buying a generator to ensure electricity supply to a hospital.

- **Sharing –** Action is taken to reduce risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Common risk-sharing techniques include purchasing insurance products, pooling risks, engaging in hedging transactions, or outsourcing an activity, public private partnership. e.g. taking out forward cover for foreign currency purchases.

- **Acceptance –** No action is taken to reduce the likelihood or impact of a risk. E.g. not to factor earthquakes greater than 5 on the Richter Scale to bridge construction due to the rare/remote probability of any seismic activity in the geographical area.

The avoidance response suggests that either the cost of other responses would exceed the desired benefit, or no response option was identified that would reduce the impact and likelihood to an acceptable level. Reduction and sharing responses reduce residual risk to a level that is line within the risk appetites, while an acceptance response suggests that inherent risk is already in line with risk appetites.

For many risks, appropriate response options are obvious and well accepted. For instance, a response option appropriate for the loss of computing availability is the development of a business continuity plan. For other risks, available options may not be readily apparent, requiring more extensive identification activities. For instance, response options relevant to mitigating the effect of global warming may require research on weather patterns and water availability.

In determining the appropriate responses, management should consider such things as:

- Evaluating the effectiveness of existing measures on reducing the risk to an acceptable level.
- Considering if there are other control measures that could be used to mitigate the risk more effectively. This is where benchmarks and leading practices are important. In the public sector there are many opportunities to benchmark and consider leading practices as applied in other government institutions, provincial departments or local authorities.
- Assessing the costs versus benefits of potential risk responses.

Step 5. Evaluating Effect of Response on Residual and Desired Residual Risk

Each risk is rated according to the inherent risk rating criteria. The effectiveness of the existing risk responses is assessed for these risks. This is done by rating the control effectiveness. A decision is

then needed to determine if the risk is managed to the desired levels of risk appetite. This is an assessment of the current residual risk.

Controls are the management activities / policies / procedures / processes / functions / departments / physical controls that the institution and Management have put in place, and rely upon, to manage the strategic and significant risks. These actions may reduce the likelihood of occurrence of a potential risk, the impact of such a risk, or both. When selecting control activities management needs to consider how control activities are related to one another.

Management then needs to assess the control effectiveness based on their understanding of the control environment currently in place. At this stage of the process, the controls are un-audited, and rated according to management's interpretation of control effectiveness.

The table below is to be used to assist management in quantifying the perceived and desired control effectiveness to mitigate or reduce the impact of specific risks.

The desired effectiveness of risk responses is determined where the desired risk exposure is not achieved with current risk responses. The desired effectiveness is measured on the same scale as the rating for current control effectiveness. This is the assessment of desired residual risk for each risk – sometimes referred to as risk tolerance. The sum of risk tolerances should measure risk appetite.

Residual risk is calculated by multiplying the inherent risk score by the rating scale for control effectiveness.

Effectiveness category	**Category definition**	**% of Risk Controlled**
Very good	Risk exposure is effectively controlled and managed	71 - 90
Good	Majority of risk exposure is effectively controlled and managed	46 - 70
Satisfactory	There is room for some improvement	21 - 45
Weak	Some of the risk exposure appears to be controlled, but there are major deficiencies	11 - 20
Unsatisfactory	Control measures are ineffective	0 -10

Some level of residual risk will always exist, not only because resources are limited, but also because of inherent future uncertainty and limitations inherent in all activities.

The difference between assessed residual risk and desired residual risk is the residual risk gap. This represents the opportunity to improve risk management and the achievement of objectives. The bigger the residual risk gap, the higher the action priority.

The ranking of risks in terms of residual risk gap provides management with some perspective of priorities, and should assist in the allocation of capital and resources in the institution.

The table below is to be used to assist management in quantifying the residual risk gap of a particular risk.

Residual risk exposure	Risk acceptability	Proposed actions	Factor	Monetary Quantification
Critical	Unacceptable	Take action to reduce risk with highest priority, accounting officer/chief executive officer and executive authority/accounting authority attention.	**≥ 25**	≥ 5% of Budget or Income
High	Unacceptable	Take action to reduce risk with highest priority, accounting officer/chief executive officer and executive authority/accounting authority attention.	**≥ 15 < 25**	≥4% <5% of Budget or Income
Medium	Unacceptable	Take action to reduce risk, inform senior management.	**≥ 8 < 15**	≥3% <4% of Budget or Income
Low	Acceptable	No risk reduction - control, monitor, inform management.	**≥ 3 < 8**	≥ 2.5% <3%of Budget or Income
Insignificant	Acceptable	No risk reduction - control, monitor, inform management.	**< 3**	2% of budget or income

The application of the approach has been depicted in the example and diagram below.

Inherent risk impact	Inherent risk likelihood	Inherent risk exposure	Perceived Residual risk	Desired Residual risk	Residual risk gap
Ranking with effective mitigation strategies in place (very good perceived effectiveness rating)					
100	0.80	80	0.30	0.10	16
Ranking with ineffective mitigation strategies in place (weak perceived effectiveness rating)					
100	0.80	80	0.80	0.10	56

Step 6. Identifying Actions to Mitigate Risk Exposure

The residual risk gap identifies possible improvement opportunities.

Action steps should be identified for the risks where there are residual risk gaps. The actions should specify the responsibilities and due dates. Management should track to progress and completion of the actions.

7 Reporting

Like any other process, the success of risk management depends on the availability of reliable information and effective communication at various levels. Pertinent information should be identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities.

Information is needed at all levels to identify, assess and respond to risks. The challenge for management is to process and refine large volumes of data into relevant and actionable information.

Risk information is to be maintained on a risk management database. The database will be maintained by the Risk Management Unit within Provincial Treasury and the institution Risk Managers. Line management will be responsible for ensuring that the risk information is complete, accurate and relevant. The database will allow the access to the risk officials and line management to execute the relevant functions.

The database structure is based on the Provincial and respective institution risk profiles. The minimum required profiles for each institution and at a Provincial level are:

- Strategic
- Operational (Including Fraud and Corruption)
- Project specific (where there are such projects)

Additional assessments can be maintained – for example incident tracking and compliance assessments.

For each profile the following minimum information is to be maintained on the database:

- Strategic and business objectives
- Risk category
- Risk name
- Risk description
- Risk owner
- Inherent risk rating
- Risk Indicator
- Control names for controls that mitigate the risk
- Control descriptions (including whether it is a preventative, detective or corrective control)
- Control effectiveness rating
- Residual risk ratings
- Task information where identified – details, due dates and the accountable officials.
- Key Performance Indicator

The databases will be used to extract the required reports to evidence the status of risk management in the Province and institutions.

8 Combined Assurance

Internal Audit is required by the PFMA to plan the audit coverage to address the risks identified through the risk management processes developed and maintained by the Province and institutions.

The risks identified cannot all be reviewed by Internal Audit. Some risks, for example reputation, are not able to be reviewed and others, such as technical construction, cannot reasonably be expected to be reviewed by Internal Audit.

There are several assurance functions that may exist in the Province and in an institution at any time and include:

- Internal Controls Units
- The Office of the Auditor General,
- Internal Audit,
- Consulting engineers,
- Ethics' specialists
- Compliance and Legal specialists

- Culture and climate surveys,
- Health and safety inspectors.
- Information security, and
- Quality
- Loss Control Units
- Monitoring and evaluation Units

The assurance that they provide is reported to different management structures and this may be outside the Internal Audit governance reporting structures, including the Audit Committees.

Internal Audit takes the responsibility to ensure the assurance activities are coordinated, provide optimal coverage of the risk profiles, where possible, and are reported to the appropriate management and governance forum. The Audit Committee approves the overall/combined assurance plan and extent of assurance coverage. They will also review the appropriateness of the recipients of the different assurance activities.

Each assurance provider should develop their coverage plan based on the risk profiles of the institution(s). Typically the plan should consider the risk assessment ratings. Where management has assessed that there is a high residual risk gap and has actions to address the gap, the assurance provider should consider reviewing the actions rather than confirming management's assessment. Conversely where there is a low or negligible gap the controls that have been assessed by management as mitigating the risk should be evaluated.

The results of the work performed should be used by the chief risk officer to facilitate, if necessary, a rerating of the risk and incorporating the agreed management actions into the risk management tasks. This will enable a central tracking capability for all such tasks and actions.

Where their work is in response to an incident or event, e.g. loss control, the results of the work performed should be used by the chief risk officer to facilitate, if necessary, a rerating of the risk and incorporating the agreed management actions into the risk management tasks.

9 Monitoring

If existing controls are weak and exposes the organisation's activities to risks, the management should come up with the action plans to reduce risk to an acceptable level. The management should decide on the implementation date of the agreed upon action plan and the responsibility for the implementation of action plan should be assigned to capable officials.
It is critical that management should develop key performance indicators regarding the performance of agreed upon controls. Key performance indicators will provide the feedback regarding effectiveness of controls against identified risks.

Management's performance with the processes of ERM will be measured and monitored through the following performance management activities:

- monitoring of progress made by management with the implementation of the ERM methodology;
- monitoring of key risk indicators;
- monitoring of loss and incident data;
- management's progress made with risk mitigation action plans; and
- an annual quality assurance review of ERM performance.

10 Embedding Risk Management

Value is created, preserved or eroded by management decisions ranging from strategic planning to daily operations of the institution. Inherent in decisions is the recognition of risk and opportunity, requiring that management consider information about the internal and external environment deploys precious resources and appropriately adjusts institution activities to changing circumstances. For governmental institutions, value is realized when constituents recognize receipt of valued services at an acceptable cost. Risk management facilitates management's ability to both create sustainable value and communicate the value created to stakeholders.

The following factors require consideration when integrating ERM into institutional decision making structures:

- Aligning risk management with objectives at all levels of the institution;
- Introducing risk management components into existing strategic planning and operational practices;
- Communicating institutional directions on an acceptable level of risk;
- Including risk management as part of employees' performance appraisals and Business Units' annual operational plans; and
- Continuously improving control and accountability systems and processes to take into account risk management and its results.