THE COUNTY GOVERNMENT OF NYANDARUA
PAMOJA TUJIJENGE

RISK MANAGEMENT POLICY FRAMEWORK

NOVEMBER 2020

1 Foreword

The County Government of Nyandarua Enterprise Risk Management Policy Statement 2020 recognizes the contribution of risk management practice to sound Governance Practice and increase in community confidence in government performance. The overall framework affirms that consistent and systematic application of risk management is central to maximizing community outcomes, deriving the benefit of opportunities, managing uncertainty and minimizing the impact of adverse events.

Consistent with this policy the County Government is committed to protecting itself, staff and the general Nyandarua population from situations or events that would prevent it from achieving its strategic goals and objectives. Risk management is an integral part of good governance practice and effective stewardship of assets to achieve the desired impact of devolution.

A systematic approach to managing risks and opportunities is more effective and efficient than allowing informal, intuitive processes to operate. Identifying risks at an early stage and developing mitigative measures to combat the risk is the only sure way of keeping development on track and safeguarding public resources

County Government of Nyandarua's adoption of a structured approach to risk management encapsulates the following:

- Defines a process for systematically managing the risk of all functions and activities in the county Government;
- Encourages a high standard of accountability at all levels of the county Government;
- Supports effective Information management systems and reporting mechanisms;
- Encourages a high standard of efficient and effective service delivery through proactive risk identification and management.
- Allows the County Government to better meet community demands and entrench accountability for devolved functions.

Risk is fundamental to the county in keeping the objectives of the CIPD2 on track, improve service delivery, assist in achieving value for money as well as reducing uninvited surprises.

This Risk framework is premised on a positive risk culture that encourages openness and discusses real service delivery issues in an open manner, based on robust accountability structures. The framework is anchored on a top down approach for systemic risk management.

The County Governing Body takes full ownership and commits to a proactive Risk Management culture. Based on this commitment, the County Government will work to break down departmental silos, encourage the elevation of best practice and strive for continuous improvement. This framework affirms collective responsibility for all county staff members to be involved in the identification, evaluation and treatment of risks and opportunities that could impact or influence outcomes for the County Government of Nyandarua.

H.E. FRANCIS T. KIMEMIA, E.G.H., CBS, HSC

GOVERNOR, NYANDARUA COUNTY

Contents

County Government of Nyandarua Risk Management Framework

2 Executive Summary

The County Government of Nyandarua is committed to optimal management of risks in order to achieve the vision of "**Excellence in County leadership for a united, prosperous County whose social economic and political development benefits are equitably distributed.**"

For this commitment to be realized, H.E the Governor and the CEC have embraced holistic enterprise risk management as a means to manage risks intelligently and enhance their awareness and oversight while also focusing on improved risk reporting. PFM Regulation 158(1) provides that an Accounting Officer shall ensure that:

a) The County Government develops Risk Management Strategies, which include fraud prevention mechanism; and
b) The County Government develops a system of Risk Management and internal control that builds robust departmental operations.

In order to achieve this systematic management of risks, H.E the Governor through CECM finance and economic development established a task force to develop a Risk Management policy Framework. The ToRs for the Task Force were:

i. Identify existing and potential risks in the County Government systems;
ii. Develop preventive, curative and mitigating strategies on the identified risks;
iii. Develop a tool to be used by all accounting officers in monthly reporting of measures implemented in addressing any risks; and
iv. Any other important measure/area relevant in risk management.

3 The scope of the Enterprise Risk Management Framework

- Review of the CIDP2.
- Formulation of questionnaires as basis for risk identification for all departments.
- Process Customization and development of a risk management tool.
- Designed the risk appetite and tolerance levels.
- Collated the risk data and inferred the results to the Risk Management tool.
- Formulation of mitigation strategies.
- Capacity building and knowledge transfer to facilitate continued reviews and improvement periodically.

This process culminated with the development of the County risk management policy framework and the Fraud and Anti-Corruption Framework.

4 Definitions of Terms

In this Framework, unless the context indicates otherwise:-

Cause: An element which alone or in combination has potential to give rise to a risk.

Communication and consultation: A continual and interactive processes that a County conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk.

Consequence: The outcome of an event affecting objectives should the risk occur. (A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives. Consequences can be expressed quantitatively or qualitatively. A consequence can escalate through cascading and cumulative effects.)

Establishing the context: Defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy

Event: An occurrence or change of a particular set of circumstances and can be something that is expected which does not happen, or something that is not expected which does happen. Events can have multiple causes and consequences and can affect multiple objectives.

External context: External environment in which the County seeks to achieve its objectives

Governing body: Refers County Executive Committee to whom the Accounting Officer functionally report.

Internal context: Internal environment in which the County seeks to achieve its objectives

Likelihood: Chances of something happening

Monitoring: Continuous checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.

Portfolio view: The composite view of risks a County faces, which positions management and the Governing Body to consider the types, severity, and interdependence of risks and how they may affect the County's performance relative to strategy and objectives.

Principal risk: A principal risk is a risk or combination of risks that can seriously affect the performance, future prospects or reputation of the County.

Risk: Is the effect of uncertainty on objectives. Risk is usually described in terms of causes, potential events, their consequences.

Risk tolerance: Means the boundaries of acceptable variation in performance related to objectives

Risk analysis: Is the process to comprehend the nature of risk and to determine the level of risk based on the assessment of the likelihood of the risk occurring and the consequences should it occur.

Risk assessment: The overall process of risk identification, risk analysis and risk evaluation.

Risk appetite: Is the amount of risk, on a governing body level, a County is willing to accept in pursuit of value.

Risk management: Means coordinated activities to direct and control a County with regard to risk.

Risk management framework: Is set of components that provide the foundations and Organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the County

Risk management plan: A scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk

Risk management policy: A statement of the overall intentions and direction of a County related to risk management

Risk management process is the systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating and reviewing risk.

Risk owner: Is a person accountable for managing a particular risk.

Risk strategy: Describes the specific management activities that are aimed towards dealing with various risks associated with County operations. It includes decision on risk tolerance levels and acceptance, avoidance or transfer of risks faced.

Risk criteria: Refers to terms of reference against which the significance of risk is evaluated.

Risk treatment: The process to modify risk.

Risk retention: The acceptance of the potential benefit of gain, or burden of loss, from a particular risk.

Residual risk: The risk remaining after risk treatment.

Risk profile: Is the description of any set of risk. It can relate to the whole County or a part of a County or as otherwise defined.

Risk register: Is a record of information about identified risks related to a specific County activity.

Severity: Is a measurement of consideration such as likelihood and impact of events or the time it takes to recover from events.

Shared risk: A risk with no single owner, where more than one County is exposed to or can significantly influence the risk.

Stakeholder: A person or County that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

5 List of Acronyms

CEC- County executive Committee

CECM – County Executive Committee member

CIDP2 – County Integrated Development plan

ERM – Enterprise- Wide Risk Management

PFMA - Public Finance Management Act

6 Purpose of this framework

The purpose of this framework is to:

- Define Risk Management;
- Achieve Compliance with the Laws, regulations, guidelines and internal policies
- Outline the County's Risk Management Plan;
- To drive a culture change in the County operations and stewardship of assets to achieve the desired impact of devolution.
- Definition of County risk appetite, Policy and Key risk indicators.
- Achieve Responsiveness to required standards and strategic requirements
- Integrated approach to risk management and the reduction of operational silos within the County
- Describe the approach managing risks based on established risk management principles;
- Outline guidance on risk management process with a detailed context;
- Outline roles and responsibilities;
- Explain the County Governments risk management recording and reporting requirements;
- Incorporate risk reporting tools in performance management including risk dashboards and Key risk indicators

7 Guiding Legal Principles

7.1 Constitution of Kenya

The constitution of Kenya is the foundation for Risk management in the public sectors; Articles 10,201 and 232 underpin the centrality of good Governance and accountability in public functions. The devolved Government is a key public function and under Chapter 11 Constitution of Kenya (Devolved Government); the objects of devolved Government to include;

- to promote democratic and accountable exercise of power,
- to ensure equitable sharing of national and local resources
- to enhance check and balances and separation of powers

These objectives enjoined with the previous articles speak to the principles of Risk management and underscore the need for the County Government to establish the Risk Management Framework to drive practices that enable its administration to achieve its constitutional objects.

7.2 Public Finance Management Act, 2012

The Devolved Government being an extension of the National Government is governed by The Public Finance Management Act 2012 and the Public finance Management regulations 2015.

The provisions under the act require the incorporation of risk management in public finance decisions and in the management of all maters public finance.

7.3 Mwongozo Governance Code for State Corporations, 2015

This detailed public sector guidelines offers an in-depth look at the requirement for all state entities. The code requires the setting up of appropriate structures to ensure adequate systems and processes of accountability, risk management and control. This code is key in reviewing the parameters within which the County Government must set up its Risk management mechanisms to meet the required standards.

7.4 County Integrated Development Plan (CIDP2)

The CIDP2 is the County's strategic document prepared based on the functions of the County Government while appreciating that the County and National Governments are interdependent. The plan centers on the inter-linkages of various development agendas, International, National and Local. For effective stewardship of the assets allocated to the County, the plan is focused on delivery of services and accountability. This approach is linked to risk management, making the CIDP2 is a core reference document for this risk management framework.

7.5 Public Sectors Risk Management Guidelines 2020

These guidelines are for use by public officers in National and County Governments and their entities to enhance capacity and provide guidance in the implementation of risk management. The guidelines have been developed to conform to the latest international risk management standards. This framework is molded around these guidelines.

8 Introduction to Risk Management

8.1 Risk Management

Risk Management means coordinated activities to direct and control an entity with regard to risk. This is the systematic application of Management policies, procedures and practices to the activities of communicating, consulting, establishing the context, identifying, analysis, evaluating, treating, monitoring and reviewing risk.

When management of risks or opportunities is effective, it often remains unnoticed. When it fails, the consequences to the County Government operations, Nyandarua County community and staff may be significant and high profile. Good risk management practice ensures that the County Government can undertake activities confident that measures are in place to maximize the benefits and minimize the negative effects of uncertainties on Strategic objectives.

Effective risk management supports good Governance as it assists in determining priorities and setting objectives, in analyzing uncertainties within decision-making arrangements, in clarifying accountabilities and in demonstrating how the public interest is best served. This helps to create and protect value.

8.2 Risk Management Principles

The principles are as follows;

No	Principles of Risk Management	How these principles apply to the County Government
1	Risk management creates and protects value	Risk Management enables the County Government to meet objectives of devolution as derived from Chapter 11 of the Constitution of Kenya. It guarantees project delivery on an incremental basis, for growth of County wealth, minimizing waste, enhancing stewardship, accountability, monitoring and evaluation.
2	Risk Management is an **integral** part of all Countyl processes	The County Government incorporates Enterprise Wide Risk Management into planning and processes across all administrative levels of the County Government and ensures consideration is given to financial, social and environmental factors. The County Government takes a holistic, consultative and innovative approach to ensure minimization of silos for systemic sustainable development goals. The County Government is continuously making impact assessment of all actions through a wide spectrum perspective analysis.
3	Risk management is part of decision making	Decisions made within the County Government by individuals, teams, units and departments, have regard to risk information and knowledge that is accurate, timely and complete.
4	Risk Management explicitly addresses uncertainty	The recording and reporting of risks within the County Government is clear, concise and is responsive to changes
5	Risk management is **systemic, structured** and timely	The risk management is a continuous process that exists within the County Government Governance framework with a reporting structure that reflects the County needs and local circumstances. County policies and procedures will be designed and integrated with risk management measures systematically at all levels and processes. Deployment of risk management measures and tools will be time based to guarantee impact and appropriate resource deployment.
6	Risk Management is based on **best available information**	The County Government has rich data sources that are fostered by open communication channels, allowing the highest level of information to be conveyed effectively to stakeholders. The County Government continuously works to collect and compile data to enhance cross cutting communication.

		Open information management system is an integral part of the County risk management approach. Risk management enhances open communication in terms of public consultation to be able to reach the lowest level possible.
7	Risk Management is **tailored**	The County Government, its departments and all its units work with risk management procedures that are tailored to meet their specific needs.
8	Risk Management takes **human and cultural** factors into account	Consultation on the development and implementation of risk management policies ensures policies; frameworks and practices in the County reflect diversity of activities of the County, its staff and its population. Policy customization informs the County Government strategy, guided by population demographics and cultural practices.
9	Risk Management is transparent **and inclusive**	Risk management in the County involves the engagement of internal and external stakeholders through respectful acknowledgment of their contribution to the communication, consultation, monitoring and reviewing processes. Public participation and consultation is integral to project implementation and delivery of value, the County Government uses an approach of conscious communication and feedback with internal and external stakeholders. Risk management in project implementation will ensure emphasis on active-continuous stakeholder inclusivity and grassroots participation. The County Government employs accountability, reporting and monitoring tools to guarantee transparency
10	Risk Management is **dynamic,** interactive and responsive to change	Risk Management in the County responds to changing needs of the County, its staff and its population by continually self-assessing, monitoring and reviewing operation processes against the County Integrated Development plan. County Risk management approach is evolutional and time bound; within a Governance structure that ensures delivery of services.
11	Risk Management facilitates continual i**mprovement** of the organization	Continuous application of risk management measures leads to improved administration practices and increased maturity of the risk management processes.

9 Risk Management Framework for County Government of Nyandarua

This section describes the essential requirements of an institutional risk management framework:

(1.) Leadership and Commitment;
(2.) Integration;
(3.) Design.
(4.) Implementation
(5.) Evaluation
(6.) Improvement

9.1 Leadership and Commitment

The County Executive Committee as **the Governing Body** of the County shall provide risk Governance through demonstrated commitment for managing risk by laying the foundations for risk management including:

- Establish Governance structures
- Demonstrate an understanding of, and Commitment to, an integrated risk management system.
- Establish risk management framework
- Develop and deploy risk management strategy

- Set the risk appetite, threshold and tolerance levels
- Assigning risk ownership
- Ensuring necessary resources to manage risks are allocated including people, skills, experience and competence; processes, methods and tools; information and knowledge management systems; and professional development and training needs.
- Ensuring risk management is a regular agenda item at Governing body level and at department meetings;
- Ensuring risk information is appropriately and regular reported internally and externally;
- Promoting systematic monitoring of risks; and
- Ensuring risk management responsibilities are included in performance management system.
- Review and periodic updating of Risk Management Framework

The risk management policy should be approved by the Governing Body.

The CEC acknowledges that Risk Governance cannot be approached from a one size fits all and are committed to continuously promote development and customization of the framework to fit the County Government needs, taking into consideration its mandates and strategic objectives

9.2 Integration

1) The Accounting Officer is accountable for ensuring that risk management is integrated into all aspects of the county and is not a standalone activity.
2) The County shall promote risk –based thinking in processes and quality management systems.
3) The risk management framework forms an integral part of the County's purpose, governance, leadership and commitment, strategy, objectives and operations and helps the entity achieve desired levels of sustainable performance and long-term viability through:
    i. Developing a positive risk management culture characterized by encouraged and acceptable behaviors, discussions, decisions and attitudes toward taking and managing risk;
    ii. Setting appropriate accountability and oversight roles;
    iii. Aligning risk management to the entity mission, objectives, strategy and culture;
    iv. Conducting risk assessment before any major decision;
    v. Embedding risk management responsibilities in performance management contracts; and
    vi. Complying with various laws that prescribe specific treatment and reporting of risks within their ambit including prevention of fraud, disaster management, health and safety and others.

9.3 Design

The County Government understands its risk management context; the external and internal context; the risk criteria and administrative arrangements that influence the design and implementation of this risk management framework. Based on the understanding the County Government also:

(i.) Has scoped the risk management initiative and develop common language of risk;
(ii.) Established this risk management strategy, framework and the roles and responsibilities;
(iii.) Assigned authorities, responsibilities and accountabilities for risk management;
(iv.) Put in place appropriate communication protocols to collect, collate, synthesize and share relevant information and feedback provided.

9.4 County Government Risk Management Policy

The Nyandarua County Government Risk Management Policy states;

"The County Government of Nyandarua recognizes that commitment to risk management contributes to sound Governance practice and increasing community confidence in Government performance"

This statement indicates that the County Government leadership is accountable for the devolved resources. The Risk philosophy which underpins this statement is that:

"**Risk management contributes to the creating of sustainable value"**

The Nyandarua County Government Risk Management Policy confirms the commitment to identify, assess and manage risks which may prevent the achievement of strategic goals and objectives.

The policy directs that the County Government will implement **Enterprise wide Risk Management** by integrating risk management into its culture, decision-making, programs, practices, Administrative planning and performance reporting.

This Risk Management Policy is applicable to the whole of the County Government operation.

9.5 Risk Management Practice within the County

The County Government is committed to maintaining and continuously improving an enterprise wide Framework that manages risks at a strategic and operational level. The Framework is designed to complement the County's' Integrated Development Plan and Promotes:

1. **Risk Management as Part of the culture**

The County Government is committed to a culture that is risk aware. The County executive Committee works closely with the Risk Management Function to strengthen the commitment to;

- A culture of enquiry, learning, reflection and trust to anticipate and objectively assess risk and opportunities associated with managing directions, services, processes, competencies, values and behaviors;
- A culture with channels of communication that are open, ethical and improve connectivity across the administrative departments;
- A culture which continually adds value to Governance structure and outcomes;

- A culture which commits to robust administrative planning and reporting cycle which is inclusive of risk management principles;
- A culture where commitment to an annual risk management review, results in and updated risk register and risk assessment matrix.

2. **Visible focus in managing strategic risk emergence and uncertainty**
    - Exercising risk leadership by example and communicating the risk culture;
    - Modelling behaviors based in principles outlined in this framework;
    - Overseeing and understanding the interdependence of risks;
    - Ensuring competencies by supporting professional development and risk management education and training; and
    - Aligning resources with managing risks and opportunities.
3. **Full Accountability for managing and reporting all risks at all levels of the County Government (strategic and operational)**

An enterprise wide risk management system as adopted by the County Government promotes full accountability for managing all risks (strategic and operational). The system encourages a high standard of efficient and effective focused service delivery to the population and;

- Provides a holistic approach to managing the uncertainty associated with strategic risks;
- Creates predictability and operational reliability.
- Allows for implementation of cost effective treatments to reduce risks and exploit opportunities;
- Ensures risk management is considered in all new projects, initiatives and reports.
- Enables risk information and knowledge that is accurate, timely and complete to be integrated into an effective decision making process.

10 Risk Accountabilities within the County Government

10.1 Risk Owner

- Risk in the strategic register must be owned by the County Executive Committee.
- All other risks are owned by the accounting officer within the Administrative department, who has the overall responsibility of the risk.
- Risk owners have the authority to manage and allocate resources to mitigate the risk.
- Risk owners understand where Risks require escalation to the next Governance level and when they should be retired.

Risk owners are accountable for the acceptance of risks that are above the recommended controlled level of risk. The County's risk appetite at a control level is moderate to low.

10.2 Control Owner

Control owners are able to effectively and efficiently manage and allocate resources when implementing a control. Control owners are expected to review their controls on a quarterly basis and ensure the control is up to date and operating as intended. Any updates to controls should be advised to the Risk Management

Function. If a control requires treatment, the control owner will liaise with the treatment owners to ensure appropriate actions are undertaken to strengthen the control.

10.3 Treatment Owner

Treatment owners are able to manage and allocate resources to ensure that the treatment they are responsible for is actioned and completed within the timeframe specified. **Provided that:** Treatment owners can also be a control owner or be separate depending on the required treatment. Any updates to the treatment are to be advised to the Risk Management Function when they occur or at the time of quarterly reporting.

The risk owners will provide documented explanation when a risk is accepted at a controlled level that is extreme or high. These risks will be reported to the County Executive Committee.

11 The Risk Management Roles and Responsibilities

11.1 County Executive Committee

The responsibilities of the CEC as the Governing Body for risk management include:

I. Approving the risk management policy and implementation plan;
II. Defining the Governing Body's risk Governance role and structure including its committees;
III. Determining and continuously assessing the nature and extent of strategic risks the County is willing to take to achieve its objectives
IV. Maintaining oversight on principal risks facing the County;
V. Assuring itself of the effectiveness of the County's risk management framework.

11.2 County Executive Committee Member (CECM)

I. Ensuring there are clear procedures within the department for bringing up significant issues to his/her attention and whenever necessary for escalation to the CEC.
II. Ensuring there are clear accountabilities for managing risks and that officers within the department are equipped with relevant skills and resources for performing their roles efficiently and effectively;
III. Cascading the risk appetite and ensuring that planning and decision making are within the accepted tolerance levels

11.3 Audit Committee

Audit Committee will support the CEC by reviewing the comprehensiveness and reliability of assurances on risk management. The responsibilities of Audit Committee in relation to risk management are stipulated in the Guidelines of Audit Committees for National and County Government and Mwongozo Governance code and include:

I. Reviewing and recommending disclosure on matters of risk in the annual financial statements and or annual report;
II. Reviewing the implementation of the risk management policy, framework, plan and strategies;
III. Reviewing the County risk profile relative to the County risk appetite and reporting requirements;
IV. Obtaining assurance on the effectiveness of the system of internal control and risk assessment.
V. Providing an assessment of the County Government's effectiveness in the annual report.

VI. Ensuring the internal and external audit plans are aligned to the County's risk profile.
VII. Ensuring that staff charged with risk management responsibilities have appropriate authority to carry out their functions;
VIII. Ensuring allocation of sufficient resources for effective management of risk.

11.4 Accounting Officers

National and County Public Finance Management Regulations, 2015, regulation 165 and 158 require all Accounting Officers to develop risk management strategies, which include fraud prevention mechanisms in their entities. To effectively discharge this responsibility in their entities designated Accounting Officers within County Government of Nyandarua will set an appropriate tone from the top for risk management by:

I. Championing the effective management of risk;
II. Articulating risk appetite;
III. Assigning responsibilities for risk management and holding management accountable for integrating risk management into operations;
IV. Evaluating alternative strategies and choosing appropriate strategies that consider the context of the department within the departmental risk appetite;
V. Ensuring that the department develops risk mitigation strategies;
VI. Providing assurance to the Governing Body and other stakeholders that key risks are properly identified, assessed, and treated; and
VII. Ensuring the risk management function is supported in carrying out its role.

11.5 Risk Management Committee for Entities (Public Finance Management Committee)

The Public Finance Management Regulations, 2015, regulation 17, 18, 19 requires the formation of Public Finance Management Committee, whose role is to identify risks and implementation of appropriate measures to manage such risks or anticipated changes impacting on the County.

The Risk Management Committees referred to above are aimed at supporting the Accounting Officer in determining and communicating policy, objectives, procedures, directing and monitoring the implementation, practice and performance of risk management activities. The responsibilities of these Risk management Committees include:

i. Reviewing the risk management policy, strategy and implementation plan;
ii. Reviewing the County's risk appetite, risk tolerance, risk indicators and risk capacity.
iii. Ensuring the County has appropriate risk identification and assessment methodologies, arrangements and tools;
iv. Developing risk treatment plans to address the significant risks of the County; and
v. Assessing implementation of the risk management policy and strategy and integration of risk management within the County operations.

While the responsibility of setting the risk appetite at the strategic level is the role of the CEC, it is vitally important that the Risk Committee of Management is able to align risk appetite to the operational activities within the County.

12 Three Lines of Defense Model of Risk Management

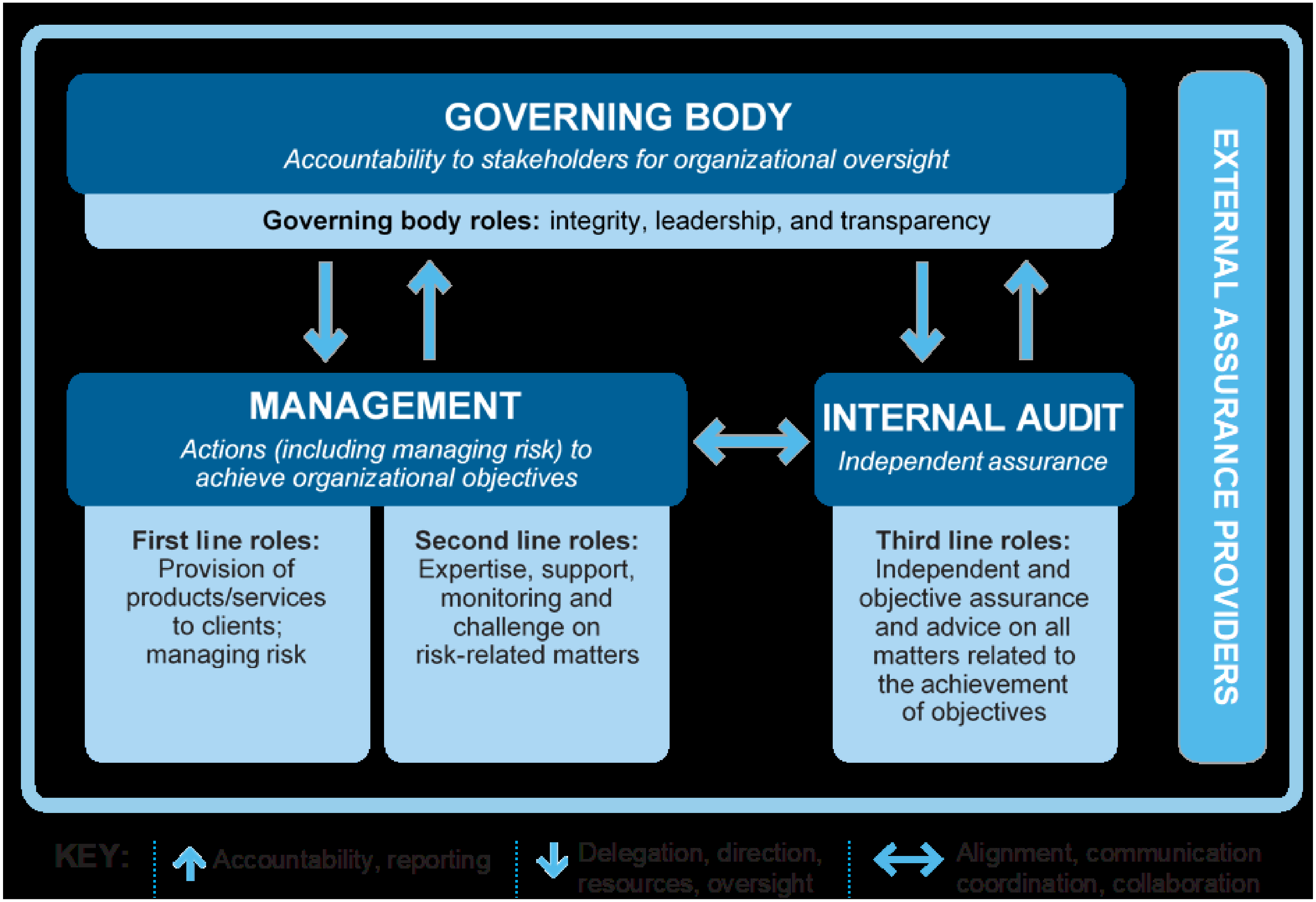
The County Executive Committee is ultimately responsible for Risk Management; the CEC has adopted an enabling structure to ensure comprehensive risk management. This model enables the CEC to delegate oversight and Management Responsibilities using the **"Three Lines of Defense Model."**

The three lines are;

Line 1.Designated Function Directors: They are responsible for the decisions relating to the taking on of risk and for the identification, assessment, treatment, monitoring and reporting of the risks that they assume.

Line 2.Risk Management Function are responsible for assisting the CEC in the design and oversight of the risk management system, and for assisting management in the execution of their responsibilities and providing oversight thereof.

Line 3.Internal Audit function is responsible for providing independent assurance by evaluating and recommending improvements for the effectiveness of risk management.


GOVERNING BODY
Accountability to stakeholders for organizational oversight
Governing body roles: integrity, leadership, and transparency
MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
First line roles: Provision of products/services to clients; managing risk
Second line roles: Expertise, support, monitoring and challenge on risk-related matters
INTERNAL AUDIT
Independent assurance
Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives
EXTERNAL ASSURANCE PROVIDERS
KEY:
Accountability, reporting
Delegation, direction, resources, oversight
Alignment, communication coordination, collaboration

The governing body and senior management are not considered to be part of the three lines of defense but are primary stakeholders served by the three lines of defense.

The goal is not to eliminate risk, but to manage the risks in all of County Government's activities to maximize opportunities and minimize adverse consequences. The roles and responsibilities of various players are;

12.1 First Line of Defense:

Officers at the Operational level have ownership, responsibility and accountability for assessing, controlling and mitigating risks together with maintaining effective internal controls. This level is closest to the activities of the County and is also primarily responsible for the operation of County activities. As "risk owners" they play a more hands-on-role in executing particular, day-to-day, risk and control procedures and are responsible for maintaining effective internal controls on a day-to-day basis.

12.1.1 Departmental Directors

The specific responsibilities for departmental Directors include:

- Identifying and managing risks as part of their everyday operations, escalating them promptly as and when necessary;
- Allocating and communicating responsibilities for managing risk;
- Developing and recommending risk tolerance thresholds for processes;
- Developing and maintaining risk registers and profile;
- Embedding risk management practices within the County operating processes;
- Monitoring risk management against risk appetite and risk tolerance thresholds;
- Promoting risk awareness within their departmental operations;
- Developing and implementing risk treatment plans;
- Providing risk profile reports and coordinating information sharing; and holding officials responsible for their risk management responsibilities.
- Directors shall nominate risk champions within their departments to coordinate the departmental efforts and support the risk management function.

12.1.2 Risk Champions

The Risk Champions act as change agents in the risk management process and are distinguished from risk owners in that champions are trouble shooters that facilitate resolution of risk related problems at departmental level. The Risk Champion should not assume the role of the Risk Owner but should assist the Risk Owner to resolve problems.

Their responsibilities will include;

- To familiarize with risk tools required to support the department (e.g. risk register)
- Facilitate the identification of risks within the department using approved risk tools.
- Assist in the development of risk response and mitigation plans.

- Ensure that the scoring techniques used within the department are consistently and accurately applied as per this framework.
- Take part in any specific functional risk analysis reviews to ensure risks are understood and reflected in all risk analysis.
- Provide support as required to risk and action owners to help them routinely and accurately report progress for the risk response plans and to complete their actions in a timely manner.
- To assist the department in interpreting and using risk based information in decision making.
- Maintain the completeness and accuracy of the data in the risk register and to generate the routine risk reporting as specified within the risk management plan.
- To champion the process of risk management within the department, building commitment to and energy for the risk management process.
- To contribute to the continuous improvement of risk management within the County.

Clear objectives and key performance indicators should be set for the Risk Champion in respect of risk management. The County shall facilitate an annual risk champion training and workshop.

12.1.3 All County staff

All County staff have responsibility for risk management and should:

- Diligently identify risks and report them to their supervisor, especially during periods of change to processes, or operational practice; and
- Comply with all risk treatments and applicable legal framework.

12.2 Second Line of Defense:

Risk management functions shall be established by management to help build and monitor the first line controls.

12.2.1 Risk Management Function

The risk management function supports and facilitates the County's management and oversights risk management processes by:

- Building the County's risk capability and defining the County's risk management practices and framework;
- Developing and implementing the risk management plan;
- Providing guidance and training on risk management processes;
- Supporting management in identifying trends and emerging risks and assessment;
- Assisting management in developing processes and risk treatment action plans;
- Monitoring the adequacy and effectiveness of risk treatment plans, and accuracy and completeness of reporting;
- Escalating identified or emerging risks exposures to the Accounting Officer and the Governance body;
- Monitoring compliance with the risk management policy; and
- Collating risk reports and maintaining risk registers.

12.3 Third Line of Defense:

12.3.1 Internal Audit

- Internal auditors shall through a risk based approach provide independent and objective assurance on the effectiveness of the County's risk management arrangements including reviewing risk management processes, the management and reporting of key risks and giving assurance that risks are correctly evaluated.
- Internal auditors may also be tasked to assist the risk management Function in establishing or improving risk management processes. Such facilitation may include developing the risk management framework and processes, training, identification and evaluation of risks and their reporting.
- Internal Auditors shall take steps to safeguard their independence and refrain from assuming any management responsibility by actually managing risks and or being overall responsible for coordinating risk management activities.
- Internal auditors should not set the risk appetite, impose risk management processes, take decisions on risk responses nor implement risk responses on behalf of management.

12.4 Additional Lines of Defense;

12.4.1 External audit and other external review bodies

These bodies sit outside the County's structure, and also have a role in the overall Governance and control structure of the County. External auditing can be considered as an additional line of defense, providing assurance to the County's Governing Body.

12.4.2 Office of the Auditor General

The Public Audit is applicable to all Entities. Section 7 (1) (a) of the Public Audit Act, requires the Auditor General to give assurance on the effectiveness of internal controls, risk management and overall Governance at national and County Government. It is therefore an expected of all Entities to have in place a risk management system.

12.4.3 National Government

The Kenyan Constitution 2010, Public Finance Management Act, 2012, National Government financial regulations mandates that the National Government has responsibility for capacity building and technical assistance to the public sector. In line with this the National Treasury is mandated to;

- monitor the financial aspects of risk management strategies and Governance structures for the County Government entities;
- design and prescribe and efficient financial management system County Governments;
- monitor and assess the implementation of the Public Finance Management Act and financial regulations;
- Enforce the Public Finance Management Act and financial regulations.

12.4.4 Constitutional Bodies

These are bodies mandated by the constitution to offer oversight. They include;

- Ethics and Anti-Corruption Commission
- Controller of Budget
- Office of the Ombudsman
- County Assembly

13 Types of Risk[1]

Within every department there are three types of risks to be considered. They are;

1. **Strategic-** Risks that are associated with strategic objectives of the County Government. These risks do not change often and are coupled with long term goals.
2. **Operational**- Risks that are related to the ongoing procedures of the County Government. These are either long or short-term risks, depending on the objective. It is important to note these risks are internal (Fraud, Health and Safety, capacity, resourcing, data security) or external (Economic downturn, regulations, extreme weather or pandemics). This type of risk can occur on a regular basis; however the overall impact to the County is often minimal. If not minimal they must be controlled and or treated to acceptable levels
3. **Project** – Risks that are linked to projects and programs within the County Government. This could involve shifting requirements of public expectation, slippage of delivery time frame and overall failure to deliver.

If a project or associated risk is deemed by the County Executive Committee Member to be extreme or high or are determined to have a strategic or operational impact that is above the administrative units risk appetite then a project risk may be moved to a County risk register when it is at its initial stages.

However, in most situations project risks that remain once the project or program reaches the transition to the operational phase need to be entered in the appropriate risk register to facilitate continued monitoring and review.

14 Key Risk Management Stakeholders

Key stakeholders in the risk management process vary from executives to management and front line staff. These individuals may be allocated responsibility for individual risks, controls or treatments and must ensure information is accurate and up to date.

Heads of departments are responsible for the information contained in quarterly reporting and are required to sign off that the information is correct.

Key stakeholders are critical to the Risk Assessment process as they provide fundamental knowledge and expertise when decisions are being made. It is important to identify who should be involved in the risk assessment process.

[1] Detailed risks are in appendix 6

- Internal Stakeholders
    - County Staff
    - Workers Union & Associations

- External stakeholder's also need to be considered in the risk management process. Key External Stakeholders
    - Nyandarua County Residents
    - Local Political Leaders
    - Faith Based Organizations
    - Donors
    - Contractors and Suppliers
- Other External Stakeholders
    - Media houses
    - Political Activists
    - Bloggers and social media influencers

The above list of stakeholders is not exhaustive but meant to be indicative of the Risk management stakeholders. The stakeholders listed above shall include other relevant stakeholders to this framework and related policies, who engage with the country or who may engage the county in future.

15 Risk Appetite and Tolerance

Risk Appetite Articulates the entities risk criteria - a statement that influences and guides decision making, clarifies strategic intent and ensures choices align with the capacities and capabilities. Otherwise defined as the amount of risk on a governing body level an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and influences the entity's culture and operating style. Risk Appetite guides resource allocation and assist in aligning the people, and process in designing infrastructure necessary to effectively respond to and monitor risks."

Risk tolerance is the acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as the objectives. In setting risk, tolerance management considers the relative importance of the related objectives and aligns risk tolerances with risk appetite. Operating within risk tolerances helps ensure that the entity remains within its risk appetite, in turn, that the entity will achieve its strategic objectives.

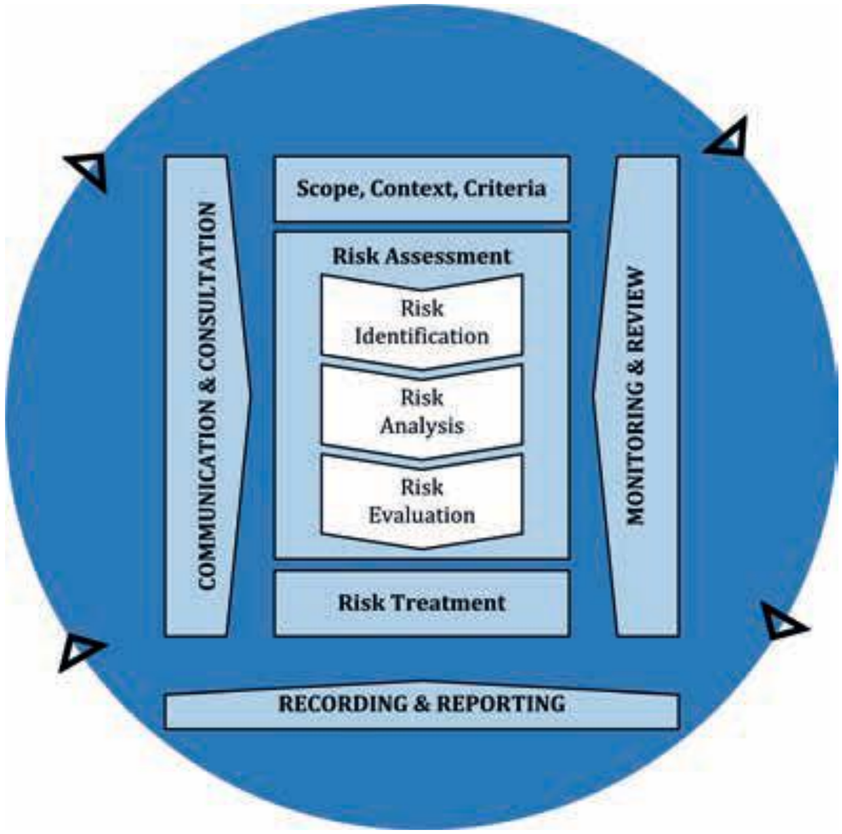
Through articulating risk appetite, the Governing Body establishes the playing field in which the county government must operate, providing boundaries within which the strategy can be executed. The risk appetite is set based on external stakeholder expectations and **risk capacity**.

The choice of strategies and the operational decisions that are made to pursue the County's objectives should be aligned to the risk appetite, risk target and risk tolerances. Appendix 2 contains a sample risk appetite.

16 Steps in Risk Management Process

- Establish the Context
- Identify the risks
- Analyze the Risk
- Evaluate the Risk
- Treat the Risk
- Communication and Consultation (Continuous)
- Monitoring and Review(Continuous)

A diagram representation is shown below;



17 Risk Management Reporting

Risk reporting involves a structured process to record information at each stage of the risk management process. The County Government maintains a risk register, which enables monitoring, review and prioritization of risks. The risk register is based on the County operational structure and incorporates the County Government's strategic objectives.

The accuracy of the risk register is the responsibility of the risk management team together with heads of department through formal training sessions and specific risk assessments.

The risk register provides evidence of risks having been systematically identified, analyzed and treated on a continual basis by departments. Risks may change regularly and without warning, so the registers should be maintained as a "living" database to accurately record the risk management process, the effectiveness of internal controls and progress of risk treatments.
Reports are submitted on a quarterly basis to the Audit Committee.

17.1 Risk Escalation Table

The table contained in Appendix 5 has been designated to demonstrate how risks are first identified and the recorded on the risk register. The table details various level of escalation for risks outside the department risk appetite are referred to senior levels and governing body. It should also be noted that risks can also be downgraded.

Appendices to the framework

18 Appendix 1. Risk Management Plan

Element	Description	When	Who
Define Scope and objective of County activities	Risk management will be incorporated into normal County activities including planning, decision making and operational processes, leading to the achievement of County Government goals.	Annually	Management
Risk Management Policy	Policy review is every year. This allows for any updates and administrative changes to be incorporated into the policy and keep the information as contemporary as possible.	Annually	Senior Management
Risk Management Framework	A review every two years of the framework allows the County Government to continually improve its processes without deviating too far from the policy and procedures.	Biennially	Risk Management Function
Risk Assessments	Formal risk assessment workshops are to be undertaken as part of the annual operational plan cycle.	Annually	All administrative County
Roles and responsibilities	Roles and responsibilities are reviewed on a quarterly basis during the reporting cycle. If responsibilities for risks, controls or treatments have changed, it will be reflected in the report.	Quarterly	All administrative County
Training and education	Risk awareness training to be done	Bi-annually	Risk Management Function

Risk Management Reporting Process	Heads of Directorates review risk registers on a quarterly basis and report to the Accounting Officer. The accounting officer reports to the CECM	Quarterly	All administrative Entities
Escalation Process (Appendix 5)	Any risks that have a high or extreme controlled level of risk OR have controls rated as less than effective require treatment plans. If the treatment plan does not reduce the level of risk or increase control effectiveness, the risk is required to be escalated to Senior management for further attention. The Risk Management committee to further review the risk and determine whether the risk is to be on the strategic risk register.	As required	All administrative Entities
Risk Treatment Plans	Risk treatment plans exist where a risk has a controlled level of risk rated as either extreme or high, or the control effectiveness has been rated as less than effective. These treatment plans are reviewed on a regular basis by the risk, control and treatment owners however they are only reported on a quarterly basis.	Quarterly	All administrative Entities
Communication	Communication and consultation occurs on a regular basis to ensure key stakeholders (both internal and external) are consulted, engaged and actively involved throughout the risk management process. This promotes a consolidated awareness of the department's risk management system and influences behavioral shifts in relation to management of risks. The County Government also has regular Risk Assessment workshops sharing of information and entrenching the culture of risk management.	Continually	Risk Management Function
Monitor and Review	This allows for lessons learned to be identified and applied to continuously improve upon the risk management framework and associated practices. This encourages and increases the successful achievement of strategic and operational objectives.	Quarterly	All administrative Entities

19 Appendix 2. Sample Risk Appetite /Tolerance Matrix

Category	Item	Green (Appetite)	Amber (Tolerance)	Red (Limit)	Internal Monitoring & Reporting	External Monitoring & Reporting
Financial	Monetary value of Financial impact of Identified risks, after mitigation	2.5% of budget or ≤ Kshs----	Between 2.5 and 5% budget or between xxx and xxx Kshs	>5% of the budget or xxx Khs	Relevant committee: > Kshs xxx or 4% of Budget Governing Body: >Kshs or 10% of budget	if deemed appropriate by Governing Body
Strategic	Strategic impact on Department measured against set KPIs	No appetite- KPI targets are met	Minor KPI target(s) are not met	we will not meet key strategic objective(s) as per legislation	Relevant committee: Minor KPI target not met. Governing Body: Will not meet a strategic objective	if deemed appropriate by Governing Body
Operational	Lack of quality in response to stakeholder requirement	0 complaints From individual stakeholders	< 2 complaints from Individual stakeholder	> 2 complaints from Individual stakeholder	Relevant committee: if >2 working days or >2 complaints from individual stakeholder Governing Body: if deemed appropriate by committee	if deemed appropriate by Governing Body
	Unavailability and / or system(s) failure	1 working day	< 2 working days	>2 working days		
	Unable to provide core services	1 working day	< 2 working days	>2 working days		
Reputational	Adverse media Coverage and/or public attitude	No Adverse media coverage	Critical articles in press and / or public criticism from regulatory body	Ministerial concern or Comparable political repacussions	Relevant committee: Critical article in press or criticism from regulatory body or < 2 concurrent complaints from individual stakeholder Governing Body: Anything involving political repercussion or >2 concurrent complaints	if deemed appropriate by Governing Body
	Loss of stakeholder confidence	0 complaints from Individual stakeholders	< 2 complaints From individual stakeholder	> 2 complaints From individual stakeholder		
Compliance	Confirmed and qualified breaches of Compliance and/or Regulatory requirements	Compliance with all Standards internal and external	Minor noncompliance with internal standards or protocols	Noncompliance with Regulatory and/or other compliance requirements	Governing Body: if deemed material by committee	if deemed appropriate by Governing Body

20 Appendix 3. Detailed Risk Management Process

20.1.1 Establish the context

To establish the context of the work environment, relevant stakeholders must meet to determine what the objectives are and understand what the internal and/or external environment is e.g. legal, cultural, political, socio-economical, physical and day-to-day aspects of County Government functions.

When the internal and external context is understood, the risk management context, can then be established. The scope and boundaries of where the risk management process will be applied must be clearly defined, taking into consideration both the costs and benefits of risk management

Questions are useful when establishing the context. Questions can relate to Department, Administrative unit or even a particular team and their function. Key questions to ask when establishing the context may include:

External

• What is the Purpose/Mission/Objective/s of our County Government unit?

• What threats do you see that may affect the achievement of our administrative unit's goals and objectives?

• What opportunities do you see that could enhance the achievement of our goals and objectives?

Internal

• What are the strengths and weaknesses of our County Government unit?

• Who are our internal and external stakeholders?

• How is our unit accountable to our stakeholders?

Sources and categories of risk also provide assistance in establishing the context.

20.1.2 Identify the risks

Identification is the first step in the risk assessment process. A list of potential things that could stop the County from achieving its goals must be developed.

This list should always be wide-ranging, as unidentified risks can cause major losses through missed opportunities or adverse events. 'Brainstorming' will always produce a broad range of ideas and all should be considered.

Relevant stakeholders are considered to be the subject experts when considering potential risks and should be included in all risk assessments being undertaken. Key risks can then be identified and captured.

The **Sources and Categories** of Risk template can be useful in this step to determine which area the risk falls under. When identifying risks, consider:

- **What** can happen?
- **Why** will it happen?
- **Where** will it happen?
- **When** will it happen?
- **How** will it happen?

During this step, opportunities for enhancement or gain across the administration may also be identified. Risks may emerge through other administrative operations including policy and procedure development, internal and external audits, stakeholder complaints, incidents and systems analysis.

A formal risk assessment is not the only process through which risks are identified.

20.1.3 Analyze the risk

The second step in the risk assessment process is to analyze the risk. This means understanding the essence of the risk and determining the causes and consequences, as well as identifying any existing controls.

Existing controls are things already in place such as policies, procedures, training programs etc. These must be rated as either effective; requires improvement; or ineffective. Once this has occurred, the level of risk can be ascertained using the risk assessment matrix.

The County Government has created a risk assessment matrix based on its 'risk appetite' and what is and isn't acceptable within the County Government structure. The County is not prepared to accept a controlled level of risk above moderate and therefore anything above that rating must have controls recorded as less than effective and have a treatment plan put in place.

However, there are circumstances where a risk with a controlled, high or extreme level of risk is not treated due to the financial impact and therefore the risk will remain at this level. Should this occur, an explanation from the risk owner must be recorded.

Risk descriptions describe the risk, its causes and its consequences. The risk description is a short, contextual statement; the causes and consequences should center on the context of the risk.

Control descriptions describe what the control is, what it does, who performs it and how it is done. If the control is a process or task performed by a particular role (committee, unit or person), they must be named in the control description. The control owner is not always the person undertaking the process or task.

Not every control will require every component; however, the description must reflect exactly how the control is working. If it requires improvement, the weakness of the control should also be captured on the risk register.

<u>Treatment descriptions</u> describe what the treatment is, what action is required and who performs the task. As with controls, the person undertaking the task is not always the treatment owner and therefore must be identified in the description.

20.1.4 Evaluate the risk

Risk evaluation uses the information obtained during the analysis to make decisions about whether the risk is acceptable in its current state or whether further action needs to be taken to mitigate the risk. A decision must be made regarding whether treatments need to be implemented and then the priority of treatments established.

The County Government Risk Assessment Matrix should be used to determine the levels of risk at the inherent and controlled stages. The control effectiveness is also considered at this point and plays a part in the decision whether treatments are then required.

The County has ascertained that:

• Any risk where controls are less than effective require a treatment plan;

• Risks that are rated at the controlled level of risk as extreme or high must have the **control effectiveness** rated as **'requires improvement'** or **'not effective'** and therefore a treatment plan;

• Risks that are rated at the controlled level of risk as either moderate or low can be accepted and monitored, if the **control effectiveness** has been assessed as **'effective'**.

An accepted risk does not mean that the risk is insignificant, rather that:

• The inherent or controlled Level of Risk is low/moderate and does not warrant using resources to treat it;

• No treatment is available;

• Treatment costs are prohibitive;

• Opportunities significantly outweigh the threats;

20.2 Treat / action the risk

Treating / actioning the risk involves selecting measures that contribute to either mitigating the risk or strengthening current controls. It is probable that a combination of options will be required to treat complex risks. The most suitable risk treatment / action options are generally:

20.2.1 Risk Acceptance:

When all treatment options have been explored and there is no course of action likely to be effective, or the option will cost more than the benefits gained. Risks may also be accepted when the risk is of low consequence and unlikely to occur. This may require an explanatory note from the risk owner if the controlled level of risk is rated at extreme or high.

20.2.2 Risk Retention:

When, after careful analysis, it is identified the risk cannot be avoided, reduced or transferred, or where the cost to do so is not justified, it is retained as a risk. This requires an explanatory note from the risk owner stating the situation and awareness of the status of the risk.

20.2.3 Risk Avoidance:

Risk avoidance occurs when stopping or not proceeding with the activity, or choosing an alternative, eliminates the risk. **This is not often an option in the public sector.**

20.2.4 Risk Transfer:

Risks may be transferred to other parties. This may include, for example, taking out insurance policies, outsourcing activities or moving operations to an area of the County better placed to handle the risk.

20.2.5 Risk Control *(reduce the likelihood and/or consequence of the event):*

Controlling risk is where the majority of effort is generally required. Management processes, such as audit and compliance programs, preventative maintenance and training of employees are some methods that reduce risks.

Ensuring that controls are in place, such as contingency plans, evacuation procedures or structural barriers, may reduce the consequences. This element also incorporates evaluating the options, preparing treatment / action plans and implementing these plans. The treatment plan may incorporate one or more of the above options and will document how chosen treatment options will be implemented.

Information that needs to be included in treatment plans includes:

- The name of the selected treatment;
- Treatment / action owner and those responsible for implementing the plan;
- What will be happening?
- When will it happen?
- The original due date and the current due date (which can either be brought forward or go beyond the original date);

Treatment / action plans should be integrated with the risk management reporting process of the administrative unit and discussed with appropriate stakeholders.

Decision makers and other stakeholders need to be involved in determining the treated level of risk i.e. the level of risk after the treatment / action has taken place. The treated level of risk must be recorded on the **electronic risk register** and subjected to monitoring, review and, where appropriate, further treatment / action. Treatment / action plans can also be implemented following recommendations provided by internal or external audit following a review.

20.3 Interactive steps in the risk management process

There are two ongoing themes are constant throughout the risk management process, these are:

20.3.1 Communication and consultation

Effective communication and consultation are essential to ensure that those responsible for managing risk, and those with a vested interest, understand the basis on which decisions are made, for example, why particular treatment / action options are selected.

20.3.2 Monitoring and review

Monitoring and review is essential.

During the quarterly reporting process, heads of departments must review risks within their area and follow up on controls and treatments / action that are mitigating these risks. Any action that is out of date and requires further attention can thus be identified. As well, completed treatments could be converted to controls; levels of risk confirmed and risks may be retired or escalated.

Monitoring and reviewing risks, controls and treatments also apply to any actions / treatments from Internal Audit. The audit report will provide recommendations that effectively are treatments for controls and risks that have been tested during an internal review.

20.3.3 Retiring a risk

Retirement of a risk occurs when the County Government no longer considers the risk relevant; in existence; or mitigated to a point where the risk is accepted. However, this can only occur when the controlled level of risk is either moderate or low.

Risks are retired for a variety of reasons and can be reactivated should there be a change in the County objectives or internal/external environment. Retired risks are not deleted from the risk register but may be archived after a period of time.

19. Appendix 4. County Government of Nyandarua Risk Assessment Matrix

19.1 Likelihood and consequence Matrix

	1- Insignificant	2 - Minor	3 - Moderate	4 - Major	5 - Catastrophic
5 - Almost Certain	High	High	High	Extreme	Extreme
4 - Likely	Moderate	Moderate	High	High	Extreme
3 - Possible	Low	Moderate	Moderate	High	High
2 - Unlikely	Low	Low	Moderate	Moderate	High
1 - Rare	Low	Low	Low	Moderate	Moderate

19.2 Risk Likelihood Descriptors

Level	Descriptor	Qualitative	Frequency of occurring in %
5	Almost Certain	The risk is already occurring, or is likely to occur more than once within the next 12 months.	80-100%
4	Likely	The risk could easily occur, and is likely to occur at least once within the next 12 months	60-80%
3	Possible	There is an above average chance that the risk will occur at least once in the next 3 years.	40-60%
2	Unlikely	The risk occurs infrequently and is unlikely to occur within the next 3 years.	20-40%
1	Rare	The risk is conceivable but is only likely to occur in extreme circumstances.	0-20%

21 Appendix 5. Risk Action and Escalation Matrix

Risk Zone	Meaning	Action Required For Risk	Risk Escalation
	Unacceptable/Catastrophic Risks that require urgent attention. Not permitted unless approved by the Governing Body	**Urgent action** required. Reduce the level of risk to major or below. Investigate and take steps to mitigate or avoid within a specified **short term (1 month)** period.	County Executive Committee Members/Governing Body
	Significant/Major Risks that require prompt action. Only acceptable if it is not practicable or efficient to reduce the level of risk	Reduce the level of risk to medium or below. **Prompt action** required, complete within three (3) months.	Accounting Officer/ CECM
	Tolerable/Moderate Risks. Are acceptable to a limited period of time to allow treatment to be in keeping with the entity/project objectives.	Treat as soon as possible but within one year. **Weighted action required** - Risks will be treated as long as the costs do not outweigh the benefits.	Heads of Directorate / Departments
	Acceptable/Minor risks. Plan to treat in keeping with other priorities.	**Periodic monitoring.** Ongoing controls as part of general or routine management activates.	Heads of Sections
	Insignificant Risks to be monitored and managed with existing controls	Can be dealt with internally	No escalation required

22 Appendix 6: Sample Risk Categories

Category Description	Category Description
Strategy risks	Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).
Governance risks	Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.
Operations risks	Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service quality and/or quantity of service), non-compliance and/or poor value for money
Legal risks	Risks arising from a defective transaction, a claim being made (including a defense to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).
Property Risk	Risks arising from property deficiencies or poorly designed or ineffective/ inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.
Financial Risks	Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources Deployed, and/or non-compliant financial reporting.
Commercial Risks	Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and /or failure to meet business requirements/objectives.
People risks	Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviour, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.
Technology risks	Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.
Information risks	Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data / information to its full potential.
Security risks	Risks arising from a failure to prevent unauthorized and/or inappropriate access to the estate and information, including cyber security and noncompliance with General Data Protection Regulation requirements.

Project/Programme risks	Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.
Reputational risks	Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

Failure to manage risks in any of these categories may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, customer and operational consequences.