KONZA
Technopolis

RISK MANAGEMENT POLICY

JULY 2020

ICPAK
Uphold Public Interest

Table of Contents

LIST OF TABLES

LIST OF FIGURES

OUR IDENTITY

Vision

To be a leading global technology and innovation hub.

Mission

To develop a sustainable smart city and an innovation ecosystem, contributing to Kenya's knowledge-based economy.

Mandate

The mandate of KoTDA is to develop Konza Technopolis as a globally competitive smart city by creating an enabling environment through utilization of ICT for socio-economic development.

Strategic Objectives

- Develop and manage a world-class smart city with a vibrant, safe and secure, healthy and sustainable ecosystem.
- Form partnerships with other actors in the National Innovation System, to recruit, attract, and develop high-end talent as well as create relevant, and smart innovative solutions and commercialize them.
- Mobilise adequate and sustainable funding to meet the Authority's mandate and changing needs of the business community and residents.
- Create a strong brand and image of Konza Technopolis that will attract, facilitate and retain investors.
- Ensure that the Authority has adequate institutional capacity to fulfil its mandate.

LIST OF ABBREVIATIONS

A&RC	Audit & Risk Committee
BA&RC	Board Audit & Risk Committee
CEO	Chief Executive Officer
COSO	Committee of Sponsoring Organizations
ERM	Enterprise Risk Management
HIA	Head of Internal Audit
HOD	Head of Department
IRMPF	Institutional Risk Management Policy Framework
ISO	International Organization Standards
IT	Information Technology
KoTDA	Konza Technopolis Development Authority
KRI	Key Risk Indicators
MDA	Ministries, Departments & Agencies
PFMA	Public Finance Management Act 2012
RMC	Risk Management Committee
RMP	Risk Management Policy
RMS	Risk Management Strategy

PROJECT BACKGROUND

Konza Technopolis is a smart city designed and implemented by the government of Kenya to enhance Kenya's innovation ecosystem and digital economy by providing the missing infrastructural and technological link.

To bridge the technological gap and ensure the city is established to smart city standards as envisaged in the city's Masterplan, the Vision 2030 Blueprint and the Kenya's Digital Economy Blueprint – 2019, the government is implementing the Konza National Data Centre and Smart City Facilities project.

Whereas to bridge the infrastructural gap and ensure the city is established to smart city standards as envisaged in the city's Masterplan, the Vision 2030 Blueprint and the Kenya's Digital Economy Blueprint – 2019, the government is implementing the Horizontal Infrastructure project which establishes Phase 1 Roads and Streetscapes, Wastewater Reclamation Facility, Municipal/ Public Buildings and Parks etc.

PREAMBLE

Public Sector management have laid emphasis on transparency and accountability. This has resulted in increased focus in governance of Public Institutions and the incorporation of risk management in all key processes. Konza Technopolis Development KoTDA was established with the objective of ensuring that Konza Technopolis grows into a sustainable world class technology hub and a major economic driver for the nation with vibrant mix of businesses, workers, residents, and urban amenities.

The KoTDA as part of the wider Public Service Institutions is determined to implement the Treasury Circular No. 3/2009 of 23rd February, 2009 and The Public Financial Management Act (PFMA) 2012 section 73 (3) (b) on Institutional Risk Management Policy Framework (IRMPF) as part of the Public Financial Reforms Agenda.

This Risk Management Policy among other documents developed will be a management tool that enables the Authority to be forwarding looking, anticipate any potential impediments/risks that can impact on the achievement of strategic objectives and put in place appropriate mitigation measures. Furthermore, effective risk management will allow the KoTDA to prioritize on critical risks and channel resources towards mitigating identified risks thereby improving the utilization of resources and the quality of services rendered to the public.

POLICY STATEMENT

The Board of Directors of Konza Technopolis Development has committed the Authority to a process of Risk Management that is aligned to the principles of best practice of corporate governance. The features of this process are outlined in this Risk Management Policy. It is expected that all Departments, Divisions, Business Units, and processes will be guided by this Risk Management Policy.

An enterprise-wide approach to risk management has been adopted by the KoTDA, which means that every key risk in each business unit shall be included in a structured and systematic process of risk management. All key risks shall be assessed within a unitary framework that is aligned to the KoTDA's objectives and strategy.

It is expected that the risk management processes shall become embedded in our business systems and processes, so that our responses to risk remain current and dynamic. All key risks associated with major changes and significant actions by the KoTDA shall also fall within the processes of risk management.

The nature of our business demands that the KoTDA adopts a prudent approach to corporate risk, and all decisions surrounding risk tolerance and risk mitigation shall reflect this approach. Nonetheless, the respective business units and departments charged with decision making shall ensure that the implementation of this policy does not slow down the KoTDA's growth with inappropriate bureaucracy. Controls and risk interventions will be chosen based on their ability to increase the likelihood that we will fulfil our mandate to the different stakeholders.

1 RISK MANAGEMENT POLICY RATIONALE AND SCOPE

1.1 Background

This is the Risk Management Policy (RMP) for KoTDA, and in developing this Policy, the KoTDA was compelled by the need to integrate effective Enterprise Risk Management principles in decision making, through a unified approach to enhance efficiency. The Policy is expected to enhance the application of good corporate governance principles, risk management and internal controls, and address challenges in both internal and external operating environment.

This Risk Management Policy is benchmarked against global best practices aligned to **COSO Enterprise Risk Management Framework and ISO 31000**. The policy is domesticated to match the expectations of the Treasury Circular on Institutional Risk Management Policy Framework in MDAs.

1.2 Risk Management Policy Objectives

KoTDA's Risk Management Policy supports the following corporate objectives:

i. To help **ensure that the risk management policy is understood** and consistently applied across the KoTDA

ii. To **enhance compliance** with relevant regulatory requirements

iii. To **create and protect value** at KoTDA by contributing to the achievement of KoTDA's objectives

iv. To **identify, measure and control risks** that might impact the achievement of KoTDA's objectives

v. To **provide a framework for formulation of Risk Management Strategies**

vi. To **identify and harness opportunities**; and

vii. To **protect and enhance the reputation** of KOTDA.

1.3 Risk Management Policy as a Management Tool

The RMP has the following benefits to the Board of Directors and Management:

- Anticipates any potential impediments/risks that can impact on the achievement of strategic and operational objectives and proposes appropriate risk treatment measures.
- Enables management to make the right decisions in an uncertain operating environment and establish pre-emptive strategies to enhance service delivery.
- Ensures that management remains focused on understanding the nature of risks and steps to mitigate the potential negative consequences.

- Allows management to evaluate, prioritize, and address critical risks and channel resources to risks thus improving the utilization of resources and quality of services rendered.
- Acts as a guide on development of strategies, procedures and controls required to manage risks within levels acceptable to the KoTDA.

1.4 Scope

This Risk Management Policy has been designed to:

i. Provide the **framework for identification and analysis of the risks**

ii. Set appropriate **risk appetite limits and controls**, and

iii. Provide framework for monitoring risks and adherence to the limits.

This Policy outlines KoTDA's approach to risk management, the roles and responsibilities of the Board, Management and Employees. The Policy also describes key aspects of the risk management process, defines the main reporting procedures, and provides a framework for monitoring and evaluating effectiveness of the Policy.

The RMP provides a framework for the management of risk inherent in all activities/operations of the KoTDA. It provides the basis for preparation of the Risk Management Strategy, which will define in detail the risks facing the business units in the KoTDA and determine mitigating measures.

1.5 Risk Management Policy Approval

This Policy shall be approved by the Board through the Audit & Risk Committee and will be applicable to all Departments, Divisions, Business Units, and Support Functions within the Authority. All staff members and Management are expected to adhere to this Policy and other linked procedures set out in the policy.

The Internal Audit & Assurance Division shall be responsible for the maintenance of this Policy.

1.6 Review

This procedure shall be reviewed every three (3) years.

2 KoTDA's RISK PROFILE

The identification and effective management of risks is critical for the achievement of KoTDA's strategic objectives. In identifying the types of risks that the KoTDA is exposed to, specific regard is accorded to guidelines on risk management and internal controls for public sector organizations. The KoTDA is exposed to some inherent risks owing to its nature of operations that entails multi-stakeholder engagements and highly technical operations in a bid to develop a pioneer silicon savanna for the region. The following section on Risk Universe illustrates the specific risks that the KoTDA is exposed to and for which the day to day management has been charged to the respective risk owners.

2.1 KoTDA's Risk Universe

The Risk Categories adopetd by the KoTDA are in line with the globaly recommended risk taxonomy for classifying risks.These include:

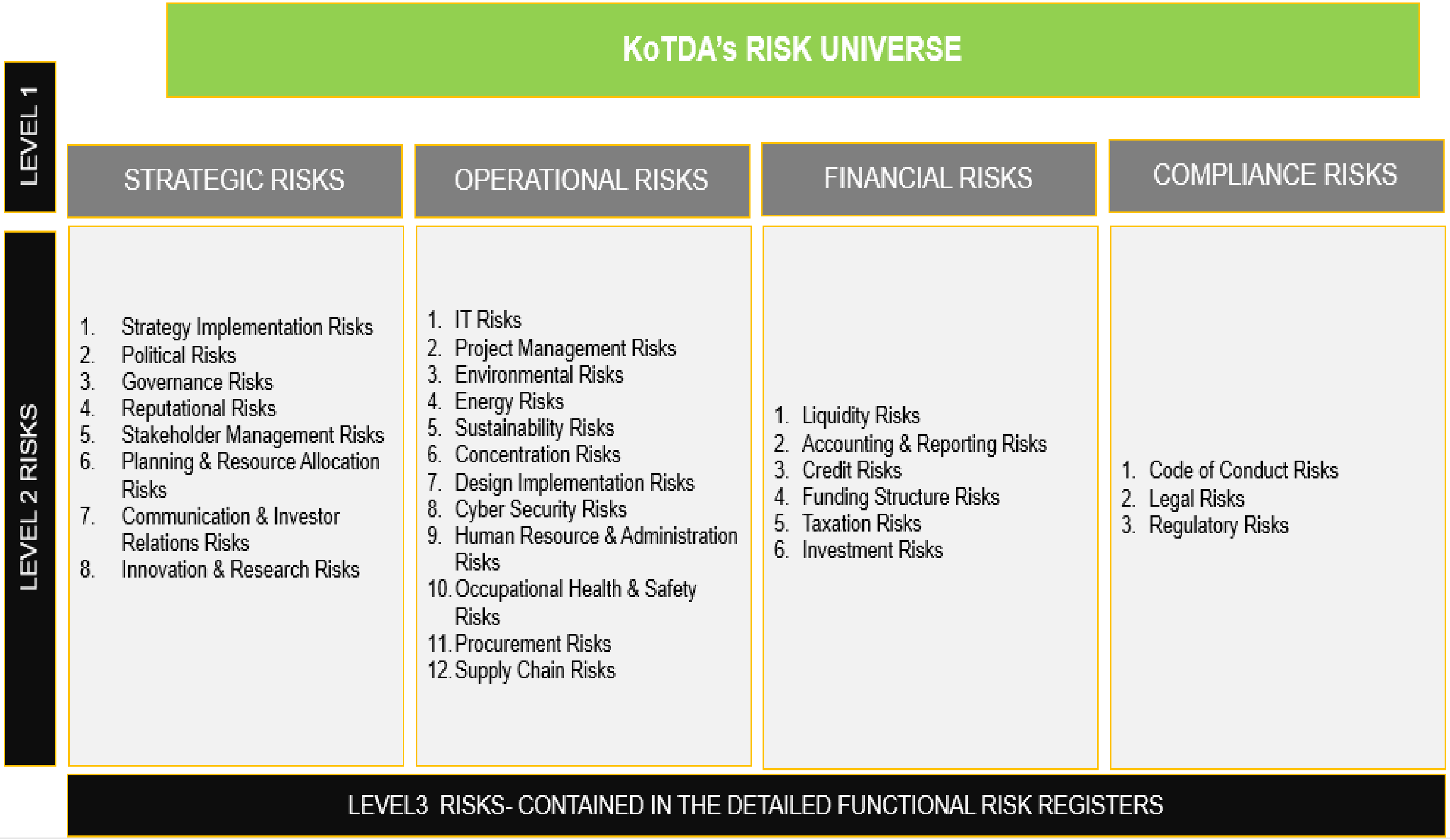
i. **Strategic Risks:** Risks arising internally from strategic decisions such as new projects and investments, new partnerships, new service lines. Risks arising from the conflicting demands of stakeholders (Customers, management, employees, suppliers, the public, regulators). Impacts may be primarily reputational as well as financial.

ii. **Financial Risks:** Risks arising from financial transactions and accounting and reporting requirements, e.g. Fraud, interest exposures, misstated management and financial accounts, misleading or omitted disclosures.

iii. **Operational Risks:** Risks resulting from inadequate or failed internal processes, people and systems or from external events. The risks resulting from the execution of the core business of the Authority are all classified under operational risks.

iv. **Compliance Risks:** These are risks relating to compliance obligations imposed by different regulators that the Authority is subjected to. These risks also can emanate from internal compliance obligations to policies and internal procedures.

The Risk Universe for KoTDA is further summarised by the diagram below:



KoTDA's RISK UNIVERSE

LEVEL 1

STRATEGIC RISKS

OPERATIONAL RISKS

FINANCIAL RISKS

COMPLIANCE RISKS

LEVEL 2 RISKS

STRATEGIC RISKS

1. Strategy Implementation Risks
2. Political Risks
3. Governance Risks
4. Reputational Risks
5. Stakeholder Management Risks
6. Planning & Resource Allocation Risks
7. Communication & Investor Relations Risks
8. Innovation & Research Risks

OPERATIONAL RISKS

1. IT Risks
2. Project Management Risks
3. Environmental Risks
4. Energy Risks
5. Sustainability Risks
6. Concentration Risks
7. Design Implementation Risks
8. Cyber Security Risks
9. Human Resource & Administration Risks
10. Occupational Health & Safety Risks
11. Procurement Risks
12. Supply Chain Risks

FINANCIAL RISKS

1. Liquidity Risks
2. Accounting & Reporting Risks
3. Credit Risks
4. Funding Structure Risks
5. Taxation Risks
6. Investment Risks

COMPLIANCE RISKS

1. Code of Conduct Risks
2. Legal Risks
3. Regulatory Risks

LEVEL3 RISKS- CONTAINED IN THE DETAILED FUNCTIONAL RISK REGISTERS

Figure 2.1-1: KoTDA Risk Universe Profile

2.2 Risk Philosophy

KoTDA's approach to risk accepts and embraces risk management as a core competency that allows it to optimise risk taking through objectivity and transparency that will ensure effective and efficient risk taking in service delivery to its Customers and stakeholders within a chosen risk appetite.

KoTDA's risk management approach utilises an approved enterprise-wide risk management methodology to ensure adequacy and effectiveness. The risk management approach will continue to ensure effeciency in operations through the application of the following core principles:

i. Clear assignment of responsibilities and accountabilities.

ii. Common enterprise-wide risk management framework and process.

iii. The identification of uncertain future events that may affect the achievement of work plans, projects, and strategic objectives; and

iv. The integration of risk management processes within KoTDA's activities.

The focus on the stakeholder is the most comprehensive approach because value creation on behalf of the stakeholders is only possible if our customers are satisfied, our employees motivated, and our partners are sufficiently reassured with respect to compliance.

2.3 Defining Risk Appetite

This Policy recognizes that not all risks will be eliminated, and some level of risk will always exist. Risk Appetite is the overall level of exposure to risk that is acceptable for the Authority to accept in pursuit of its strategic and operational objectives. KoTDA's risk appetite will be expressed as the boundary, above which the risk level will not be tolerated, and further actions taken to mitigate risk.

The risk appetite will be operationalized through a determination of the risk tolerance limits for each risk identified. Management will be mandated to ensure that KoTDA operates within the tolerance limits.

Risk appetite reflects KOTDA's ability to take on risk as derived from its capacity to bear risk and the philosophy or attitude towards risk taking. Risk Appetite is measured using qualitative and quantitative factors that are based on specific key performance indicators. As risks are part of doing business, KoTDA strives to reduce the same to an acceptable level.

The Authority expresses its acceptable levels of risk through carefully articulated risk appetite statements that have been forumulated by Management as guided by the Consultant. These Risk Appetite Statements shall be approved by the Board from time to time as proposed by Mangement.

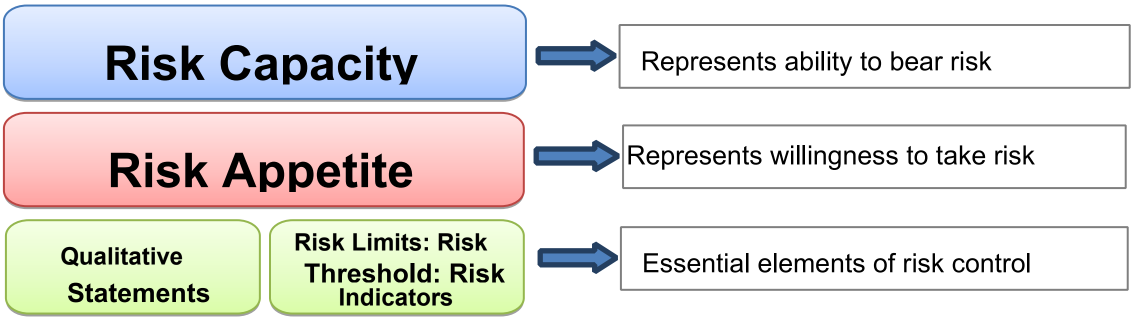

Risk Capacity
Represents ability to bear risk
Risk Appetite
Represents willingness to take risk
Qualitative Statements
Risk Limits: Risk Threshold: Risk Indicators
Essential elements of risk control

Figure 2.3-1: Defining Risk Appetite

The Board shall define the risk statement of KOTDA based on recommendations from the Audit & Risk Commitee. Risk appetite is stated in terms of the entire Risk Universe i.e.***Strategic, Operational, Financial & Compliance Risks.***

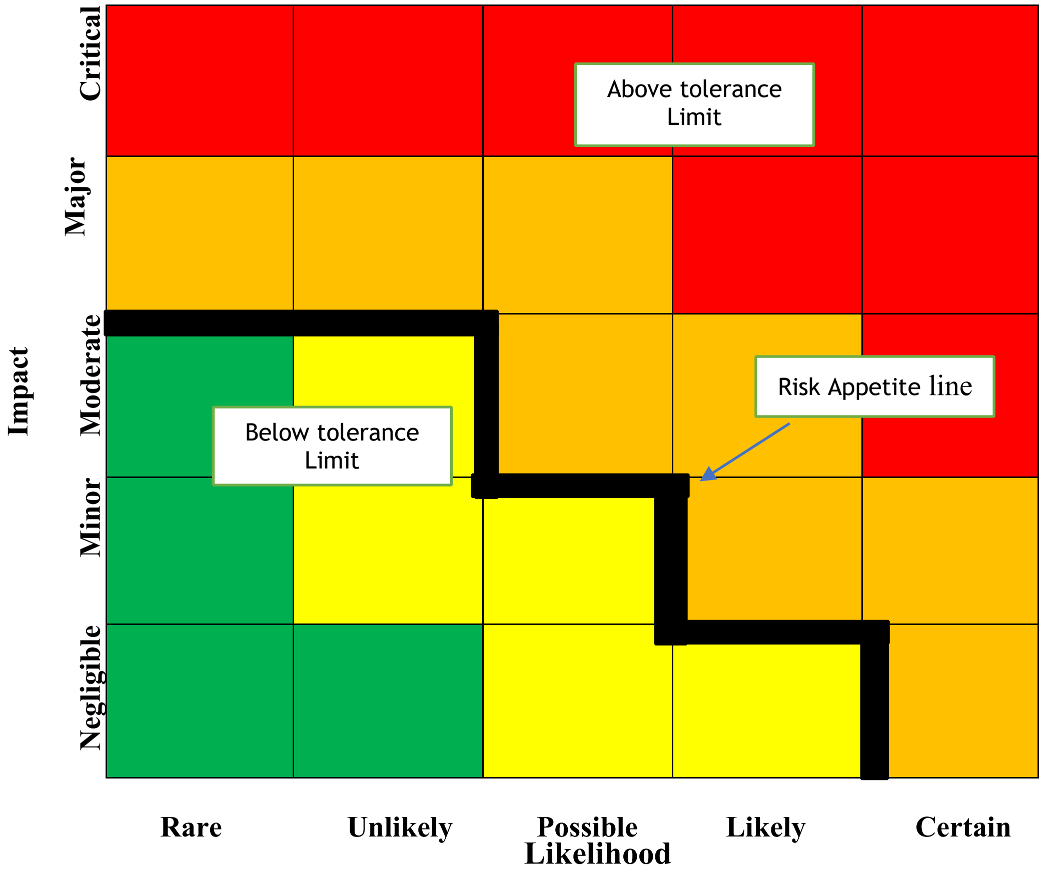


Figure 2.3-2: Risk Appetite Line

2.4 Risk Appetite Statement

KoTDA is exposed to a variety of risks as it strives to achieve its mandate as set out in its Strategic Plan. These risks will be identified, managed and assessed within a risk management framework.

KoTDA's approach is to minimize its exposure to governance, strategic, reputational, operational and financial risk, whilst accepting and encouraging an increased degree of risk in pursuit of its mission and objectives. It recognizes that its appetite for risk varies according to the activity undertaken, and that its acceptance of risk is subject to ensuring that potential benefits and risks are fully understood before developments are authorized, and that sensible measures to mitigate risk are established

The KoTDA shall manage risks to enable sustainable business strategy execution in the interest of all its stakeholders and hence:

i. Always **consider the reputational impact** of business decisions made

ii. **Complies with all laws and regulations**, low tolerance for regulatory breaches.

iii. **Maximise Customer satisfaction** and remain innovative in response to economic, regulatory, technology and competitive influence

iv. Invests in new **business but with a low appetite** for potential losses

The risk appetite matrix below defines risk appetite against various risk categories and shall be approved by the Board from time to time:

RISK CATEGORY	**BOARD LEVEL ARTICULATION**
Strategic	Zero appetite for risk with regards to governance exposure commensurate with opportunities to serve our customers and fulfil our mandate.
	KoTDA accepts a low level of risk where there are significant opportunities to serve our core stakeholders and achieve our mission.
	KoTDA has low appetite for non-attainment of strategic objectives.
	It is regarded as critical that KoTDA preserves a high reputation.
	KoTDA has zero appetite for activities that could lead to undue adverse publicity.
Operational	KoTDA has zero operational appetite for process failure.
	KoTDA has zero operational appetite for fraud and losses.
	Zero tolerance for IT and data security breaches.
	KoTDA employs suitably skilled and experienced staff.
	KoTDA is an equal opportunity employer.
	KoTDA has zero appetite for Project failure.
Financial	High appetite for maintaining a long-term financial viability and overall financial strength.
	Low tolerance for Technopolis Investors attrition
Compliance	Zero appetite for legal action against KoTDA.
	Zero tolerance with regards to non-compliance with agreements, legislation, and policies.
	Zero tolerance for high priority internal audit/regulatory issues.
	Potential conflicts of interest are avoided and or disclosed.

Table 2-1: Risk Appetite Statement

3 RISK MANAGEMENT STRATEGY

3.1 Key principles

KoTDA's Risk Management Strategy is to develop, implement and continuously improve on its risk management framework and related processes. Various principles have been developed to guide in implementation of this strategy. The following key principles underline KoTDA's approach to risk management:

i. KoTDA shall adopt an open and receptive approach to discussing and addressing risks.

ii. KoTDA shall only support decisions made where there is evidence of a proper and thorough assessment of associated risks.

iii. KoTDA shall establish a centrally coordinated Risk Management Policy and Management process to ensure consistency throughout the Authority. Management is responsible for the system of risk management and internal control within their areas of operations and responsible for notifying executive management where exposure to risk is of a material nature.

iv. Risks shall be allocated to section heads placed and empowered to control and manage them.

v. At a minimum, KoTDA will undertake an annual review of the most significant risks facing it and evaluate their impact on it as the operational environment changes.

vi. There shall be a continual evaluation and review of the internal and external environment factors that may affect the achievement of objectives.

vii. Risk is central to all policy and decision-making, as well as project and operational management. Risks must be considered throughout project plan formulation, project management processes and delivery of service to stakeholders and at all aspects of the strategic, project management and operational processes,

viii. Ongoing monitoring, review, and provision of re-assurance on the effectiveness of the risk management process by the Internal Audit & Assurance Division and ongoing reporting to the respective stakeholders on the results and status of risk management.

3.2 Approaches to Risk Management

Risk management is an integral part of the strategic management of an organization. As part of Risk Management, KoTDA shall develop a Risk Management Strategy (RMS) which shall methodically identify and address the risks attached to all KoTDA activities to achieve sustained benefit(s) from each/all activities.

The RMS will detail the impact of the identified risks on achievement of strategic and operational objectives, the treatment of the identified risks including residual risks, considering the risk tolerance levels. The RMS will form the basis on which to provide assurance that the processes are effective through formal audit, review, and monitoring.

The process is illustrated below.

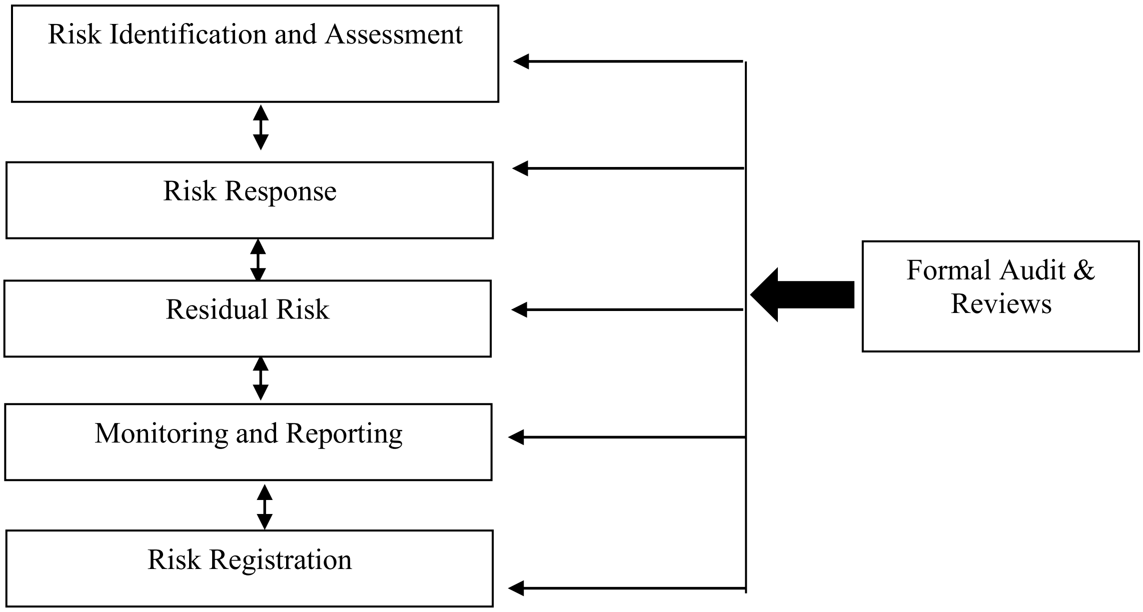


Figure 3.2-1: Risk Management Strategy

While risk identification and assessment will be primarily aimed at those events that may occur within the planning period, Management shall not ignore long term risks. Risk Assessment will be guided by the following parameters:

- Risk definition and classification;
- Impact descriptors; and
- Risk appetite.

3.3 Risk Identification

Identification of risks will be the first step in building of the Corporate risk register. Risk identification and profiling will be a continuous process. The original risk register will be based on risks identified based on past occurrences and an evaluation of the current and future operating environment.

Risks may be identified by management, departments, project teams, risk champions and process owners.

All risks identified at departmental levels shall subsequently be listed in the corporate risk register, which will be KoTDA's risk profile. The corporate risk register will be a live document with opportunities for review and update. Identified risks shall be assigned to a ‘Risk Owner’ whose responsibility will be to ensure that the risk is managed and monitored over time.

All staff have the responsibility of identifying and monitoring risks within their area of operation and to bring risks to the attention of their supervisors. It is the responsibility of Heads of Departments and Divisions to put controls in place and to gain assurance that risk in their area of control are being monitored appropriately.

3.4 Root Cause Analysis

The root cause of a risk is the underlying event or control breakdown that causes the risk to occur. Sources of risk can be either internal or external. The purpose of identifying potential root causes is to give direction to risk-intervention measures.

3.5 Gross Risk Assessment

Risks shall be assessed based on their Impact to business objectives and likelihood of occurrence. Gross risks assessment is the impact and likelihood of a risk when measured without any controls. The purpose of evaluating risks at a gross level is to gauge the overall effects of the risks when the organisation takes no measures to mitigate them.

3.5.1 Risk Likelihood

Risk likelihood assessment will involve determining the score of the event occurring (probability).

The following are the five levels of risk likelihood as shown in the table 3.1 below:

Scale	Description	% Likelihood	Relative Frequency
5	Certain	90% - 99%	Weekly
4	Likely	70% - 89%	Quarterly
3	Possible	50% - 69%	Biannually
2	Unlikely	30% - 49%	Within 2 years
1	Rare	10% - 29%	Within 10 years

Table 3-1: Risk Likelihood Criteria

3.5.2 Risk Impact

Risk impact assessment will involve determining the effect that a risk has on the overall strategy of KoTDA and the specific process objectives that support the strategy.

The following are the five levels of impact as shown in the table 3.2 below.

Scale	Description	Criteria					
		Budget	Brand	Regulatory	Operations	Safety	Attention
5	**Critical**	> 35 % of expenditure. Potential Impact of revenue that is >Ksh.1M	International condemnation	Licences withdrawn	Total loss of operations	Loss of life	Events and problems will require board and senior management to resign.
4	**Major**	26%-35% of expenditure-Potential Impact of revenue that is between Ksh. 500,001 and Ksh.1M	Major media scandal	Regional suspension	Prolonged loss of a major unit	Medical attention required	Events and problems will require Board and Senior Management attention.
3	**Moderate**	15%-25% of expenditure -Potential Impact of revenue that is between Ksh. 250,000 and Ksh. 500,000	Regional media coverage	Major prosecution	Partial loss of operations	Reportable incidents	Event will require Senior and Middle-level Management intervention.
2	**Minor**	10%-15 % of expenditure Potential Impact of revenue that is up to Ksh.250,000	Negative chat room items	Minor fine	Minor problem at a unit	First aid required only	Issues will be delegated to Middle-level Management for resolution.
1	**Negligible**	<10% of expenditure Potential Impact of revenue that is up to Ksh.50,000	Single complaint in media	Negligible fine	Easily rectifiable problem	Minor near misses	Issues can be solved at Operational Level.

Table 3-2: Impact Ranking Criteria

Identified risks will be analyzed on the weights of the likelihood of occurrence and projected consequences to determine if they are critical, Major, moderate, minor or negligible risk.

Identified risks will be ranked on the weights of the likelihood of occurrence and projected consequences to determine if they are Critical, moderate, or Minor risk as shown in Figure 3.5-1 below:

Risk Analysis	Negligible	Minor	Moderate	Major	Critical
Certain	High	High	Extreme	Extreme	Extreme
Likely	Medium	High	High	Extreme	Extreme
Possible	Medium	Medium	High	High	Extreme
Unlikely	Low	Medium	Medium	High	Extreme
Rare	Low	Low	Low	High	Extreme

Figure 3.5-1: Risk Heat Map

The definition and recommended actions for the above risk levels is tabulated in Table 3.3 below:

Risk Levels	Recommended Response Options & Reporting
Critical and Major Risks	i. Evaluate compliance to the tolerance limits. If in deviation of the limits, prepare immediate/emergency management plan to address catastrophic risks. ii. Evaluate effectiveness of existing mitigation measures, if inadequate, identify corrective measures to improve the control. iii. Allocate action team and resources for prompt implementation. iv. Carry out regular internal reporting. v. Promptly report risk to Board Audit & Risk Committee and Board of Directors as per the risk management standards.
Moderate	i. Evaluate compliance to the tolerance limits. If in deviation of the limits prepare & implement a specific management plan for medium risks. ii. Allocate action team & resources to minimize risks where controls are deemed inadequate & monitor implementation. iii. Report to Management Committee on quarterly basis.
Minor	i. Accept and Monitor low priority risks ii. Monitor through normal internal reporting structures & routine procedures iii. Heads of Departments & Divisions to monitor on regular basis

Table 3-3: Risk Classification and Response Options

3.5.3 Evaluation of existing controls

Upon established which controls management has in place to manage the risk in question, it is necessary to assess the control effectiveness. This is a measure of how well management perceives the identified controls to be working and effectively managing the risks. The standard table below classifies controls into 4 levels of effectiveness:

Control Effectiveness Legend		
Weak/Unsatisfactory	< 50%	Some of the risk exposure appears to be controlled, but there are major deficiencies. Control measures are ineffective.
Satisfactory	50%-70%	There is room for some improvement.
Good	71%-85%	Majority of risk exposure is effectively controlled.
Very Good	> 85%	Risk exposure is effectively controlled.

Table 3-4: Control Effectiveness Rating

3.6 Risk Response

Treatment of risks will be part of risk management process in which decisions are made about how to treat risks that have been identified and prioritized. Risks shall be treated through appropriate responses for each level as outlined in Table 3. Options for risk treatment will include:

i. **Acceptance** – an informed decision to accept/tolerate risks without any further action being taken. Even if it is not tolerable, ability to do anything about such risks may be limited, or the cost of taking any action may be disproportional to the potential benefit gained. In this case, the response would be to tolerate the existing level of risk. This option will be supplemented by contingency planning for handling the impacts that will arise if the risk is realized.

ii. **Reduction** – a large number of risks will be addressed through reduction. The purpose of treatment will be that, whilst the activity giving rise to the risk continues, action (control) is taken to contain the risk to an acceptable level through systematic reduction in the extent of exposure to a risk and/or likelihood of its occurrence.

iii. **Transfer** – the best response for some risks will be to transfer them through either, conventional insurance or paying a third party to take care of the risk. This option will be particularly appropriate for mitigating financial risks to assets.

iv. **Avoidance/Terminate** - this technique will involve taking steps to remove the activities giving rise to the risk.

v. **Additional information** - some uncertainty may be caused by lack of relevant information which if available would reduce the level of perceived risk. Some risks will be avoided or reduced if additional relevant information is obtained for decision making.

3.7 Residual Risk

Residual risk is the risk remaining after controls have been put in place to mitigate the inherent risks. The residual risk will be acceptable provided it can be demonstrated that all measures have been taken to limit the inherent risk within the limits set i.e. in terms of the costs and benefits. Monitoring and reporting on the residual will be an integral part of risk management.

3.8 Monitoring and Reporting

3.8.1 Monitoring

An elaborate reporting and monitoring regime are necessary in the entire risk management process. Monitoring will ensure that appropriate and timely corrective measures are taken and weaknesses in the process are addressed.

The RMP monitoring process will embrace regular review and update of the corporate risk register and an effective on-going monitoring regime including early warning triggers/indicators. The monitoring process will enable KoTDA respond to threats to progress at an early stage and to take appropriate action.

Monitoring shall determine whether:

i. Risk measures adopted resulted in what was intended.

ii. Procedures adopted and information gathered were appropriate.

iii. Improved knowledge would have helped to reach better decisions.

iv. There are lessons learned for future assessments and management of risks.

3.8.2 Reporting

The purpose of risk management reporting is to allow management to:

i. Understand, at a meaningful level, the departmental risk profiles, and consolidated risks at the enterprise level.

ii. Report on risks within the context of a risk appetite and capacity guidelines from the board;

iii. Develop a basis for early-warning systems on significant changes in risk profile;

iv. Identify issues and unfavourable trends in a timely manner to permit corrective actions to minimize KoTDA risk and hard cash losses.

3.8.3 Internal Reporting Processes for Risk Information

A critical aspect of the risk management plan is the internal reporting process around risk information. KoTDA is required to report on three main aspects:

i. The current rating of the risk;

ii. The performance of controls for the risk;

iii. Any losses incurred as a result of the risk during the reporting period in question.

3.8.4 Defining reports

The factors that need to be considered in determining the type of risk management reports include:

i. User of the report;

ii. Level of detail required for the report;

iii. Availability of information required for the reporting elements.

iv. Frequency required for the report given subject matter.

The reporting cycle should be reviewed on an annual basis:

Predetermined reports should be prepared on a fixed interval as prescribed in the risk management guidelines.

Ad hoc reports on items of interest will be created as issues develop.

3.9 Risk Registration

KoTDA shall maintain a risk register that details all risks, 'risk owners', the likelihood and impact of each risk as assessed and measures assigned. For each risk, measures will be identified to prevent/minimize risk and to provide for crisis management/disaster recovery and business continuity in case the risk is realized. The risk register will be reviewed and updated on a regular basis.

3.10 Reviews

The risks facing the Authority are likely to change periodically owing to the dynamic operating environment. The risk management policy and strategy shall be reviewed as is appropriate to reflect these changes. The risk management reviews will involve identification of new risks, changes in existing risks and the identification of risks that are no longer relevant to the KoTDA.

Review of the RMP shall consider the following factors:

- Government Policy and/or circulars.
- Changes in the strategic objectives of the KoTDA.
- Dynamics in the business environment.

- Benchmarking policy to industry; and
- Other internal and external factors.

The review process will be undertaken through a consultative process involving departments, senior management team, Board Audit Committee and the Board of Directors.

4 RISK MANAGEMENT POLICY FRAMEWORK

The Risk Management Framework represents the mechanisms and structures that will be used to oversee and manage the risks. The framework is developed along four building blocks, namely:

i. Culture and rules.
ii. Structure and process.
iii. Resources and Capabilities; and
iv. Tools and Techniques

For each of the foregoing building blocks, specific elements are outlined, which are aligned to KoTDA's strategic objectives.

Table 6: RMP Building Blocks

Building Blocks	**Elements**
Culture & Rules	• Commitment & support from Board of Directors, CEO & Management • Positive organizational culture of honesty & good ethical behavior • Definition of risk appetite • Effective management oversight including finance and audit committees
Structure & Process	• Reliable institutional risk identification and mitigation process • Strong budgetary, accounting & internal control systems • Policies and processes that promote transparency, accountability, integrity & fairness and delivers value for money • Inbuilt fraud and corruption prevention mechanisms • Effective procurement unit • Effective monitoring & evaluation
Resources & Capabilities	• Effective Communication • Training • Adequate, qualified, competent & motivated personnel well versed with risks in their functional areas
Tools & Techniques	• Business Continuity plan • Reporting procedures of risk information • Adequate social accountability mechanisms • Risk indicators profile • Reward/recognition measures • Efficient & sound record management systems & processes on creation, use & disposal of records

The delivery of the risk policy will be through the following levels:

- The Board of Directors
- Board Audit & Risk Committee
- Management Committee
- Internal Audit& Assurance Division
- Departmental and Divisional Heads

- Risk Champions
- Employees

4.1 Risk Management Structure

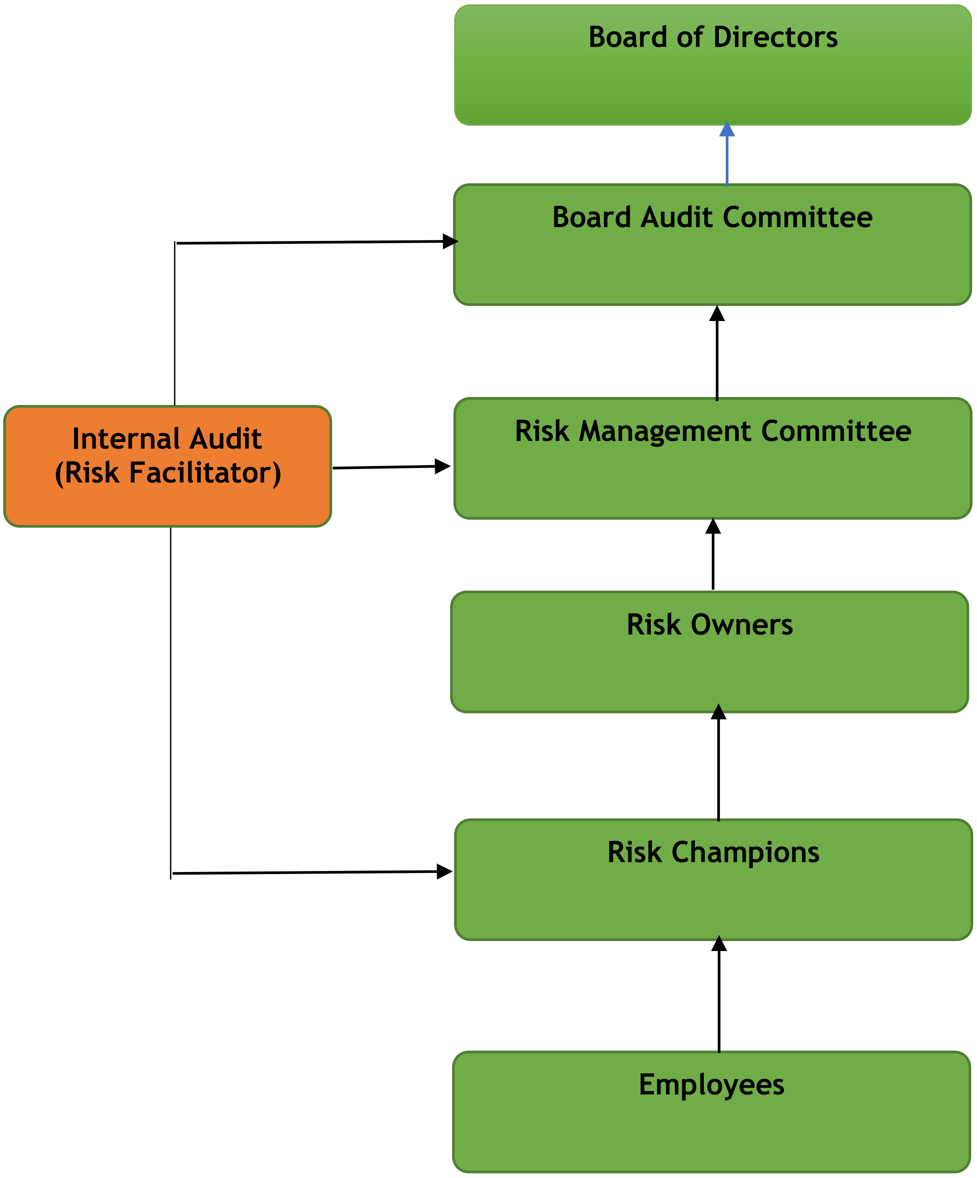


Figure 4.1-1: Risk Management Structure

4.2 Risk Management Standards

Ref.	Standard	Responsibility	Frequency
4.2.1.1	**Board Responsibilities**		
01	Approve the Risk Management Policy Framework	CEO	Once
02	Delegate to Management the responsibility of implementing the Risk Management Plan	CEO	Once
03	The Risk Management Committee will review Risk Management progress on quarterly basis.	CEO	Quarterly
04	Review an Internal Audit written assessment of the effectiveness of system of internal controls and risk management.	CEO	Annually
4.2.1.2	**Reporting Responsibilities**		
01	Presentation of Risk Management reports to the Board	Chair A&RC	Quarterly
02	Presentation of the Risk Management report to the Audit & Risk Committee	Manager, Internal Audit & Assurance	Quarterly

Ref.	Standard	Responsibility	Frequency
03	Submission of a risk management report to the Board Audit & Risk Committee. The report will focus on the following: ➢ Significant risk in a Risk Heat Map (Extreme and High risks) ➢ Management mitigation plan to address the significant risks. ➢ Any risk developments or losses ➢ The progress in the implementation of action plans recommended by the risk function. ➢ Any emerging risks	Manager, Internal Audit & Assurance	Quarterly
04	Each department will submit a Risk Management Report to the RMC once every quarter. This submission will focus on the following: ➢ Significant risk in a Risk Heat Map (Extreme and High risks). ➢ Departmental Management mitigation plan to address the risks identified. ➢ Any emerging risks	Heads of departments	Quarterly
05	Each Risk Champion will submit a Risk Management Report to the Departmental Risk Management Meeting once every Quarter. This submission will focus on the following: ➢ Departmental risk register ➢ Any emerging risks	Heads of Departments	Quarterly

Ref.	Standard	Responsibility	Frequency
06	Each risk champion will make a submission to the Risk Champions team detailing: ➢ Any emerging risks ➢ Incidences of control breakdown ➢ Risk events that have occurred in the month	Risk champions	Quarterly
07	Annual risk assessment and updating of the Departmental risk registers	Risk Champions	Annually
4.2.1.3 **Control Responsibilities**			
01	The Board will consider Management's Report concerning the effectiveness of internal controls at least once a year.	Audit & Risk Committee Chairperson	Annually
02	The HIA will report to the Board Audit & Risk Committee regarding the performance of internal controls for those risks in the risk registers.	HIA	Quarterly
03	Heads of Departments will report to the RMC regarding the performance of internal controls for those risks in the departmental risk registers.	Heads of departments	Quarterly
04	All departmental risk registers will contain action plans for improving risk controls and risk interventions. Each forum will review progress made with these action plans.	All	As scheduled

Ref.	Standard	Responsibility	Frequency
4.2.1.4	**Governance Responsibilities**		
01	Each risk will have a nominated owner who will be responsible for the following: ➢ Updating the risk information ➢ Providing assurance regarding the risk's controls ➢ Coordinating the implementation of action plans for the risk ➢ Reporting on any developments regarding the risk	Departmental Managers	As scheduled
02	The Internal Audit function will use the outputs of risk assessments to compile its audit coverage plan and investigate the effectiveness of risk controls.	Internal Audit & Assurance Division	Annually
03	The internal audit function will formally review the effectiveness of the KoTDA's risk management processes once a year.	Internal Audit & Assurance Division	Annually

Table 4-1: Risk Management Standards

4.3 Roles and responsibilities

4.3.1 Role of the Board

The Board is accountable for risk management within KoTDA. Its responsibilities are stated as follows:

The Board is responsible for the identification of major risks, the entire process of risk management, as well as for forming its own opinion about the effectiveness of the process. Management is accountable to the Board for designing, implementing, and monitoring the process of Risk Management and integrating it into the day-to-day activities of KoTDA.

The Board must identify and fully appreciate the organisational risk issues affecting the ability of KoTDA to achieve its strategic objectives.

The Board must be assured that appropriate systems are in place to help manage the identified risks, measure their impact, and proactively manage it, so that KoTDA's mandate and reputation are suitably protected.

Each member of the Board must understand his accountability for Risk Management within KoTDA. The induction of Directors includes an outline of Director's responsibilities in this regard. Although the Board may choose to nominate one Director as the coordinator of risk management reporting requirements, all Directors have accountability for Risk Management within KoTDA.

The Board will provide stakeholders with assurance that key risks are properly identified, assessed, mitigated, and monitored.

The Board must receive credible and accurate information regarding the Risk Management processes within KoTDA to give the necessary assurance to stakeholders. The reports from the Management committee must provide an evaluation of the performance of risk management and internal control. The Board must make sure that the various processes of risk management cover the entire spectrum of organisational risk. The assurance process includes statements regarding the appropriateness of KoTDA's risk/reward trade-off.

Because of the fluid nature of risk in KoTDA, it is imperative that risk is confronted in a systematic and structured manner. In our complex environment, where there are numerous strategic, operational, and financial risks, it is vital that the assessment of risk is undertaken in a formalized manner. The Board will provide stakeholders with the assurance that management has a pre-emptive approach to risk.

The Board will maintain a formal risk policy for KoTDA.

It is appreciated that stakeholders need to understand the Board's standpoint on risk. The Board will therefore maintain KoTDA's formal risk policy which decrees KoTDA's approach to risk. The risk policy statement underpins the development of KoTDA's ERM process. This policy can be used as a reference point in matters of dispute and uncertainty.

The Board will formally evaluate the effectiveness of KoTDA's risk management process once a year.

The Board will evaluate the effectiveness of KoTDA's risk management processes. Success with Risk Management will be evaluated from the Risk Management Committee reports and implementation of the mitigation measures, KoTDA's risk culture, unexpected losses, internal control effectiveness, and organisational success. The Board's evaluations will be formally recorded in the minutes of Board meetings.

It is recognized that risk management has evolved into a complex management discipline. The Board's evaluation of risk management, therefore, will be supplemented by an independent review to be performed by KoTDA's Internal Audit and Assurance Division. The annual review will be undertaken by qualified personnel who are able to review all aspects of risk management.

The Board will confirm that the risk management process is accurately aligned to the strategy and performance objectives of KoTDA.

The Board will help ensure that the risk management processes address risk in a balanced way, giving due attention to all types of risk. The Board will evaluate whether appropriate resources are being applied to the management of strategic risks, reputation, financial, operational, regulatory, and health, safety and environmental related risks. The Board will evaluate whether risk management processes are aligned to the strategic and performance objectives of KoTDA. A balanced perspective of risk and risk management is required in proportion to the weighting of potential risk impact across KoTDA. Directors must help ensure that there is a future-looking orientation included in the consideration of risk.

The Board Audit & Risk Committee will monitor KoTDA's risk management processes.

The Board Audit & Risk Committee shall be responsible for addressing the corporate governance requirements of risk management and monitoring KoTDA's performance with respect to risk management. The Board Audit & Risk Committee has a defined mandate and terms of reference which cover the following aspects:

- Constitution
- Membership
- KoTDA
- Terms of reference
- Meetings

The Committee shall meet at least four times a year.

4.3.2 Chief Executive Officer (CEO)

The overall responsibility for developing, coordinating, implementing, and assessing the effectiveness of the RMP is delegated to the CEO by the Board of Directors. The CEO shall also perform the following functions under this policy:

- Guide the policy implementation process through the issuance of appropriate circulars.
- Define appropriate institutional structures for effective implementation of the RMP;
- Appoint the Risk Management Committee.

4.3.3 Role of Senior Management

KoTDA's Senior Management consists of KoTDA's CEO, Heads of Departments and heads of Divisions. They have the primary responsibility of operating the KoTDA in a manner that is consistent within the parameters established by the Board.

4.3.4 Risk Management Committee

The Management Committee will be consisting of the Senior Management team. The Committee will be given the mandate of overseeing the risk management activities on behalf of the Board. The Management Committee's primary goals and objectives are to:

- Ensure strong internal controls and a safe working environment.
- Monitor the implementation of the Risk Management Policy Framework
- Approve or modify all entries in KoTDA's risk register
- Monitor emerging risks.
- Approve or modify KoTDA's Risk Management Training Program.
- Direct actions to be taken in relation to annual risk management internal audit reports.
- In consultation with the CEO, develop risk action plans for all risks assessed as high or above and set the timeframe for their implementation; and
- Approve and monitor the risk action plans once developed.

The Risk Management Committee shall consist of the following:

- The CEO as the Chair
- Direct reports to the CEO
- Head Internal Audit as the Secretary
- Any other Member of the management that CEO, in Consultation with the function in charge of Risk Management, may co-opt

4.3.5 Role of Internal Audit Function

The Internal Audit's primary roles are as follows:

- Develop ERM policies, including defining roles and responsibilities.
- Promoting ERM competence and awareness throughout KoTDA, including facilitating development of technical ERM expertise and helping managers align risk responses with KoTDA's risk capacity and developing appropriate controls.
- Guiding integration of ERM with other organizational planning and management activities.
- Establishing a common risk management language that includes common measures around likelihood and impact, and common risk categories.
- Facilitating manager's development of reporting protocols, including quantitative and qualitative thresholds, and monitoring the reporting process.
- Work with the Board Audit Committee in ensuring the identification and prioritization of risks.
- Bring to the attention of management any shared risks not owned by process owners.

- Assist in ensuring that key risks are being managed appropriately by management;
- Ensure updated assessments are performed when significant changes occur;
- Monitor that risk mitigation efforts are progressing as required;
- Monitor implementation of action plans;
- Proactively identify emerging risks;
- Reporting to the CEO on progress of implementation and recommending actions as required;
- Consolidating the reports received from the risk champions for presentation to the Board Risk Committee and the management committee; and
- Be the Secretary to the Management Committee and Board Risk Committee

4.3.6 Departments and Divisions

The day-to-day responsibility for implementation of the Risk Management Policy is delegated to Departmental Heads as '*Risk Owners'*. Section heads shall manage risks in their respective sections on day to day basis and facilitate departmental risk reporting.

Heads of Departments shall convene Departmental/Section risk management meetings for purposes of identifying, analyzing, and managing risks as stipulated in this policy document.

The purpose of Departmental/Section risk management meetings will be to provide the Management, assurance that the major business risks are being identified and consistently assessed and that measures are in place to address risks. The Heads of Department will be responsible for:

- Implementation of the principles, actions and requirements of the Risk Policy and regular review of progress against action plans for all risk items;
- Regular review of the current list of risk items and making any necessary changes to the risk status of individual items;
- Regular reporting of the status of risks;
- Appraisal of 'risk owners' actions taken to manage risk and correction of substandard performance;
- Internal compliance and control systems for the implementation of the Risk Policy; and
- Assist in carrying out the internal risk audit as per stipulated guidelines and in compliance with regulatory requirements and best practice.

The HODs will work with the risk champions to fulfill their mandate. The risk champions will have a delegated responsibility during the ERM process, but the ultimate responsibility still lies with the HODs.

4.3.7 Risk Champions, Employees and Other Project Staff

All KOTDA staff will be fully involved and adequately informed on the risks associated with their day to day activities and their responsibilities. Through training and sound management standards and procedures, the Board and Management will develop a disciplined and constructive control environment in which all employees understand their roles and obligations.

The Risk Champions will coordinate their respective process areas through the entire ERM process.

Functions of the employees will include:

- Risk identification and reporting
- Risk control
- Compliance to procedures
- Implementation of agreed upon improvement action plans.

5 ENTERPRISE RISK MANAGEMENT PROCEDURES

The scope of the ERM program at KoTDA is enterprise wide. Accordingly, this policy manual is applicable to all processes including:

- Physical Planning, Design and Compliance.
- Construction Operations and Management
- Business Development and Innovation
- Corporate Research and Strategy
- Corporate Services
- Corporation Secretary & Legal Services
- Supply Chain Management
- Internal Audit & Assurance

Primary Users of this Procedures Manual

The primary users of this manual are those within KOTDA, who have responsibility for any aspect of ERM, including:

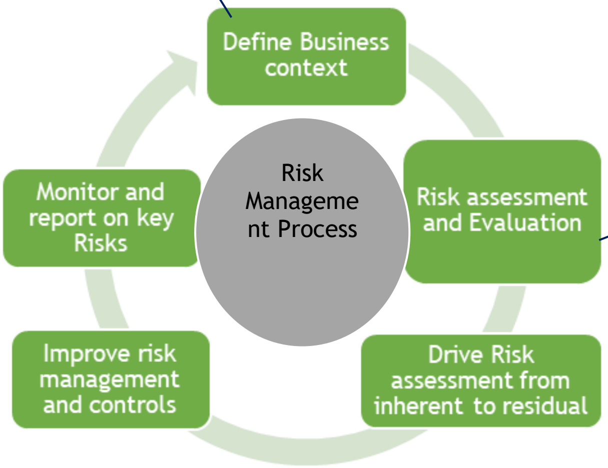
- Developing and/or modifying key KoTDA processes.
- Identifying, assessing, and analysing risks related to both new and existing KoTDA processes and activities.
- Risk reporting and monitoring.
- Internal controls assessment and testing.

5.1 ERM Process Overview

The following diagrams provide an overview of KoTDA's ERM process.

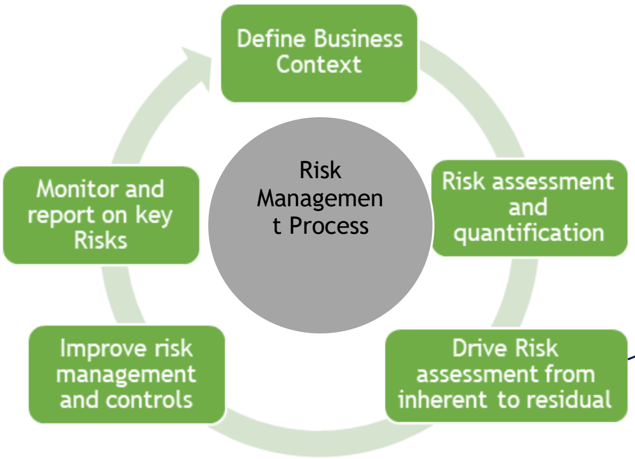
Step 1. Define the business context

- Identify the organization's departments, sections and processes to be reviewed and assessed.
- Identify key contact persons and risk owners.
- Obtain or develop documentation of critical organization processes.
- Obtain an understanding of the strategic objectives of the organization as a whole.
- Obtain an understanding of key processes and respective process objectives and the organization context in which such processes are performed and conducted.
- Prepare to perform risk identification and assessment.


Define Business context
Risk assessment and Evaluation
Drive Risk assessment from inherent to residual
Improve risk management and controls
Monitor and report on key Risks
Risk Manageme nt Process

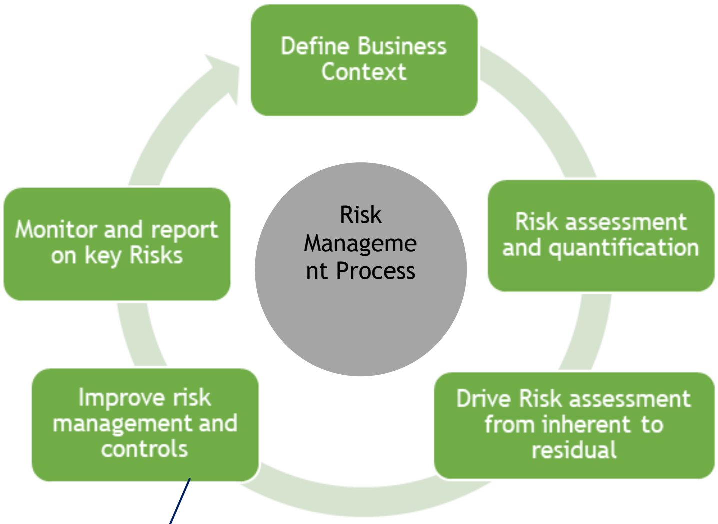
Step 2. Identify, assess and quantify key risks

- Conduct structured individual/group interviews and/or small group workshops (per department, section or process) to identify key risks in the organization processes identified in step #1.
- Identify the risks in the organization processes that would affect the achievement of process level objectives.
- Perform a root cause analysis of the risks identified
- Identify the best point of intervention among the causes identified above.
- Identify the qualitative and quantitative consequences for the occurrence of the identified risk.
- Apply NDMA's standardized assessment methodology to assess identified **gross risks** in terms of likelihood and impact.
- Assess the **gross risks** assessment results with risk owners and other key stakeholders.


Define Business Context
Risk assessment and quantification
Drive Risk assessment from inherent to residual
Improve risk management and controls
Monitor and report on key Risks
Risk Managemen t Process

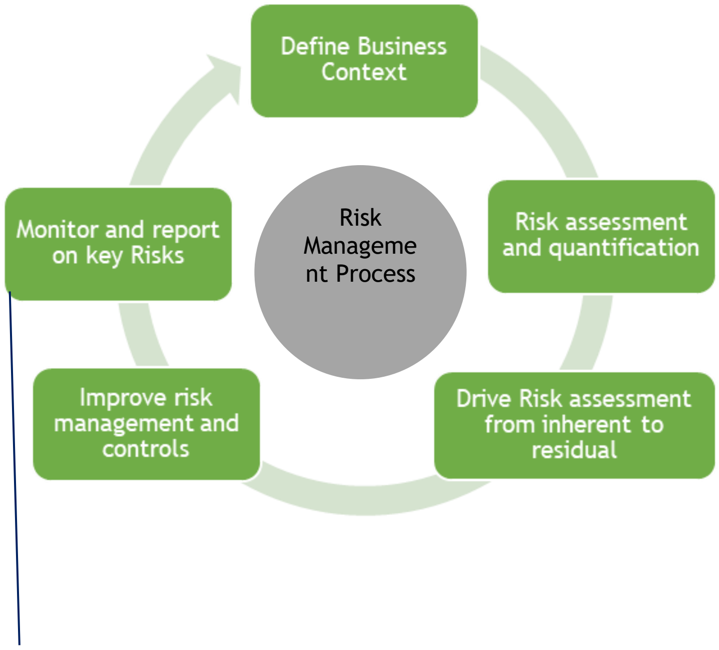
Step 3. Drive risk assessment from gross to residual risk

- For each process, assess the process and related controls design.
- Identify key controls and mitigations relative to identified gross risks.
- Assess and test the effectiveness of controls and mitigation.
- Assess identified risk at the residual risk level.
- Rank residual risk.
- Identify actions to respond to risk occurrence and manage risk consequence.


Define Business Context
Risk assessment and quantification
Drive Risk assessment from inherent to residual
Improve risk management and controls
Monitor and report on key Risks
Risk Manageme nt Process

Step 4: Improve risk management and controls processes

- Identify risks requiring monitoring.
- Establish key risk indicators.
- Establish the tolerance limits for each indicator.
- Monitor any deviation from the tolerance limits.
- In case any deviation is noted, identify improvement action plans to ensure that the tolerance limits are not exceeded.
- Develop and prepare standard and ad hoc reports for submission to the board audit committee and the management committee in accordance with agreed upon procedures, guidelines and escalation protocols.


Define Business Context
Risk assessment and quantification
Drive Risk assessment from inherent to residual
Improve risk management and controls
Monitor and report on key Risks
Risk Manageme nt Process

Step 5. Monitor and report on key risks

- Assess controls for each process and risk identified.
- Identify and recommend steps to be taken to reduce risks in order to improve risk management processes, controls and activities.
- Remediate identified control and mitigation gaps identified.

Figure 5.1-1: KoTDA's ERM Process

5.1.1 Step 1: Define the organization context

The risk assessment process at KOTDA begins by identifying the departments, sections and processes that will be included in the risk assessment process. This determination, designed to focus attention on areas of greatest potential risk, is made by consideration of factors such as the following:

- Criticality of the departments, sections and processes to KoTDA's core organization, strategy and objectives;
- Scale of operational activity;
- Regulatory and/or legal requirements; and
- The significance of any changes to the organization, processes and/or systems.

Key Task	Responsibility
A. Identify the KoTDA's departments, sections, and processes to be reviewed and assessed. • Hold initial briefing meeting: • Agree on assessment scope in terms of departments, sections and processes. • Agree on the process to be followed during the risk assessment. • Provide overview of the process to everyone within the process who will be participating in the risk assessment process. • Emphasize the importance of this process and the priority given to it by senior management.	Internal Audit HODs Risk Champions
B. Identify key contact persons and risk owners. • The HOD appoints a risk champion(s) for each process. The Internal Audit supports the risk champion during the risk assessment process.	HOD Internal Audit
C. Obtain or develop documentation of critical organization processes. • **Perform background research**: Review the following documents or information: - Departmental goals and objectives. - Audit and compliance reports for the department. - Internal management reports. - Risk committees' information. • **Draft a process overview**: Utilize existing process documents to determine the following: - Process objectives. - Departmental chart.	HOD Risk Champions

- Overview of key tasks and activities.	
D. Obtain an understanding of the strategic objectives of the KoTDA as a whole. • Review and understand the strategic objectives of KOTDA. • Identify the strategic objectives that relate to the process under assessment. • Provide feedback as to whether the process under review is in support of the achievement of the strategic objectives identified to relate to that process.	Risk champions Internal Audit
E. Prepare to perform risk identification and assessment. • **Prepare the risk context document:** This step develops the content or reporting that is designed to assist the HOD and his or her staff during the next stage of the risk assessment process. The contents should include: - Departmental overview (process maps and descriptions etc.). - Historical losses summary that may point to potential risks. - Organizational business continuity planning status. - Summary of expected changes over the coming 12 months. - Summary of open audit or compliance issues. - Key external and internal stakeholders. - Key dependencies (services that the department relies on to deliver its mandate).	Risk champion HOD Internal Audit

Table 5-1: Tasks in Defining Organization Context

***Note**: Involvement in the risk identification and assessment process should be preceded by training to help ensure that individuals leading and/or participating in the risk management program activities are sufficiently educated to successfully fulfil their duties and responsibilities.*

5.1.2 Step 2: Identify, assess, quantify and aggregate key risks

Departmental self-assessment of risks is an important aspect of the risk management framework at KOTDA. Each of the departments will assess the results of their respective risk assessments, including both the gross and residual levels of risk. The departments through the risk champions will also be responsible for the mitigation of unacceptable levels of residual risk identified during the risk assessment process.

The risk assessment is a tool to identify and prioritize gross and residual risks in each department. On at least a quarterly basis, each respective HOD with the assistance of the risk champions will complete the following tasks:

Key Task	Responsibility
A. Conduct structured individual/group interviews and/or small group workshops (per department, section or process) to identify key risks in the KoTDA processes identified in step #1. **Hold risk assessment meetings:** The risk champion with assistance from the Internal Audit will conduct facilitated discussions with the group identified above to identify the key risks relative to core activities and processes within his/her department. The risk assessment meeting could be conducted in a workshop format, smaller meetings or individual one on one session. In any case, participants will be expected to prepare in advance and review all materials prior to the meeting. The risk champions will distribute risk assessment materials in advance to all participants. Meeting objectives are to: • Identify/assess key risks. • Estimate potential impact. • Estimate likelihood of occurrence. • Develop an overall gross risk assessment for each identified risk.	HOD Risk champions Internal Audit
B. Identify gross risks in the organization processes. The risk champions and HODs will collaborate to identify key risks that impact its operations and core activities. This includes identifying and documenting significant **existing and emerging gross risks** in the department's processes.	HOD Risk champions Internal Audit
C. Perform a root-cause analysis of the risks identified. • Iteratively ask **Why** the risk occurred and write the answer down	HOD Risk champions Internal Audit
D. Identify the best point of intervention from the cause identified above Any improvement action plans should be based on the best	HOD Risk champions

point of intervention. This is because this is the point at which the most benefit is obtained.	Internal Audit
E. Identify the qualitative and quantitative consequences for the occurrence of the identified risk. Quantitative consequences are any measurable consequences. Qualitative consequences are any non-measurable consequences.	HOD Risk champions Internal Audit
F. Apply KoTDA's standardized assessment methodology to assess identified gross risks in terms of likelihood and impact. The criteria for this assessment has been described in the ERM policy framework.	HOD Risk champions Internal Audit
G. Assess the gross risk assessment results with risk owners and other key stakeholders. • When all risks have been assessed, each department needs to challenge the thoroughness of risks identified for all appropriate processes within KOTDA (for instance, if no "legal" risks have been noted, challenge the need to identify risks fitting that process). This allows for thorough risk identification. • Distribute risk identification and analysis register to the HOD for review. • Hold follow-up meeting as necessary. • Help ensure all pertinent risks have been identified. • Identify enterprise-level risks that will require centralized or management risk committee attention.	HOD Risk champions Internal Audit
H. Rank risks at the gross risk level. • Utilize the magnitude of impact and probability of occurrence definitions above to assess each risk identified. The impact and probability should be set first at a "gross risk" level, as if no controls were in place regarding these risk items.	HOD Risk champions Internal Audit

Table 5-2: Key Tasks in Risk Assessment

5.1.3 Step 3: Drive risk assessments from gross risk to residual risk.

Based on information contained in the departmental risk profile, an assessment should take place to identify factors that determine the need for and the type and form of any immediate risk mitigation and control actions. Alternative risk treatments should be identified and reviewed with the Internal Audit and potentially the management risk committee.

The steps below summarize the main tasks and action required:

Key task	Responsibility
A. For each process, assess the process and related controls design. • Identify significant risk exposures from the risk profile. These items may result in occurrence of risk due to lack of or deficient controls in place. They may also result from a higher level of gross risk given the nature of the departmental activity.	Risk champions Internal Audit
B. Identify key controls and mitigation relative to identified gross risk. • For each risk identified, the Internal Audit, the risk champion and respective HOD will collaborate to identify key controls and/or mitigating actions/factors/processes in place to control, reduce, transfer or otherwise address the risk as appropriate.	Risk champions Internal Audit HOD
C. Assess and test the effectiveness of controls and mitigation. • A control assessment can be made utilizing the definitions indicated in the ERM policy framework. For example, if risk control processes are in place but are not all functioning effectively and residual risk remains too high, the control assessment would be "weak". • The controls assessment is made relative to the level of gross risk. The assessment will consider loss history; indicate the effectiveness and trend of key risk indicators and audit ratings for the department. • If the controls are assessed as "weak", the issues should be elevated to the HOD, risk champion and Internal Audit to take appropriate steps to enhance the controls. • The risk champion should document the risks and corresponding action plans resulting from this process and provide for ongoing tracking and monitoring. • The Internal Audit and the risk champion will meet quarterly with each HOD to develop: - The list of each KoTDA' key risks or any changes thereto. - An assessment of the controls to mitigate these risks.	Risk champions Internal Audit

Key task	**Responsibility**
- The status of plans to close any control gaps.	
D. Assess identified risk at the **residual risk** level.	Risk champions Internal Audit
E. Rank overall residual risk.	Risk champions Internal Audit
F. Aggregate residual risk for the entire organization. The Internal Audit will review the composite risk profiles for all the departments and prepare an aggregated risk profile for KOTDA. The Internal Audit will present such composite risk profile to the management risk committee and the board risk committee.	Risk champions Internal Audit

Table 5-3: Key task in review of controls to determine residual risk

5.1.4 Step 4: Improve risk management and control processes

Identify and recommend steps to be taken to help reduce risks to an acceptable level and improve risk management processes, controls and activities.

Once risks have been identified and assessed at the gross level, the risk champion with assistance from the Internal Audit will work with management to identify the controls and other mitigating actions, in place to avoid, control, transfer or otherwise reduce the risk to an acceptable level in accordance with the risk appetite and tolerance of KOTDA.

Key task	Responsibility
A. Assess controls for each process and risk identified.	Risk champion Internal Audit
B. Identify and recommend steps to be taken to reduce risks in order to improve risk management processes, controls and activities. • Identify control gaps and remedial action. Controls that do not mitigate or reduce the level of risk should be reviewed and a remediation plan established. This should include: - Consider residual risk after applying controls. - Assign an individual risk champion from the department responsible for remediation. - Establish a course of action and timeline for remediation. - Review and approval by the Internal Audit and HOD. - Internal Audit to monitor using issue tracking database. • Identify risk reduction options. Consider how to reduce the potential impact or likelihood of occurrence. Document course of action and provide to Internal Audit. Examples include: - Contingency planning. - Increase clarity and consistency of process documentation. - Modify control by e.g. requiring approval from HOD before execution of a task. - Transfer risk (insurance or outsource).	Risk champion Internal Audit
C. Remediate control gaps identified.	Risk champion Internal Audit

Table 5-4: Key Tasks to improves risk management and control processes

6 REPORTING AND MONITORING PROCEDURES

Critical risks with greatest impact and highest likelihood should be measured, monitored, and reported.

The objectives of measuring and monitoring are as follows:

- Identify which risks should be measured and monitored. This will help ensure that all material risks are addressed.
- Develop Key Risk Indicators (KRIs) which are consistent with the complexity and diversity of the activity.
- Establish tolerance limits for KRIs identified.
- Compare actual results versus expected performance and identify any deviation from the defined tolerance limits.
- Assess level of risk posed, given risk tolerance determined.
- Determine that KRI assumptions and data sources are tested for reliability.
- Timely reporting of risk monitoring activities.

Key questions to be addressed by monitoring and reporting risk:

- How do you measure risk management performance?
- Do you receive summary risk management information and can you use this to challenge KoTDA assumptions?
- How is risk information consolidated and presented and does this provide consistent visibility of the key risks of KOTDA and how they are managed?
- How do you get assurance that risk management is applied in practice in the departments in line with the requirements of KOTDA?
- What is the nature and frequency of risk management information that should be provided to KOTDA, the board audit committee and management risk committee?
- Who prepares this information?
- How would you rate the information you have available to monitor risk exposures of the organisation?
- Explain rationale for ratings. If only adequate or poor, identify improvement priorities.

6.1 Reporting and Monitoring Process Overview

Key task	Responsibility
A. Establish metrics (KRI) and tolerance limits. • Set key measures. Identify KRI to monitor the risk exposure. • Continuous monitoring. • Monitor until risk exposure has been mitigated in accordance with the board and management defined risk appetite and tolerances.	HOD Risk champions Internal Audit
B. Develop and prepare standard reports for submission to the board risk committee and the management risk committee in accordance with the reporting standards defined in the ERM framework.	HOD Risk champions Internal Audit

Table 6-1: Key Tasks in Reporting & monitoring

6.2 Define the KRIs

For each risk or control to be monitored, a KRI should be identified.

KRIs are typically focused on measurable events which are categorized into:

- Operational indicators
- Perception indicators
- Key performance indicators

Workshops can be conducted to assess KRIs and identify the information required to measure them.

Task	Responsibility	Action step
Establish KRIs		
Review existing reports.	Risk champion/Risk owner	• Obtain existing scorecards and or other reports used by management to track operational performance. • May request these during data gathering.
Determine appropriate KRI for risks to be monitored.	Risk champion/Risk owner	• Determine if appropriate reporting exists. • Establish new reporting if appropriate measure does not exist.
Assess measurement	Risk champion/Risk owner	• Discuss with HOD and the Internal

Task	Responsibility	Action step
selection (establish KRI).		Audit key risks and related KRIs. - Obtain agreement as to measurement criteria.

Table 6-2: Key Tasks in Definition of Key Risk Indicators

6.3 Establish tolerance limits for each KRI

For each KRI a tolerance limit should be established to set the tolerance for escalation and actions required.

Task	Responsibility	Action Step
Establish measurement criteria		
Establish expectation for KRI tolerance limits.	Risk champion/Risk owner	- Review historical trends and budget information. - Review industry trends if available. - Set expected tolerance limits.
Assess expected tolerance limits.	Risk champion/ Risk owner/ Internal Audit	- Review historical trends, budgets/strategic plans and any industry data that has been collected. - Obtain agreement on the adequacy and appropriateness of the tolerance limits.

Table 6-3: Keys Tasks in Establishment of KRIs

6.4 Risk Management Reporting

6.4.1 Escalation procedures

- Based on KRIs and tolerance limits established, escalation parameters will need to be put in place for items requiring escalation within the risk management structure.
- Additionally, for assessing risk trends, a baseline needs to be established to permit a basis for assessing changes in risks.

Characteristics of issues which would require escalation
- Departments with KRIs out of benchmarked tolerance limits. - Areas where a hard cash loss over an established threshold has occurred.

- Significant regulatory findings. - Areas with delinquent control remediation plans. - Any early-warning trend signifying a change in risk profile. - Areas where trends indicate a quickly changing environment with systems, people, organization processes, or regulatory environment.

Table 6-4: Issues requiring escalation

6.4.2 Preparation of the initial reports

After key measurement criteria has been established the risk champions and Internal Audit will need to prepare a report for the Risk Management Committee. It is important that KRIs are compared to the expected tolerance limits and that key trends are identified and summarized at this step.

Task	Responsibility	Action step
Preparation of risk reports by risk champions		
Assemble raw data and summarize.	Risk champion/ risk owner	- Assemble KRIs. - Assess KRIs. - Analyse KRIs comparing actual KRIs to tolerance limits. - Interpret trend information versus last quarter and previous year.
Prepare report.	Risk champion/ risk owner	- Summarize findings. - Submit findings to the Internal Audit.

Table 6-5: Preparation of Risk Reports

6.4.3 Preparation of Board Committee reports

After the risk champions have completed all respective reports, the Internal Audit will prepare the reports for the Risk Management Committee, the Board Audit & Risk Committee and the Board.

Task	Responsibility	Action step
Prepare report for management risk committee		
Prepare quarterly management risk committee report.	Internal Audit	- Assemble data submitted by risk champions. - Summarize findings in a draft report. - Review performances of KRIs compared to the established tolerance limits and

Task	Responsibility	Action step
		identify significant trends. • Review trends for emerging risks. • Summarize findings. • Compile the bimonthly management risk committee report. • Present report at the Management Risk Committee meeting.
Prepare quarterly Board Audit & Risk Committee report.	Internal Audit	• Compile the Board Risk Committee quarterly report incorporating the details of the previous quarter management risk committee reports and any updates since. • Present the draft Board Risk Committee report to the Risk Management Committee. • Incorporate CEO's comments and finalize the report. • Present final report to the board risk committee.
Prepare annual report to the Board.	Internal Audit	• The report presented to the Board on an annual basis will be based on the quarterly Board Audit & Risk Committee reports presented during that financial year.

Table 6-6: Reporting to the Board

7 REVIEW OF THE POLICY

This policy shall be reviewed after three years, or as may be deemed necessary as a result of the changes in the environment KoTDA operates in. Any need for change shall be reported to the CEO for approval.

8 EFFECTIVE DATE

This policy comes into effect on this _____________ day of ____________________ 2020.

Eng. John Tanui MBS
CHIEF EXECUTIVE OFFICER

A Appendix 1 – Glossary

Term	Definition
Assurance	An evaluated opinion based on evidence gained from a review that risks are under control (errors are prevented, detected and corrected in an efficient and effective manner).
BA&RC	This is the Board Audit & Risk Committee/ Audit Committee.
Controls	Existing processes, devices, practices or other actions that act to minimize negative risks or enhance positive opportunities.
Corporate risk register	The documented and prioritized overall assessment of a range of risks faced by the KoTDA.
ERM	ERM is an entity wide process for managing the myriad of risks KOTDA faces.
Exposure	The consequences as a combination of impact and likelihood, which may be experienced by the KoTDA if a specific risk is realized.
Gross risk/ Inherent risk	The initial assessment of risk without controls.
Impact/magnitude of occurrence	Significance of a particular risk to KOTDA. The significance of a particular risk can range from minor to major. Magnitude of impact is determined with respect to KoTDA's risk appetite, risk capacity, and objectives.
KRI's (Key Risk Indicators)	A measure used in risk management to indicate occurrence of risk.
Likelihood of occurrence	Probability that a particular risk will occur. These probabilities range from unlikely to likely.
Objectives	Description in measurable terms, usually by KPI of what must be accomplished to reach the goals.
Process	Structured set of activities within an entity, designed to produce a specified output.
Process owners	Person or group of people who are responsible for managing a business process. Managing a business process includes taking responsibility to meet KoTDA's strategic objectives relating to the process.
Residual risk	The risk remaining after considering the effectiveness of

Term	Definition
	management's risk responses/controls.
Risk	Anything that could affect KOTDA as it pursues its objectives.
Risk capacity	The level of risk KOTDA is not prepared to exceed or is not financially capable of exceeding. Risk capacity may be defined as: • A financial measure. • By the level of variability of results KOTDA can survive. • The maximum loss KOTDA can, or is willing, to tolerate, or any other quantifiable measure KOTDA chooses.
Risk appetite	The level of risk which KOTDA is prepared to tolerate in its organisation and within which management must operate.
Risk assessment	Overall process of identifying, analyzing, and evaluating risks.
Risk categories	The means by which KOTDA determines how it will group risks together. The grouping of risks with similar characteristics is used in establishing KOTDA risk portfolio.
Risk function	A reporting line in KOTDA with responsibility to co-ordinate the management and reporting of risk. It is led by Internal Audit.
Risk identification	The process of determining the risks The KoTDA is exposed to.
Risk management	The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects of risks.
Risk mitigation strategies	The objectives and associated activities which management undertakes to reduce the level of risk related to management processes.
Risk policy	Policies and procedures necessary to embed risk management within KoTDA's culture.
Risk portfolio	Association of risks into categories based on known or likely interdependences.
Risk profile	Identification and listing of risks, typically in order of highest to lowest based on a qualitative or quantitative

Term	Definition
	criterion approved by management.
Risk register	A documented record of each risk identified. It specifies: - A description of the risk. - Its causes and its rating. - An outline of the existing controls. - An assessment of the consequences of the risk should it occur. - The likelihood of the consequence occurring, given the controls. - A risk rating; and an overall priority for the risk.
Risk response	Any action taken by management to enhance the likelihood that established objectives and goals will be achieved by mitigating risks.
Risk strategy	The way in which the KoTDA aligns identified risks to the objectives and strategies of the KoTDA. Aligning KoTDA's risk strategy to business strategy requires maintaining relevant and timely information on KoTDA's risk portfolio.
Strategy	Management's formalized strategy which outlines how KoTDA plans to achieve its objectives.
The Board	The board of directors of KoTDA.

B Appendix 2 – Risk register template

Risk register	KOTDA
Department/Division/Function/Business Unit	
Risk Champion	
Period	

Ref No	Departmental/ Project Objectives		KPIs

Objective Ref	Risk	Root Cause	Gross Risk Assessment			Existing Controls	Control Effectiveness	Residual Risk Assessment			Improvement Action Plans	Person Responsible/ Risk Owner	Timelines
			Likelihood	Impact	Overall			Likelihood	Impact	Overall			