



**KENYA PLANT HEALTH INSPECTORATE
SERVICE
ENTERPRISE RISK MANAGEMENT POLICY**

FEBRUARY 2023

FOREWORD

Kenya Plant Health Inspectorate Services (KEPHIS) is a regulatory body, mandated to undertake quality assurance services of agriculture inputs, plant variety protection and plant health. KEPHIS has identified risk units within its operations. These units are the Directorate of Phytosanitary & Biosecurity, Directorate of Seed Certification & Plant Variety Protection, Directorate of Corporate Services, Directorate of Laboratory Services, and Directorate of Planning & Strategy, Corporate Secretary & Legal Services, Internal Audit & Risk, and Supply Chain Management functions.

The management recognizes the importance of having a positive risk culture-based organization. The development of this policy is one step toward ensuring that KEPHIS manages risks at all levels.

Therefore, the Management shall use this policy as a tool, to continuously improve the organization's processes. ERM puts in place various monitoring, and reporting mechanisms as well as an implementation time frame.



Prof. Theophilus M. Mutui, (Ph.D)

MANAGING DIRECTOR

Effective Date:7/11/2023.....

DEFINITION OF TERMS

Risk: The uncertainty of an outcome that an event will occur and affect achievement of objectives. Effect of uncertainty on objectives may be negative or positive.

Risk Management: A process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, manage risks to be within its risk appetite and to provide reasonable assurance regarding the achievement of entity objectives.

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

Risk Owner: The person primarily responsible for coordinating a response to a particular project or business unit. It could be the Managing Director, Directors, Deputy Directors or Senior Managers.

Risk Culture: A system of values and behaviors present throughout an organization that shape day to day risk decisions. Values, beliefs, knowledge and understanding about risk shared by a group of people with a common purpose.

Impact: The potential loss should the risk materialize and will pronounce the severity or consequences

Likelihood: The probability that an adverse event which could cause materialization of the risk, may occur.

Strategic Risk: An event that affects the organization's ability to achieve its goals and objectives, including competitive and market factors.

Risk Factor: Something that increases the chance of an occurrence.

Risk Driver: An environment that leads one to believe that a particular risk will occur.

Committee: A group of people officially delegated to perform a function.

Risk Indicator: A measure used in risk management to indicate how risky an activity is.

ABBREVIATIONS/ ACRONYMNS

BOD	Board of Directors
MD	Managing Director
KEPHIS	Kenya Plant Health Inspectorate Service
SMIAR	Senior Manager, Internal Audit and Risk
ERM	Enterprise Risk Management
ARGC	Audit, Risk and Governance Committee
RMMM	Risk Mitigation, Monitoring and Management
PFM	Public Finance Management

TABLE OF CONTENTS

FOREWORD.....	i
ABBREVIATIONS.....	iii
DEFINITION OF TERMS.....	iv
TABLE OF CONTENTS	vi
1.0 INTRODUCTION.....	2
1.1 Policy Statement	2
2.0 PURPOSE OF THE POLICY	3
3.0 KEPHIS SCOPE	3
4.0 RISK GOVERNANCE STRUCTURE.....	3
5.0 ROLES AND RESPONSIBILITIES.....	4
5.1 Board of Directors (BOD)	4
5.2 Audit, Risk and Governance Committee.....	4
5.3 Managing Director.....	5
5.4 Enterprise Risk Management Committee.....	5
5.5 Senior Manager, Internal Audit and Risk	5
5.6 Risk Owners.....	6
5.7 Risk Champions.....	6
5.8 KEPHIS staff	7
6.0 RISK MANAGEMENT PROCESS	7
6.1. Integration with other systems and processes.....	10
7.0 RISK CATEGORIES.....	11
8.0 RISK REGISTER.....	12
9.0 RISK REPORTING.....	12
10.0 RISK MANAGEMENT PERFORMANCE	13
11.0 RISK APPETITE AND TOLERANCE.....	Error! Bookmark not defined.
12.0 REVIEW AND APPROVAL.....	14
13.0 REFERENCE AND RELATED DOCUMENTS	14

Risk Ranking: The weight given to a risk based on the impact of occurrence, the likelihood of occurrence and detectability. Risks can be ranked as high, medium or low.

Emerging Risk: A condition, situation, or trend with a great degree of uncertainty or lack of clarity that could be internal or external factor that significantly impact KEPHIS operational strength, competitive position or reputation.

Enterprise Risk Management (ERM): The culture, capabilities and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving and realizing value.

Risk Matrix: Tool used to rank risks within defined ranges by identifying consequence and likelihood in order to analyze and prioritize management of enterprise risks.

Risk Register: List of enterprise risks that could impact KEPHIS and their associated ratings, based on the enterprise risk matrix, plotted on a heat map.

Risk Appetite: The desired level of risk that KEPHIS is prepared and willing to accept/take in pursuit of its mandate.

Risk Tolerance: KEPHIS readiness to bear the risk after risk treatment in order to achieve its objectives.

Action Points: A specific proposal for action to be taken. They are reported in point form and are precise.

2.0 PURPOSE OF THE POLICY

The purpose of this Enterprise Risk Management (ERM) Policy is to institutionalize a formal risk management process and framework to support the achievement of KEPHIS objectives, safeguarding of resources and decision-making.

3.0 SCOPE OF THE POLICY

This policy applies to all KEPHIS activities. It forms part of KEPHIS governance framework and applies to all employees and other stakeholders.

4.0 RISK GOVERNANCE STRUCTURE

The risk governance structure of KEPHIS comprises of key players whose functions are highlighted below:

Board of Director shall provide policy, oversight and review of risk management

Audit, Risk and Governance Committee shall oversee regular review of risk management activities

Managing Director shall drive culture of risk management and signs off on annual risk attestation

Internal audit and risk department shall co-ordinate and monitor implementation of the enterprise risk management framework.

Enterprise Risk Management committee shall continuously improve the risk management policy, strategy and supporting framework

Risk Owners shall ensure staff in their operational units comply with the risk management policy and foster a culture where risks can be identified and escalated.

Risk champions shall identify, analyze and report risks in their respective operation units

Staff and Stakeholders shall comply with risk management policies and procedures

1.0 INTRODUCTION

Kenya Plant Health Inspectorate Service (KEPHIS) is a regulatory body that is established by the KEPHIS Act No.54 of 2012. KEPHIS is mandated to implement the Agriculture Produce (Export) Act CAP 319, Plant Protection Act CAP 324, and the Seeds and Plant Varieties Act CAP 326. The role of KEPHIS is to undertake regulatory function in the agricultural sector in matters relating to plant protection, seeds and plant varieties that assures the quality of agricultural inputs and produce, thereby promoting sustainable agricultural and economic growth.

Recent trends in public sector management have laid emphasis on transparency and accountability. This has resulted in increased focus in governance of public institutions, incorporation of risk management and financial controls. The Mwongozo code of conduct and Treasury Circular No. 3/2009 of 23rd February 2009 and Regulation 2012 of PFM Act section 165 (1), directed that all public institutions develop and implement a risk management framework. It is on this basis that KEPHIS has developed this enterprise risk management policy.

KEPHIS is committed to managing risks to an acceptable level across all areas of its operations, so that its objectives can be achieved. The risk commitment extends to third party interaction. KEPHIS recognizes that risk management is an integral part of the management process and intends to promote a positive risk culture within its operations. To effect this, KEPHIS will communicate to all staff their role in risk management, and provide the means for employees to play that role.

1.1 Policy Statement

The Board of Directors is committed to ensuring that Enterprise Risk Management is entrenched into KEPHIS daily operations. KEPHIS shall apply risk management principles to support realization of its strategic objectives by implementing the risk management framework for effective governance.

6. Monitor risks and compliance procedures.
7. Make recommendations on adequacy and effectiveness the ERM reports.

5.3 Managing Director

The Managing Director shall;

1. Drive culture of risk management and signs off on the annual risk plan.
2. Ensure that the risk management framework is developed and implemented.
3. Be the overall risk owner.
4. Appoint an ERM committee and risk champions responsible for risk management in KEPHIS.
5. Facilitate the implementation of the ERM policy through provision of resources.

5.4 Enterprise Risk Management Committee

The role of the enterprise risk management committee shall;

1. Review the KEPHIS Enterprise Risk Management Policy.
2. Oversee implementation of Enterprise Risk Management Policy and framework.
3. Ensure implementation of recommendations of the Audit, Risk and Governance Committee.
4. Report on the implemented action plans by the risk owners to reduce risks.
5. Deliberate on risks, giving workable suggestions mitigation measures on the same.
6. Ensure implementation of the approved annual risk plan.
7. Recommend removal of suggested risks from the risk register by the risk owner.

5.5 Senior Manager, Internal Audit and Risk

SMIAR shall;

1. Coordinate risk management activities in KEPHIS.
2. Monitor risk exposure and advise management accordingly.
3. Develop and implement the Annual Risk plan.
4. Collate the risk registers and prepare a summary report to the ERM committee.
5. Is the secretary to the ERM Committee.

5.0 ROLES AND RESPONSIBILITIES

5.1 Board of Directors (BOD)

As per Mwongozo, The Code of Conduct for state corporations, 3.2, KEPHIS BOD shall;

1. Ensure development of ERM policy, which should consider sustainability, ethics and compliance risks.
2. Set out its responsibility for risk management in the Board charter.
3. Approve the risk management policy and the risk management framework.
4. Delegate to management the responsibility to implement the risk management plan.
5. Monitor that risks taken are within the set tolerance and appetite levels.
6. Review the implementation of the risk management framework on a quarterly basis.
7. Appoint a Board committee responsible for enterprise risk management in KEPHIS.
8. Ensure that the committee obtains relevant technical advice where necessary.
9. Evaluate the performance of the committee once a year.
10. Establish a risk management function within KEPHIS.
11. Ensure that risk assessment is carried out on a continuous basis.
12. Receive from the internal audit function, a written assessment of the effectiveness of the system of internal controls and risk management.
13. Receive assurance from management that the risk management framework is integrated in the daily activities of KEPHIS.

5.2 Audit, Risk and Governance Committee

The ARGC shall;

1. Advise on policy directions of Risk Management.
2. Report to BoD on internal controls and any emerging risks and issues.
3. Oversee internal and external audits as required in its review of internal controls.
4. Provide advice to the Board on the effectiveness of the internal controls system, including the ERM.
5. Approve the annual risk plan.

3. Sensitize staff on Enterprise Risk management issues.
4. Build a risk-aware culture within the organization.
5. Provide periodic risk reports of their respective departments or regions.

5.8 KEPHIS staff

This policy shall apply to all staff (permanent and temporary) and be included in staff induction material and sensitization. Roles are;

1. To comply with risk management policies and procedures.
2. Support in identification of risks.

6.0 RISK MANAGEMENT PROCESS

The risk management process shall consist of eight stages:

- a. Establishing the Scope, Context and Criteria - Objectives of the departments/ regions/ sections are defined.
- b. Identifying risks – uncertainties that affect the organization from achieving its objective are identified.
- c. Analyzing risks – risks are categorized and assessed by scoring them for impact and likelihood.

Likelihood Matrix

Rank	Likelihood Matrix	Definition
5	Almost Certain	Very likely. The event is expected to occur in most circumstances as there is a history of regular occurrence
4	Likely	There is a strong possibility the event will occur as there is a history of frequent occurrence
3	Possible	The event might occur at some time as there is a history of casual occurrence
2	Unlikely	Not expected, but there is a slight possibility it may occur at some time
1	Rare	Highly unlikely, but it may occur in exceptional circumstances. It could happen but probably never will

6. Prepare quarterly reports on the status of implementation of the annual Risk plan for submission to the Audit, Risk and Governance Committee.
7. Develop and implement an internal risk-based audit strategy.
8. Manage the enterprise risk management program and evaluate its effectiveness.
9. Conduct Ad-Hoc risk assessments when requested by management and advise accordingly.
10. Periodic review of quarterly risk registers.
11. Liaising with the ERM Chairman to plan for meetings, ensuring meetings are effectively organized and minutes taken.
12. Ensure communication and correspondences to the ERM committee members, including risk champions, risk owners and other related stakeholders on risk management.
13. Ensure induction and sensitization of staff on ERM policies and procedures.

5.6 Risk Owners

The risk owners shall;

1. Ensure staff in their operational units comply with the risk management policy.
2. Foster a culture where risks can be identified and escalated.
3. Be responsible for identification and management of risks within their functional areas.
4. Develop action points/plans.
5. Be responsible for risk evaluation.
6. Ensure implementation of measures to mitigate risks.
7. Be responsible for monitoring and evaluation of action points identified to mitigate risks.
8. Ensure staff are sensitized on Enterprise Risk management issues.

5.7 Risk Champions

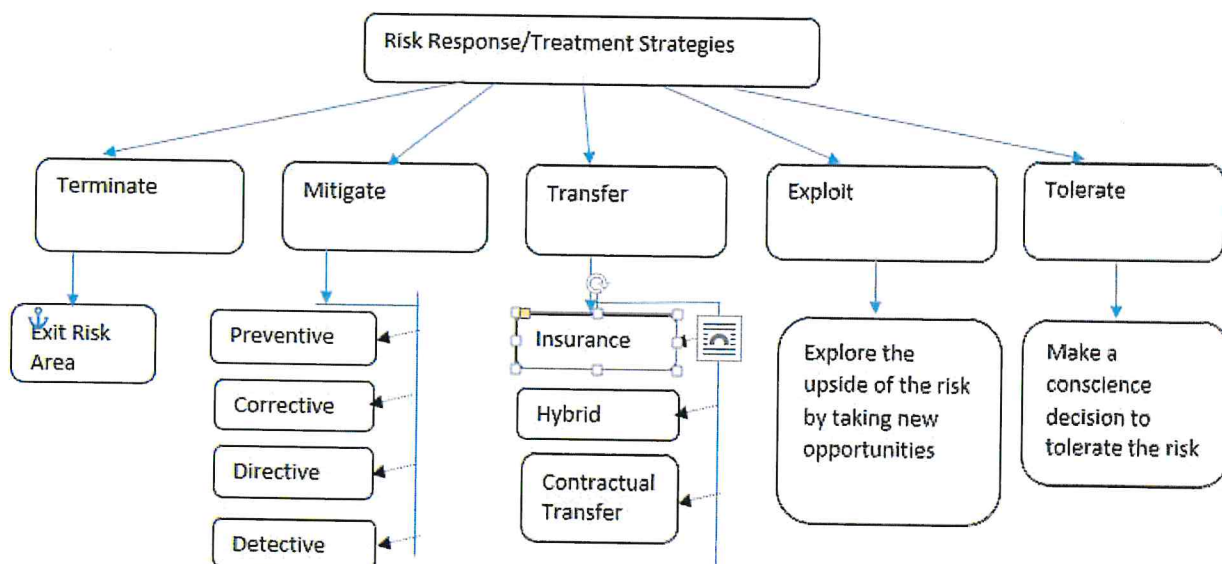
Risk Champions shall;

1. Act as the lead person in identification, ranking, monitoring and evaluation of risks.
2. Prepare risk registers.

KEPHIS-Enterprise Risk Management Policy

		Negligible 1	Minor 2	Moderate 3	Major 4	Extreme 5
Likelihood	Almost Certain 5	Medium	Medium	High	High	High
	Likely 4	Low	Medium	Medium	High	High
	Possible 3	Low	Medium	Medium	Medium	High
	Unlikely 2	Low	Low	Low	Medium	Medium
	Rare 1	Low	Low	Low	Low	Medium
		Impact				

- e. Treating the risks - Shall involve selecting treatment and implementing options for addressing risks. The prescribed treatment can be one or more options



- Risk Acceptance/ Tolerance – Acceptance of risks is considered not to affect the ability of the Organization of achieving the stated institutional objectives or ability

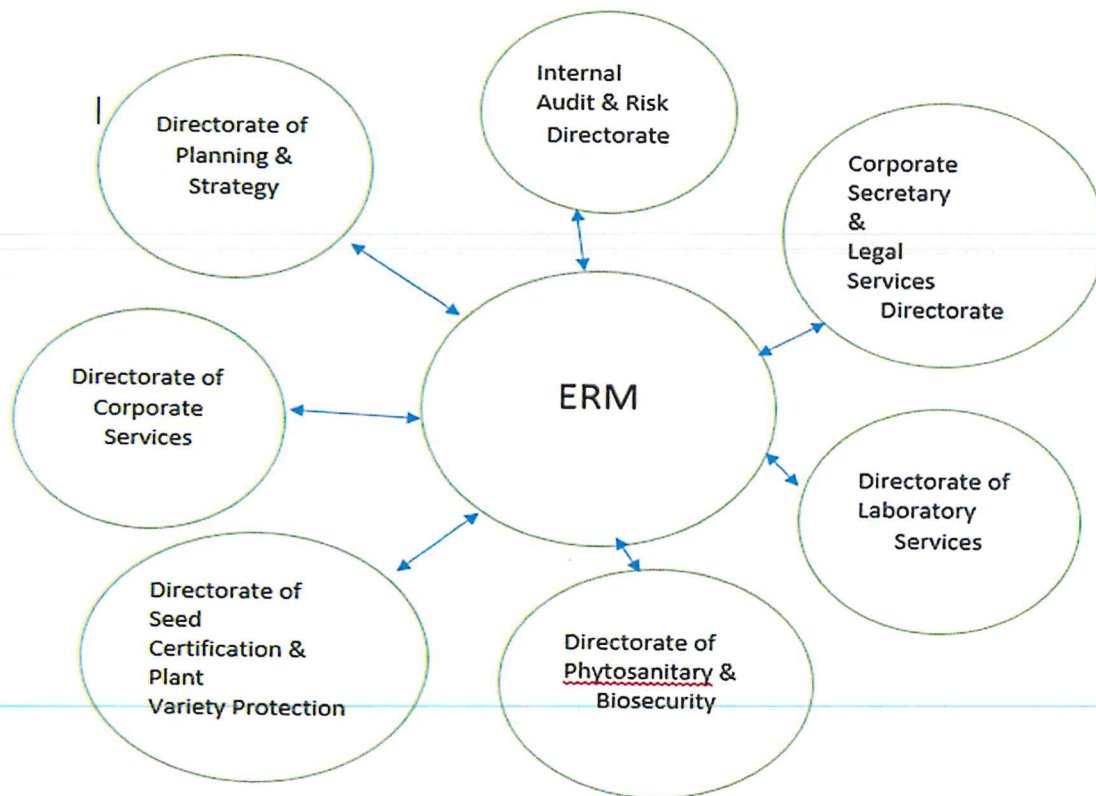
KEPHIS-Enterprise Risk Management Policy

Impact Matrix

Rank	Impact Matrix	Definition
5	Extreme	A risk that if occurs will have a severe impact on achieving desired results to an extent that one of more of its critical outcome/objectives will not be achieved
4	Major	A risk that if occurs will have a major impact on achieving desired results to an extent that one of more of its critical outcome/objectives will fall below acceptable levels
3	Moderate	A risk that if occurs will have a moderate impact on achieving desired results to an extent that one of more of its critical outcome/objectives fall well below goals but above minimum acceptable levels
2	Minor	A risk that if occurs will have a minor impact on achieving desired results to an extent that one of more of its critical outcome/objectives fall well below goals but above minimum acceptable levels
1	Negligible	A risk that if occurs will have negligible or little impact on achieving outcome/objectives

The detailed impact matrix shall be populated as per the various units and annexed to the procedure.

- d. Evaluating and prioritizing risks - shall involve comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. 1-4 = Low; 5-14 = Medium; 15-25 = High



7.0 RISK CATEGORIES AND APPETITE STATEMENTS

Risk Appetite shall be determined by The Board. It will define the organization's willingness to accept risk in pursuit of its objectives assessed against the key drivers of success and it is intended to guide employees in their actions and ability to accept and manage risks. ERM Risk categories that relate to service delivery have been mapped accordingly. KEPHIS risks have been categorized as below:

to comply with the applicable legal requirements, nor to impinge on the Organization's ability to meet regulatory and contractual obligations;

- Risk Avoidance/ Elimination – The Organization will implement appropriate changes to either the organizational environment, systems or wherever required to ensure the risk is no longer applicable and faced by the Organization;
- Risk treatment/ Mitigation – Methods which apply technical or non-technical controls to reduce the threat, vulnerability or impact of a risk;
- Risk Sharing/Transfer – involves risk sharing with insurance to support consequences or managed service. It is possible to share the responsibility to manage risk but not the liability of impact;
- Risk Transformation/ Exploit - converting what could be a possible risk into an opportunity.

f. Monitoring and reviewing of the risks - shall consist of monitoring existing risks, identifying new risks, identifying any trouble spots and evaluating the effectiveness of current risk treatment strategies.

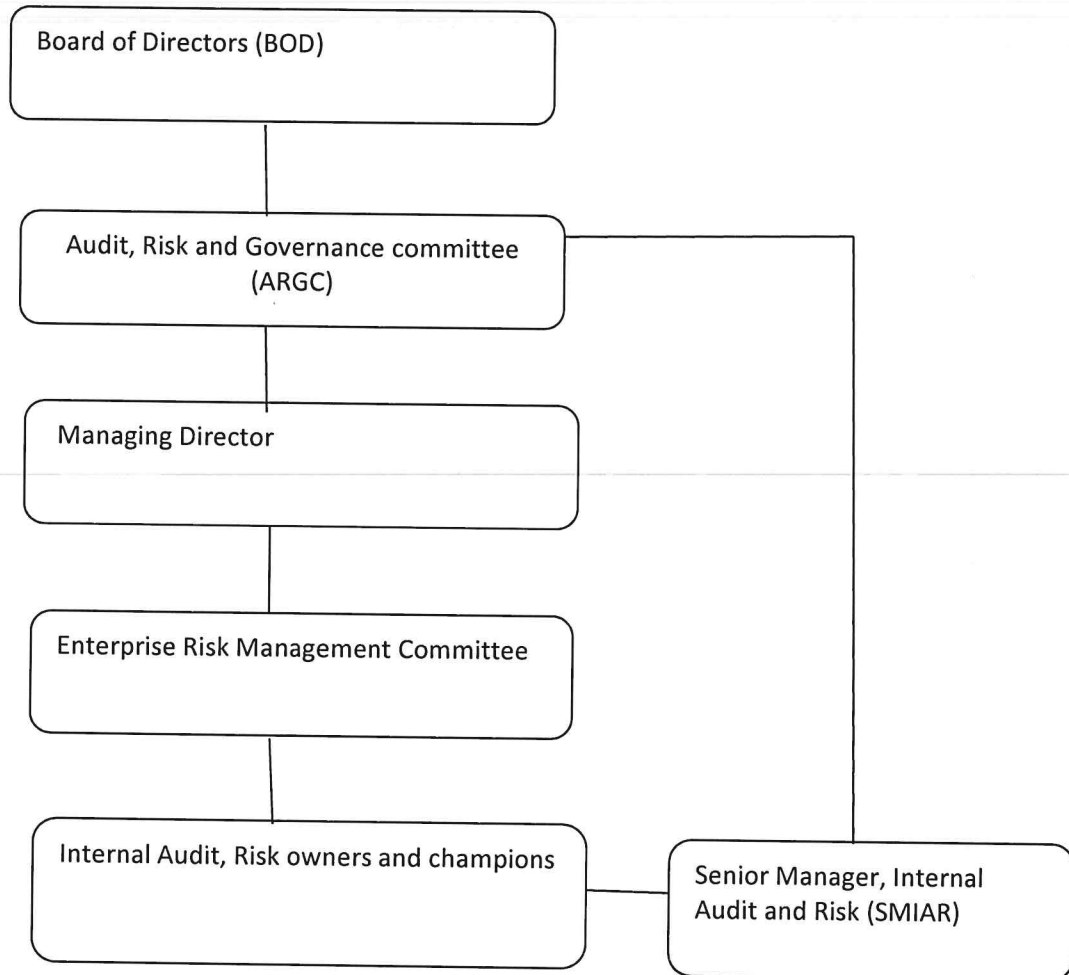
g. Reporting of risks - shall include periodic documentation of the assessment process, risks identified and the measures designed to reduce the impact of these risks.

h. Communicating Risks - The action plans to be implemented shall be communicated and consultation done to and fro amongst the staff, risk owners and risk champions.

6.1. Integration with other systems and processes

Risk management is factored and integrated in all KEPHIS processes and activities.

report of Institutional risks for review by the ERM Committee. The reviewed report shall be forwarded to the Audit, Risk and Governance committee for recommendation and adoption.



10.0 RISK MANAGEMENT PERFORMANCE

- a) The SMIAR shall prepare a risk-based annual internal audit plan geared towards providing an independent and objective assurance to the management and the BoD that controls put in place to manage risks are effective.
- b) Periodic reports on management action plans on risk mitigation measures with timelines and follow up to ensure implementation shall be presented to management and the Audit, Risk and Governance committee.

KEPHIS-Enterprise Risk Management Policy

No.	Risk Category
1	Hazard Risk Category- This category will include OSH, Environmental and Security related risks. These are the risks that poses a level of threat to life, health, property, or the environment.
2	Political Risk Category- Risks faced by KEPHIS caused by political decisions, events, or conditions that will significantly affect the achievement of objective.
3	Operational Risk Category- Risks resulting from inadequate or failed internal processes in the technical areas, people (human capital) and corruption risks.
4	Financial Risk Category- Risks that the Institution may be long-term/ short-term financial demands or risks arising from cash-flow inadequacies, financial transactions, accounting and reporting requirements.
5	Compliance Risk Category- Risks arising from failure to comply with laws and regulations, standards, guidelines, internal policies and contractual arrangements.
6	Technological Risk Category- Risks arising from inadequate or failed system infrastructure including all network, hardware, software, communications and their interfaces
7	Reputational Risk Category- Risk resulting from damages to the reputation of the institution and bad publicity

Risk appetite statement for each identified category will include in the procedure.

8.0 RISK REGISTER

The institution shall maintain a risk register to manage risks. The register shall include details from the categories highlighted in section 7.0 above. Emerging risks shall be reported immediately and updated in the register of the respective risk areas. Periodic reviews of risk registers shall be done by the Senior Manager Internal Audit and Risk. Removal of risks from the register shall be upon recommendation by the ERM Committee.

9.0 RISK REPORTING

The departmental/ sectional/ regional risk champions shall prepare periodic reports through the risk owners forward to SMIAR for review. SMIAR shall prepare a summary

- c) Periodic trend reports on impact of mitigating measures on institutional risks shall also be presented to the Audit, Risk and Governance committee.

11.0 REVIEW AND APPROVAL

The ERM Committee shall spearhead the review of this policy after three (3) years of operation, or if significant changes occur to ensure its continuity, suitability, adequacy and effectiveness.

This policy is in operation until revoked or modified

12.0 REFERENCE AND RELATED DOCUMENTS

- a) Treasury Circular No. 3/2009, done on 23rd February 2009
- b) Mwongozo, Code of Conduct for Board of Directors
- c) Public Sector Risk Management Guidelines, January 2020
- d) ISO 31000, Risk Management Guidelines
- e) ISO 9001, Quality Management Systems (QMS)
- f) ISO 27001, Information Security Management Systems (ISMS)
- g) KEPHIS Internal Audit Policy and Procedures Manuals
- h) Public Finance Management Act 18 of 2012.
- i) KEPHIS Act of 2012 and other policies and regulations.

