NTINGA O.R. TAMBO DEVELOPMENT AGENCY SOC Ltd

RISK MANAGEMENT POLICY

POLICY NUMBER	
POLICY TYPE & CATEGORY	Governance
LAST APPROVAL DATE	30 April 2021
COMMENCEMENT DATE	03 August 2017
INITIAL APPROVAL DATE	03 August 2017
PREVIOUS REVIEWALS	02
NEXT REVIEW DUE	30 June 2022
RESPONSIBLE OFFICIAL	Chief Executive Officer

TABLE OF CONTENTS

KEY DEFINITIONS

Term	Definition
COSO	The Committee of Sponsoring Organizations (COSO) Treadway Commission is a voluntary private sector organization. It is dedicated to helping improve the quality of financial reporting through business ethics, effective external controls, and corporate governance. According to COSO, the three primary objectives of an internal control system are to "ensure efficient and effective operations, provide accurate financial reporting, and comply with laws and regulations."
Enterprise Risk Management (ERM)	An integrated approach to assessing and managing all risks that threaten the entity's ability to achieve its strategic objectives. The purpose of ERM is to understand, prioritize, and develop action plans to maximize benefits and mitigate risks of greatest concern to the institution. The ERM framework enables management to work collaboratively to identify, assess, and manage existing and future risks that are integrated across all functions.
Impact	Result or effect of an event. The impact of an event can be positive or negative relative to the entity's strategic objectives, and there can be a range of possible impacts associated with any single event.
Inherent Risk	The risk to the entity in the absence of any actions management might take to otherwise alter the likelihood the risk could result in an event with a negative impact.
Internal Environment	Encompasses the culture of an entity and sets the basis for how risks are viewed and managed, including risk management philosophy, risk appetite, integrity and ethical values, and the overall environment in which the organization operates.
Likelihood	The possibility that a given event shall occur.
Matrix	The means in which to measure the effectiveness and/or success of risk mitigation strategies.
Opportunity	The possibility that an event shall occur that shall have a positive impact on the institution and the achievement of its strategic objectives.
Performance Assessment	The retrospective activity applied to evaluate the performance of a unit, a process or a function against a pre-determined target or standard over a state period of time.

Term	Definition
Municipal Finance Management Act (MFMA)	The MFMA is an act of parliament, act no. 56 of 2003 first published in 2006 and supported by Treasury Regulations. It is the overriding financial legislation in relation to municipalities and municipal entities. It is mandated in terms of section 214 of the Constitution.
Public Sector Risk Management Framework	The framework represents the pre-eminent source of reference and guidance on risk management practices in the public sector. The Framework aims to support the objectives of public sector institutions through providing information and guidance to enable the implementation and maintenance of effective systems to identify and mitigate the risks that threaten the attainment of service delivery and other objectives, and optimise opportunities that enhance institutional performance.
Residual Risk	The risk that remains after the entity has employed risk strategies/mitigation.
Risk	The threat that an event or action shall adversely affect the entity's ability to achieve its objectives and to execute its strategies successfully. *a) The combination of the probability of an event and its consequences. Risk is inherent in all types of undertaking and may carry the potential for benefit or be a threat to success.* *b) The opportunities, uncertainties, threats, and barriers to which an entity must respond in order to achieve its objectives.*
Risk Acceptance	Occurs when no action is taken to affect a risk's likelihood from developing into an event resulting in a negative impact on the institution
Risk Analysis	Identifying and describing risks and estimating the impact of each on the institution, and developing corresponding risk profile.
Risk Appetite	An entity's tolerance for risk. The broad amount of risk the entity is willing to accept in pursuit of its mission or vision. The measurement of risk appetite may be evaluated qualitatively or quantitatively.
Risk Assessment	Determining the impact of an identified risk on the entity. Risks are assessed on an inherent and residual basis.
Risk Assessment Activities	*Risk identification*—the qualitative determination of significant risks that can potentially impact the entity's achievement of its strategic objectives. This is often done through structured

Term	Definition
	interviews of key personnel by internal or external experts. *Risk prioritization*—the ranking of risks on scale, such as frequency and/or severity.
Risk Avoidance	Avoiding the activities giving rise to the risks.
Risk Control	The technique of minimizing the frequency or severity of potential losses through training, safety procedures, and engineering and security measures.
Risk Evaluation	Comparing the results of estimating risks to the significance of the risks to decide whether to accept and manage them, transfer them by means such as insurance, a combination of the two, or eliminate the risks all together.
Risk Identification	The qualitative and, whenever possible, the quantitative determination of risks that are material; i.e., that potentially can impact the achievement of the entity's strategic objectives.
Risk Mitigation	Actions which reduce a risk or its consequences.
Risk Register	A list of risks identified and evaluated by an entity, that represent a portfolio of risks at a certain time.
Risk Prioritisation	The ranking of material risks on an appropriate scale, such as frequency and/or severity.
Risk Reduction	Action taken to reduce risk likelihood or impact, or both of frequency or severity of potential losses.
Risk Response	Management selection of risk avoidance, acceptance, reduction, or sharing risk, and developing a set of actions to align risks with the entity's risk appetite and tolerances.
Risk Tolerance	The acceptable level of risk relative to the achievement of an objective.
Risk Treatment	The process of selecting and implementing measures to modify the risk.

1. PREAMBLE

The Ntinga Board and Chief Executive Officer (CEO) have committed Ntinga OR Tambo Development Agency (Ntinga) to a process of risk management that is aligned to the principles of good corporate governance, as supported by the Municipal Finance Management Act 56 of 2003, King IV and Treasury Regulations.

Risk Management is recognised as an integral part of responsible management and Ntinga therefore adopts a comprehensive approach to the management of risk. It is expected that all programmes and units, operations and processes shall be subject to the risk management strategy; in a consistent and integrated manner, with the overall objective of reducing risk, as far as reasonably practicable.

Effective risk management is imperative to the agency to fulfill its mandate, the service delivery expectations of the public and the performance expectations by the shareholder and within the agency.

The realisation of Ntinga's strategic plan depends on us being able to take calculated risks in a way that does not jeopardise the direct interests of our stakeholders. Sound management of risk shall enable us to anticipate and respond to changes in our service delivery environment, as well as take informed decisions under conditions of uncertainty.
We subscribe to the fundamental principles that all resources shall be applied efficiently and economically to ensure:

- The highest standards of service delivery;
- A management system containing the appropriate elements aimed at minimising risks and costs in the interest of all stakeholders;
- Education and training of all our staff to ensure continuous improvement in knowledge, skills and capabilities which facilitate consistent conformance to the stakeholders expectations; and
- Maintaining an environment, that promotes the right attitude and sensitivity towards internal and external stakeholder satisfaction.

The risk management processes shall become embedded into Ntinga's systems and processes, ensuring that our responses to risk remain current and dynamic. All risk

management efforts shall be focused on supporting Ntinga's objectives. Equally, they must ensure compliance with relevant legislation, and fulfill the expectations of employees, and other stakeholders in terms of corporate governance.

The risk policy shall be reviewed annually to reflect the current activities on risk management.

2. POLICY MANDATE

Risk Management derives its mandate from Section 95 (c) (i) of the MFMA, Treasury Regulations and Chapter 5 of the King IV Code on Corporate Governance.

MFMA Act No. 56 of 2003

Section 95 (c)(i) of the Municipal Finance Management Act states that " the accounting officer of a municipal entity is responsible for managing the financial administration of the municipal entity, and must for this purpose take all reasonable steps to ensure that the entity has and maintains effective, efficient and transparent systems of financial and risk management and internal control; ..."

King IV report on Corporate Governance

In terms of King IV management should make sure of generally recognized risk management and provide enable assurance regarding the achievement of the organization objectives with respect to:

- Effectiveness and efficiency of operation;
- Safeguarding of the state assets (including information);
- Compliance with applicable law, regulation &supervisory requirement;
- The reliability of reporting;
- Behaving responsibility towards all stakeholders.

3. POLICY OBJECTIVES

The objectives of this policy include the following:

- Alignment of risk-taking behavior of NTINGA with strategic business objectives;

- To promote an innovative risk management culture in the organisation and improve risk transparency to the stakeholders;
- To manage risks that may impact the defined financial and performance drivers;
- To assist NTINGA in enhancing and protecting those opportunities that represent the greatest service delivery benefits;
- Provide a sound basis for integrated risk management and internal control as components of good corporate governance.

4. POLICY IMPLEMENTATION

The policy shall be communicated throughout the agency by means of formal presentations to the board, management and staff; notice boards and the agency's website.

The policy shall be signed by the Board Chairperson and the CEO as a commitment to its approval, implementation and adherence thereto.

Successful implementation of this policy shall be evidenced by efficient and effective administration relating to relevant stakeholders and the responsible workforce and the board.

Legislation in place for the management of specific risks such as Occupational Health and Safety and, Equal Opportunity and Research Ethics shall be complied with.

The Risk Management Policy does not relieve the unit's responsibility to comply with other legislation. Training and facilitation shall, in the first instance, "*assisted through an assessment process, by internal audit. IA shall remain independent in this process.*

5. RESPONSIBILITY FOR RISK MANAGEMENT

5.1 Chief Executive Officer

The accounting officer is accountable for ensuring that a risk management system is established within the agency, implemented and maintained in accordance with the legislative mandate and good governance practices.

Assignment of responsibilities in relation to risk management is the prerogative of the CEO.

5.2 Audit and Risk Committee

The audit and risk committee shall be accountable for the oversight of the processes for the identification and assessment of the general risk spectrum, reviewing the outcome of risk management processes, and for advising the Board as necessary.

5.3 Executive/ Senior Management

Executive or senior management is accountable for strategic risk management within areas under their control including the dissemination of the risk management process to operational managers. These activities can be delegated to the Risk Steering Committee. Collectively the Risk Steering Committee is responsible for:

- The formal identification of strategic risks that impact upon the agency's objectives.
- Allocation of priorities.
- The development of strategic risk management plan; and
- Review of the implementation against risk management plans and communicating this to the Audit and Committee and the agency at large.

5.4 Operational management

Operational management is accountable to the CEO via Executive/ Senior management for:

- Implementation of this policy within their respective areas of responsibility;
- Quarterly and annually reporting on the status of the risk register, insofar as it impacts on their respective responsibilities;
- Ongoing maintenance of the risk register insofar as it impacts on their respective responsibilities; and
- Ensure compliance with risk assessment procedures.

5.5 Internal Audit

Internal Audit shall be accountable through the Audit and Risk Committee for the implementation of this policy in key areas of the Agency, maintaining a programme for risk reassessment and a risk register for the Agency.
Key audit areas shall flow from the results of the risk assessment and the risk management plan. The Director / Manager Internal Audit shall provide advice to the relevant managers on risk management matters pertaining to the Agency "in line with IA's audit objectives. Internal Audit plans shall be driven by risk assessment processes and procedures."

5.6 Employees

Every staff member of Ntinga is responsible for the effective management of risk including the identification of potential risks. Management is responsible for the development of risk mitigation plans and the implementation of risk reduction strategies.
Risk management processes should be integrated with other planning processes and management activities.

6. POLICY MONITORING

Monitoring of the Risk Management Policy is, in principle, the responsibility of management. The oversight function shall be executed by the Audit/Risk Management Committee. Therefore, the Internal Audit functions shall provide technical assistance in as far as monitoring is concerned.

7. GENERIC SOURCES OF RISK AND THEIR AREAS OF IMPACT

Identifying source of risk and areas of impact provides a framework for risk identification and analysis. A generic list of sources and impacts shall focus risk identification activities and contribute to more effective risk management.
Each generic source has numerous components, any of which can give rise to a risk.

Generic sources of risk include:

- Commercial and legal relationships including but not limited to contractual risk, product liability, professional liability and public liability.
- Economic circumstances. These can include such sources as currency fluctuations, interest rate changes,
- Human Behavior such as riots, strikes, sabotages.
- Natural Events. These can include fire, water damage, earthquakes, vermin, disease and contamination.
- Political Circumstances such as legislative changes or changes in government Policy that may influence other sources of risk.
- Technology and Technical Issues. Examples of this include innovation, obsolescence and reliability.
- Management Activity and Control such as poor safety management, the absence of control and inadequate security.
- Individual Activity including, misappropriation of funds, fraud, vandalism, illegal entry, information misappropriation and human error.

Areas of Impact

A source of risk may impact on one area only or several areas. Areas of impact include:

- Asset and resource base including personnel,
- Revenue ,
- Cost both direct and indirect,
- People,
- The community,
- Performance,
- Timing and schedule of activities,
- The environment,
- Intangibles such as reputation , goodwill and the quality of life, and
- Organizational behavior.

8. NTINGA'S PROCEDURE FOR RISK MANAGEMENT

Ntinga follows the Enterprise-wide Risk Management (ERM) Framework which consists of eight interrelated components derived from the way management runs the Agency and is integrated within the management process.

Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, interactive process in which almost any component can influence another.

Internal Environment

Consists of:

- Tone at the top
- Ethical values
- Oversight
- Roles and responsibilities, i.e.
    - ❖ ERM Steering Committee
    - ❖ Senior Managers
    - ❖ Operational staff

Objective Setting

Consists of:

- Related objectives
- Risk appetite
- Risk Tolerance

Event Identification

Consists of:

- ✓ Influences

Categorisation matrices

- ✓ Techniques
- ✓ Updating mechanisms

Risk Assessment

Consists of:

- ✓ Inherent risk
- ✓ Residual risk
- ✓ Assessment techniques
- ✓ Risk aggregation
- ✓ Portraying risk assessments

Risk Response

Consists of:

- Risk response strategies:
  - ❖ avoidance
  - ❖ reduction
  - ❖ sharing
  - ❖ acceptance
- Controls

Control Activities

Consists of:

- Selection of appropriate control activities

Information and Communication

Consists of:

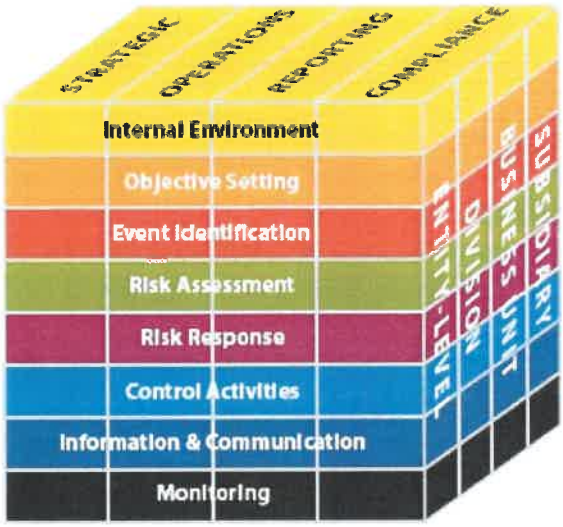
- Information criteria
- Internal communication
- External communication
- ERM automation

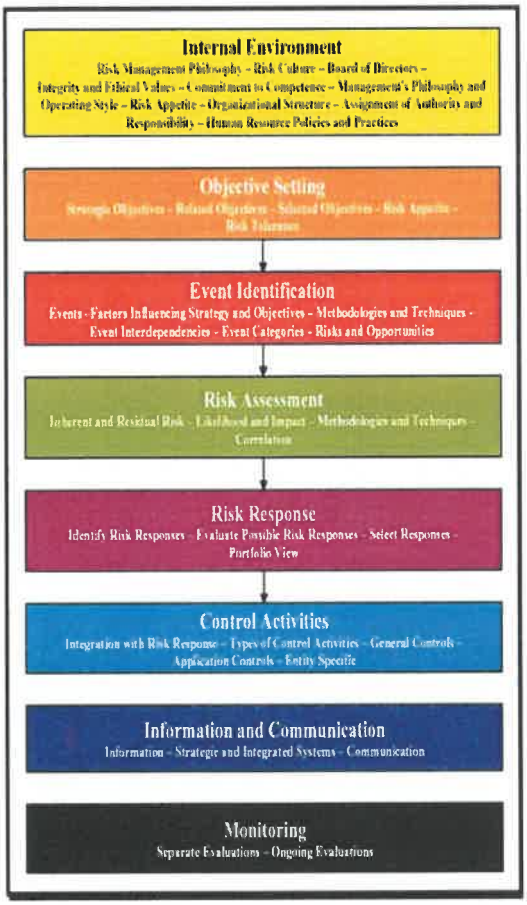
Monitoring

Consists of:

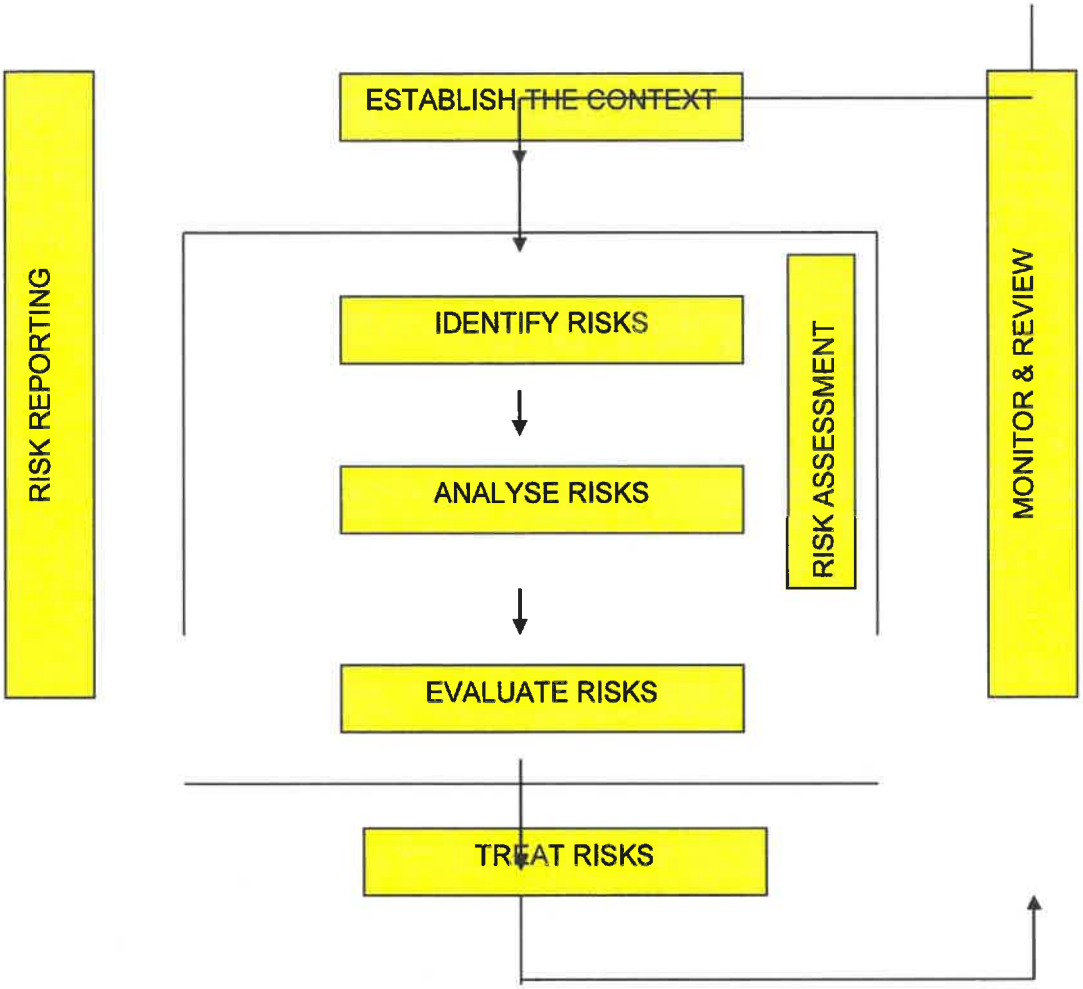
- Ongoing monitoring activities
- Separate evaluations

9. SCHEMATIC PRESENTATION OF NTINGA'S PROCEDURE





The Entity's Risk Management Process is depicted below:



Set out below is a discussion on each element of the process

9.1. Establish the context

✓ The risk assessment processes begin with the profiling of the Entity context. The outputs of this task must be documented and should include amongst others:

- Business environment;
- Total size of the core/ support services;
- Key players;
- Stakeholder's driving forces.

- ✓ Establishing the context is a pre-requisite to the process of identifying risks in any given situation. Establishing the context is about placing a boundary around the subject matter that is being subjected to the risk management process. Contexts can be entire businesses, functions, departments, processes, projects, activities, specific business decisions that must be taken and the like. In setting the context, consideration must be given to:
  - the business objectives of the subject matter that is being covered;
  - the purpose, scope and depth of the risk management process to be applied;
  - the time horizon to be covered for risk identification purposes;
  - establishing the roles and responsibilities of the various people and
  - parts of the organization participating in the risk management process;
  - subdividing the subject matter into a set of elements in order to provide a logical framework that helps ensure that significant risks are not overlooked; and
  - deciding the criteria against which risks will be evaluated.

9.2. Identify risks

- ✓ The purpose of risk identification is to identify all risks within the context established above. The aim is to generate a comprehensive list of risks that might have an impact on the achievement of each of the objectives identified in the context phase above.
- ✓ These events might prevent, delay or enhance the achievement of those objectives.
- ✓ In this regard, risks identified should not only be events that could hinder/threaten the achievement of objectives but also events that could have a positive effect on the achievement of objectives.
- ✓ Comprehensive identification using a well-structured, systematic process and involving the right people is critical, **because a risk not identified at this stage may be excluded from further analysis.** Risk identification should include all risks irrespective of whether or not they are under the control of the Entity.

9.3. Analyse risks

This phase covers the following elements:

Each of these elements is dealt with below.

✓ **Risk exploration** (understanding the causes and consequences of identified risks).

The purpose of risk exploration is to understand the causes and consequences of the identified risks. In the absence of a precise understanding of the cause of a risk one is unable to design effective **preventative** control measures to manage the cause. Similarly, in the absence of a precise understanding of the nature of the consequences of a risk one is unable to accurately measure the impact that the risk may have nor implement effective **corrective** control measures to manage the impact.

✓ **controls evaluation** (evaluating existing risk treatment controls)

This involves obtaining an understanding of the existing preventive and corrective controls currently in place to treat the risk together with the operating effectiveness of those controls. This information is vital for accurately assessing the residual risk level which is covered below.

✓ **determine risk level** (measuring the impact and likelihood levels of identified risks)

Risk assessment involves assessing the magnitude of the consequences of a risk, should it occur, and the likelihood of the event occurring. This consequence and likelihood is combined to produce a risk level. The risk assessment tool set out in Annexure B should be used to facilitate this process. Based on this tool, any given risk will be assessed at one of [5] levels.

- ✓ Two types of risk assessments could be performed, namely qualitative and quantitative.
- ✓ Qualitative assessments are used where risks do not lend themselves to quantification or when either sufficient credible data required for a quantitative assessment is not practically available or a quantitative assessment is not cost-effective. Qualitative assessments are typically based on subjective views of individuals. The following are some of the information sources when performing a qualitative assessment:
  - Past incidents and experience;
  - Published literature;
  - Consultations with stakeholders; and
  - Expert judgements
- ✓ Quantitative techniques involve the use of mathematical models, bring more precision and are typically used in more complex and sophisticated activities to supplement qualitative techniques.
- ✓ It should be noted that qualitative assessments will suffice for the vast majority of risks.

- ✓ Risks are normally assessed at an inherent level and at a residual level. It is accepted, however, that in certain contexts the inherent risk assessment will not add value and that only a residual assessment is performed.
- ✓ The inherent assessment is an assessment of the level of risk before the evaluation of existing risk treatment controls has been considered.
- ✓ The residual risk assessment is an assessment of the level of risk after risk treatment controls have been evaluated.

9.4. Evaluate risks

- ✓ The purpose of risk evaluation is to make decisions, based on the outcomes of risk analysis, about which risks need treatment as well as well as risk treatment priorities.
- ✓ Risks assessed as Level 1 risks will receive the highest priority, followed by levels 2 to 9 respectively. Individual risks or an aggregation of common risks at level [1 and 2] will generally be considered as beyond the Entity risk tolerance level and therefore risks at these levels must be considered for further treatment.
- ✓ Each business unit and corporate function will need to set their own tolerance levels based on their unique circumstances. However, these tolerance levels will need to be aligned with the group tolerance levels.

9.5. Treat risks

- ✓ Risk treatment involves identifying and evaluating the range of available options for treating a risk and the preparation and implementation of appropriate treatment plans.

Available options

Avoidance – Exiting the activities giving risk to the risk. Examples include:

- disposing of a business or a component part
- deciding not to proceed with the project/activity that gives rise to the risk

Reduction – Action is taken to reduce the impact or likelihood, or both. Examples include:

- establishing limits of authority;
- introducing new internal control measures

Sharing – Reducing risk likelihood or impact by transferring or sharing a portion of the risk with third parties. Examples include:

- purchasing insurance products
- engaging in hedging activities

- ✓ Retaining the risk - Some level of residual risk will always be retained after the implementation of risk treatment plans and management will need to decide whether the remaining risk level is acceptable or not.
- ✓ Selecting the most appropriate response or a combination of responses involves, amongst other things, balancing the costs of implementing the treatment against the benefits to be derived. The cost of managing a risk must be commensurate with the benefits to be derived.
- ✓ Preparing and implementing risk treatment plans
- ✓ The purpose of risk treatment plans is to document how the chosen options will be implemented. The treatment plans should include:
  - proposed actions;
  - resource requirements;
  - responsibilities;
  - timing;
  - performance measures; and
  - reporting and monitoring requirements

9.6. Monitor and review

- ✓ Any risk profile will change over time. Risk treatment plans that were once effective may become irrelevant; control activities may become less effective, or no longer be performed; business objectives may change or regulatory requirements may change.
- ✓ This can be due to the arrival of new personnel, changes in the business structure or direction, the introduction of new systems and processes or developments in the external environment.
- ✓ In the face of such changes, management needs to continually monitor the effective functioning of the risk management process. This monitoring should occur in the normal course of management activities.
- ✓ The following monitoring mechanisms should be implemented:

Monitoring of implementation of risk treatment plans.

- ✓ Action plans to develop and implement risk treatment plans need to be monitored to ensure that the necessary plans are implemented on schedule and as intended.
- ✓ This monitoring process should be embedded within the normal day to day monitoring processes already in place within the business e.g. departmental meetings, management meetings, etc.

- ✓ Internal audit will also evaluate the status of action plans for significant risk exposures as part of their routine audits.

Monitoring of ongoing effectiveness of risk treatment controls

- ✓ The effective operation of risk treatment controls must be evaluated on an on-going basis.
- ✓ Each functional area within the Entity will need to develop its own plans as to the frequency and scope of these reviews taking into account, inter alia, legal and regulatory requirements. These reviews may include management reviews, self-assessment reviews and third-party reviews as appropriate. Internal audit will also perform an independent review of selected risk treatment controls.

Identification and assessment of new/ emerging risks

- ✓ There is a need to regularly review risk registers to ensure that they remain relevant and complete. This applies to strategic, functional/departmental and process level risk registers.
- ✓ It is a group requirement that this review is formally done at least twice annually across all areas of the business. However, the occurrence of any one or more of the following events should trigger the need for an immediate review:
  - Changes in business strategy
  - Legal & regulatory changes
  - Restructuring of the business or departments or processes or major changes to people, processes and technology
  - Loss of key personnel
  - Significant control deficiencies identified by internal and/or external auditors
  - Incidences of fraud
  - Legal liabilities and challenges
  - Changes to business objectives
  - Changes to key performance indicators

Monitoring of the effectiveness of the risk management process as a whole

- ✓ The efficacy of the entire risk management process needs to be reviewed on a periodic basis.
- ✓ The Internal Audit department will be responsible for performing such review and providing assurance that the risk management process has been applied appropriately across the organization and that all elements of the process are suitable and sufficient.

9.7. Risk reporting

- ✓ The essence of risk reporting is that the right people must receive the right information at the right time.
- ✓ Risks at all levels must be reported internally (formally and informally) at different levels within the Entity. Each department or division will need to develop its own reporting framework taking into account existing management reporting processes and legal and regulatory requirements.

10. POLICY EVALUATION

The evaluation of the Risk Management Policy shall be continuous as risk management in the Entity is an ongoing process.

Evaluation shall be done by the Internal Audit in terms of the International Standards for the Professional Practice of Internal Auditors (ISPPIA) and the Auditor General in terms of the Auditor General's mandate. This is to ensure independent review of the Policy and the risk management process.

11. POLICY REVIEW AND AMMENDMENT

The policy shall be reviewed annually or when the need is determined by the Risk Management Committee in consultation with Audit and Risk Committee. Amendments could be influenced by changes in the policies which affect risk management and any other legislation, international requirement or best practices.

12. VIOLATION AND ENFORCEMENT

The violation of this policy may lead to disciplinary processes taken against the offender.

13. COMMUNICATION AND APPROVAL

Supported by:

.....
Chief Executive Officer

Approved by:

For Board: .....

Date: .....

BOARD APPROVED COPY
NTINGA O.R. TAMBO DEV. AGENCY
Date: 03/08/2017
S.O.C
Signature: .....