

ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026



Province of the
EASTERN CAPE
COOPERATIVE GOVERNANCE
& TRADITIONAL AFFAIRS

ENTERPRISE – WIDE RISK MANAGEMENT
POLICY
2026

SERVING OUR COMMUNITIES BETTER



ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026

Contact Details	
Physical Address	Tyamzashe Building Phalo Avenue Bhisho 5605
Postal Address	Department of Cooperative Governance and Traditional Affairs Private Bag X0035 Bhisho 5605
Document Number	1
Document Name	Enterprise - Wide Risk Management Policy
Contact Person	Mrs N Mosehana
Designation	Director
Component	Risk, Anti – Corruption & Integrity Management
Telephone No.	
Cell Phone No.	082 0700 431
E-mail Address	<u>nomathamsanqa.mosehana@eccogta.gov.za</u>
First Approval	25 July 2012
Last Reviewed	01 April 2023
Current Review	01 April 2026
Next Review Date	31 March 2031

POLICY STATEMENT

Head of Department

Executive Authority
Initials E-A-W

HOD
Initials u

ENTERPRISE – WIDE RISK MANAGEMENT POLICY 2026

The Accounting Officer commits the Department of Cooperative Governance and Traditional Affairs to an **Enterprise – Wide Risk Management** that is aligned to the principles of good corporate governance, as supported by the Public Finance Management Act (PFMA), Act No 1 of 1999 and other applicable pieces of legislation.

An integrated Risk Management approach applied at macro and micro levels of the Department enhances fulfilment of Department's mandate, as well as service delivery expectations of the public and the performance expectations within the Department.

The Department defines and adopts an Enterprise – Wide Risk Management approach, as a coordinated management effort, that enables the Department to appropriately respond to risks towards the achievement of Departmental outcomes.

Sound management of risks will enable the Department to anticipate, respond and monitor changes in our environment, as well as taking informed decisions under conditions of uncertainties. This policy, therefore, sets out the components that provide for foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving management of risks throughout the Department.

It is expected that all programmes, operations, and processes will be subject to the Risk Management Implementation Plan. It is the intention that the programmes will work together in a consistent and integrated manner, with the overall objective of reducing risks, as far as reasonably practicable.

ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026

SIGN OFF

1. Head of Department

This Policy on the Whistleblowing has been recommended by Mr. V. Mlokothe in his capacity as Head of Department for the Eastern Cape Department of Cooperative Governance and Traditional Affairs.

I am satisfied and concur with the contents of this Policy.

The development of this policy will ensure that the department complies with the provisions of section Protected Disclosures Act, (No. 26 of 2000)

SIGNED:	 MR. V. MLOKOTHI
DESIGNATION:	HEAD OF THE DEPARTMENT
DATE:	23/07/2026

2. Executive Authority

The department of Cooperative Governance and Traditional Affairs has an opportunity to improve the livelihoods of the people by effectively rendering the many services that it is expected to provide. We have envisaged a department that has the required capacity to respond adequately to challenges of its people.

I therefore trust that guidance from this Policy will contribute to the effective fulfilment of the departmental mandate, the service delivery expectations of the public and the performance expectations within the department.

SIGNED:	 MR. Z.A WILLIAMS
DESIGNATION:	MEMBER OF THE EXECUTIVE COUNCIL
EFFECTIVE DATE:	12.08.2026.

ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026

TABLE OF CONTENTS		
No.	ITEM	PAGE
1.	INTRODUCTION	6
2.	LEGISLATIVE FRAMEWORK	6
3.	POLICY OBJECTIVES	7
4.	ENTERPRISE-WIDE RISK MANAGEMENT PRINCIPLES	7
5.	SCOPE AND APPLICABILITY	8
6.	ERM METHODOLOGY	8 - 9
7.	BENEFITS OF RISK MANAGEMENT PROCESS	10
8.	ROLES AND RESPONSIBILITIES	10 - 13
9.	RISK MANAGEMENT COMMITTEE	14
10.	POLICY REVIEW	15
11.	VERSION CONROL AND CHANGE HISTORY	15-16
12.	KEY RISK MANAGEMENT VOCABULARY	17-27

ENTERPRISE – WIDE RISK MANAGEMENT POLICY 2026

1. INTRODUCTION

Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is a “**risk**”.

Management cannot be expected to deal in a structured, planned, and confident manner with unexpected events or unexpected opportunities, if such events are not planned for.

Therefore, Risk Management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to achieve its objectives and build value.

Features and activities of the Enterprise – Wide Risk Management process are outlined in the Department’s Risk Management Implementation Plan.

The Risk Management policy considers the following additional broad areas of risk:

- Departmental Strategy
- Policy Development and Implementation
- Operations (Systems, Processes and People)
- Technological Factors
- Legal Compliance
- External Factors
- Change in Conditions

2. LEGISLATIVE FRAMEWORK

Sections 38(1) (a) (i) of the PFMA

The Accounting Officers for a department must ensure that their department has and maintains effective, efficient, and transparent systems of risk management and internal controls.

Public Sector Risk Management Framework of 2025 – Chapter 3.7

The Institution must operate within the terms of a risk management policy approved by the Accounting Officer and Executive Authority

**ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026**

The Treasury Regulation 3.2.1

The accounting officer must ensure that a risk assessment is conducted regularly to identify emerging risks of the institution.

3. POLICY OBJECTIVES

The policy:

- Provides a framework for effective identification, assessing, responding, monitoring and reporting of Departmental risks;
- Enhances application of Enterprise-Wide Risk Management to improve risk governance as well as to create a favourable risk management culture;
- Embeds instinctive and consistent consideration of risks in the day-to-day operations;
- Drives specific risk management and control processes to respond to the potential threats and opportunities;
- Provides a common understanding of how the Department, its business processes and people, describe and priorities objectives, risk and control;
- Provides clarity in respect of the roles and responsibilities of the various key stakeholders in the Enterprise Risk Management value chain.

4. EC COGTA ENTERPRISE-WIDE RISK MANAGEMENT PRINCIPLES

The principles contained in this policy will be applied at both strategic and operational levels within the Department and will consider external risks arising from or related to our external stakeholders.

- Our positive approach to risk management means that we will not only look at the risk of things going wrong, but also the impact of not taking opportunities or not capitalising on our corporate strengths.
- All risk management activities will be aligned to organisational values, principles, objectives and organizational priorities, and aim to protect and enhance the reputation and standing of the Department.
- Risk Management will form part of the strategic planning processes and will also be integral to the risk-based Internal Audit planning and approach.

ENTERPRISE – WIDE RISK MANAGEMENT POLICY 2026

- Our risk management approach will inform and direct our work to gain confidence on the reliability of our risk controls strategies and therefore provide assurance.
- Employees at all levels will have a responsibility to identify, evaluate and manage or report risks, and will be equipped to do so.
- Risk, Anti-Corruption & Integrity Management will have free access to information.

5. SCOPE AND APPLICABILITY

All Cooperative Governance and Traditional Affairs stakeholders (internal and external) have a role to entrench a culture of risk management in the Department.

6. ERM METHODOLOGY

6.1 Establishing the Context

The process of risk management starts by defining the outcomes that the department wants to achieve, how it intends to achieve these Departmental outcomes, and which factors (both internal and external) may prevent the achievement of those goals.

6.2 Risk assessment

This process identifies what could cause the Department to deviate from its Departmental outcomes, to determine how likely it is to happen, as well as what the consequences could be if it does happen. Risk assessment also determines which risks need to be addressed first, which risks are less urgent, and which risks do not warrant intervention.

6.3 Risk response

Once risks have been identified, assessed, and evaluated there will be enough information to begin the process of responding to the risks. This involves selecting the options for modifying and/or mitigating the identified risks and implementing these options.

ENTERPRISE – WIDE RISK MANAGEMENT POLICY 2026

Risk response:

- Accepting or tolerating the risk
- Manage or treat the risk
- Terminate risk source or avoid the risk
- Transferring the risk

6.3.1 Risk Appetite Framework:

The risk response strategy considers the approved Risk Appetite Framework where the risk appetite and risk tolerance parameters are articulated in detail to inform the response strategy to be implemented on the identified risks.

The table below should inform the risk response option (for each risk) that must be selected.

Risk value (%)	Risk magnitude	Risk acceptability	Proposed actions
80 – 100	Maximum	Unacceptable	Take action to reduce risk with highest priority.
61 – 79	High risk	Unacceptable	
31 – 60	Medium risk	Unacceptable	Take action to reduce risk.
21 – 30	Low risk	Partially Acceptable	Control and monitor
1 – 20	Minimum risk	Acceptable	No risk reduction - control,

6.4 Monitoring and reporting

Monitoring and reviewing ensures that the risk management process works in accordance with the Departmental policy, and that it happens at the appropriate level.

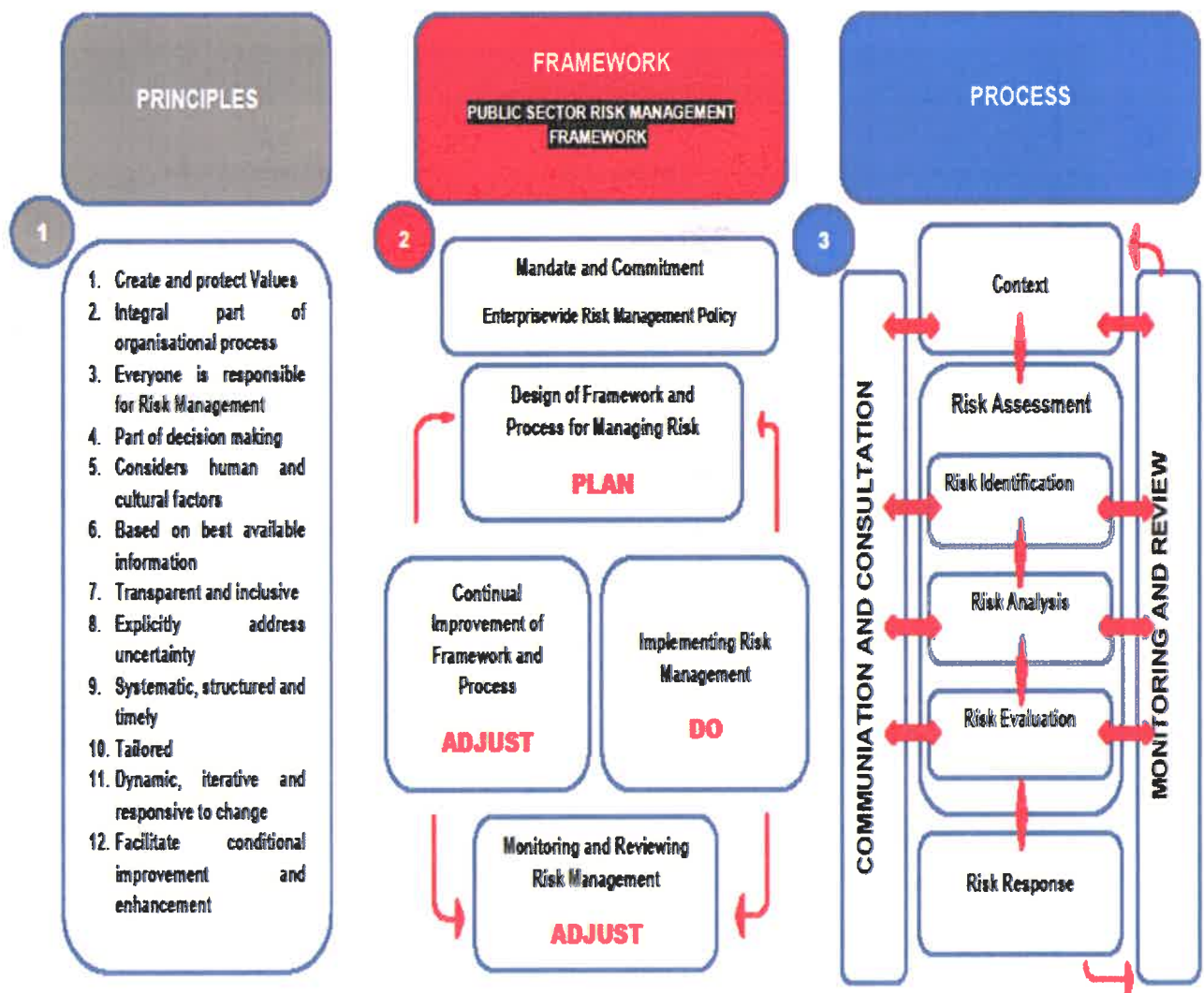
The approved annual Departmental Risk Management Implementation Plan details how risks will be monitored and reported i.e.

- Use of Risk Coordinators Working Group.
- Risk Management Monthly Monitoring. (Quarter 1, 2 and 3)
- Discussions with Management and other employees
- Reports on management of risks to the Oversight Structures.

ENTERPRISE – WIDE RISK MANAGEMENT POLICY 2026

Management reports progress on strategic risks directly to the office of the Head of Department, while operational risks are reported to the office of the Chief Risk Officer.

ERM METHODOLOGY based on ISO 31000



ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026

7. BENEFITS OF EFFECTIVE ERM

Effective implementation of the ERM process will assist the Department to achieve, among other things, the following outcomes needed to underpin and enhance performance:

- Informed decisions underpinned by appropriate rigor and analysis;
- Increasing probability of achieving Departmental outcomes;
- Increased efficiency, effectiveness, and economy of operation;
- Improved level of compliance;
- Identify opportunities for continuous improvement;
- Avoid certain audit adverse outcomes; and
- Reduce the potential loss of resources.

8. ROLES AND RESPONSIBILITIES

8.1 Executive Authority

The Executive Authority shall take an interest in risk management to the extent necessary to obtain comfort that properly established and functioning systems of risk management are in place to protect the Department against significant risks.

High level responsibilities shall include:

- Ensuring that the Department strategies are aligned to the government mandate;
- Obtaining assurance from management that Department's strategic choices were based on a rigorous assessment of risks;
- Obtaining assurance that key risks inherent in Department's strategies were identified and assessed, and are being properly managed;
- Assisting the Accounting Officer to deal with fiscal, intergovernmental, political and other risks beyond their direct control and influence;
- Insist on the achievement of outcomes, effective performance management and value for money.
- Instil a culture of accountability, and efficiency.

ENTERPRISE – WIDE RISK MANAGEMENT POLICY

2026

8.2 Head of Department

The Head of Department is accountable for the overall governance of risk. By setting the tone at the top, he promotes accountability, integrity and other factors that will create a positive control environment.

High level responsibilities shall include:

- Setting an appropriate tone by supporting and being seen to be supporting the Department's aspiration for effective risk management;
- Holding Management accountable for designing, implementing, monitoring and integrating risk management into their day-to-day activities;
- Delegating responsibilities for risk management to Management and governance committees;
- Providing leadership and guidance to enable Management and internal structures responsible for various aspects of risk management to properly perform their functions;
- Ensuring that the control environment supports the effective functioning of risk management;
- Ensuring appropriate action in respect of the recommendations of the Audit Committee, Internal Audit, External Audit and Risk Management Committee to improve Risk Management processes.

8.3 Management (Risk Owners and Action Owners)

Management is responsible to integrate risk management into the operational routines.

High level responsibilities of Management should include:

- Risk management as a Key Performance Area in the Performance Agreement;
- Identifying risks within their line function;
- Designing and implementing controls to mitigate identified risks;
- Devoting personal attention to overseeing the management of key risks within their area of responsibility;
- Periodically review the adequacy & effectiveness of existing control systems and risk response strategies;

ENTERPRISE – WIDE RISK MANAGEMENT POLICY 2026

- Aligning the functional risk management methodologies and processes with the Departmental process (APP, OPS etc);
- Holding employees accountable for their specific risk management responsibilities;
- Monthly reporting of the management of risks to the Accounting Officer.

8.4 Risk Champions (DDGs)

The Risk Champion is a person with the skills, knowledge, leadership qualities and power of office required to Champion a particular aspect of risk management and ensure the adequate management of strategic risks and high operational risks.

High level responsibilities of Risk Champions should include:

- A key part of Risk Champions' responsibility involves intervening in instances where the risk management efforts are being hampered, for example, by lack of co-operation by Management and other officials.
- The Risk Champion may also add value to the risk management process by providing guidance and support to manage "problematic" risks and risks of a transversal nature that require a multiple participant approach.
- The Risk Champion must not assume the role of Risk Owner but should assist the Risk Owner to resolve problems and account to the Risk Champion.

8.5 Risk Coordinators

Risk Coordinators are identified by their Risk Owners and formally designated by the Accounting Officer:

High level responsibilities of Risk Coordinators should include:

- The Risk Coordinator is a person at the middle management level with coordination and interpersonal skills to interact with Action Owners (Directors) in providing support to the Risk Owner (Chief Director).
- Coordinate the Chief Directorate's risk management process / activities.
- Facilitate monthly submission of the Risk Management Monthly Monitoring Tools approved by Risk Owners (Chief Directors).

ENTERPRISE – WIDE RISK MANAGEMENT POLICY

2026

- Attend standing Risk Coordinators working group meetings as per the schedule.
- Interact with the office of the Chief Risk Officer on regular basis.
- Attend workshops facilitated by the Chief Risk Officer.

8.6 Other employees

Other employees are responsible for integrating risk management into their day-to-day activities. They must ensure that their delegated risk management responsibilities are executed and continuously report on progress to their line managers.

High level responsibilities of other employees should include:

- Applying the risk management processes in their respective functions;
- Implementing the delegated action plans to address the identified risks;
- Informing their supervisors and/or the Risk, Anti-Corruption & Integrity Management Directorate of new risks and significant changes in known risks; and
- Co-operating with other role players in the risk management process and providing information as required.

8.7 Chief Risk Officer

The primary responsibility of the Chief Risk Officer is to bring about specialist expertise to assist the Department to embed risk management and leverage its benefits to enhance performance.

The high-level responsibilities of the Chief Risk Officer should include:

- working with senior management to develop the Department's vision for risk management;
- Communicating the Department's risk management framework to all stakeholders in the Department and monitoring its implementation;
- Assisting Management with risk identification, assessment and development of response strategies;
- Monitoring the implementation of the response strategies;
- Reporting about effective management of risks to the Head of Department, Management, the Risk Management Committee and the Audit Committee;

**ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026**

- Participating with Internal Audit and Management in developing the combined assurance plan for the Department.

8.8 Risk Management Committee

The Risk Management Committee is appointed by the Head of Department to discharge their responsibilities for risk management. The membership of the Risk Management Committee should comprise both management and external chairperson with the necessary blend of skills, competencies, and attributes.

The chairperson of the Risk Management Committee should be an independent external person, appointed by the Head of Department. Roles and responsibilities of the Risk Management Committee are defined in its Charter.

8.9 Minimum Frequency of Meetings

Clause: Risk Management Committee Meetings

The Risk Management Committee shall meet at a minimum of once every quarter.

This

aligns with Treasury Regulations 3.2.1 and King IV. Additional special meetings

may be

convened by the Chairperson as and when required to address urgent risk matters.

The

schedule of meetings for the financial year shall be approved at the first meeting of

each

financial year.

8.10 Quorum

Clause: Quorum

The quorum for a meeting of the Risk Management Committee shall be fifty percent

(50%)

plus, one (1) of the appointed members, of which one must be the Chairperson, or

the

Chairperson may request any appointed member to chair the meeting in their

absence. No

decisions shall be taken in the absence of a quorum. If a quorum is not present within

thirty

ENTERPRISE – WIDE RISK MANAGEMENT POLICY 2026

(30) minutes of the scheduled start time, the meeting shall be adjourned and rescheduled.

8.11 Declaration of Conflict of Interest

Clause: Declaration of Interest

All members of the Risk Management Committee are required to **declare any direct or**

indirect interest in any matter tabled for discussion at the beginning of each meeting. Such

declaration shall be recorded in the minutes. A member with a declared conflict of interest

shall recuse themselves from the discussion and decision-making on that item and shall not

participate. Failure to disclose a conflict of interest may result in disciplinary action in line

with the **Public Service Code of Conduct**.

8.12 Audit Committee

The Audit Committee is an independent committee responsible for oversight of the Department's control, governance, and risk management. The responsibilities of the Audit Committee about risk management are formally defined in its charter.

8.13 Internal audit

The role of the Internal Auditing in risk management is to provide an independent, objective assurance on the effectiveness of the Department's system of risk management.

- Internal Auditing must evaluate the effectiveness of the entire system of risk management and provide recommendations for improvement where necessary.
- Internal Audit responsibilities are formally described in the Internal Audit Charter.

8.14 External audit

ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026

The external auditor (Auditor-General) provides an independent opinion on the effectiveness of risk management.

9. POLICY REVIEW

The policy must be reviewed every five (5) years or earlier when the need arises to reflect the current stance on risk management. Every employee has a part to play in this important endeavour.

10. VERSION CONTROL AND CHANGE HISTORY

Version Control	Date Effective	Approved By	Amendment
Start from	YYMMDD (the date the policy takes effect)	Contact person – full name & title.	Include any superseded procedures and what the amendment is to the document.
2013	11 March 2013	Mlibo Qoboshiyane (MEC)	The contents of this policy are all aligned to be in line with departmental policy guideline.
2016	1 April 2016	Fikile Xasa (MEC)	The contents of this policy are all aligned to be in line with departmental policy guideline.
2019	1 April 2019	Xolile Nqata (MEC)	The contents of this policy are all aligned to be in line with departmental policy guideline.
2021	March 2021	Xolile Nqata (MEC)	The contents of this policy are all aligned to be in line with departmental policy guideline.
2023	June 2023	Zolile Williams (MEC)	The contents of this policy are all aligned to be in line with departmental policy guideline.
2026	April 2026	Zolile Williams (MEC)	The contents of this policy are all aligned to be in line with departmental policy guideline.

ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026

11. KEY RISK MANAGEMENT VOCABULARY	
Basic Terms	
Accounting Officer	An employee responsible for the overall day-to-day operations of the organisation ultimately accountable for Risk Management amongst other responsibilities.
Chief Risk Officer (CRO)	A paid executive of the organisation, who may have other duties/responsibilities, but who is <i>primarily</i> responsible for advising on, formulating, overseeing and managing all aspects of the organisation's risk management system; and monitors the organisation's entire risk profile, ensuring that major risks are identified and reported upwards. The CRO provides and maintains the risk management infrastructure to assist the Board of Directors and executive management team in fulfilling their risk management responsibilities.
Risk Managers / Risk Facilitators	Employees of the company who assist the CRO and Head of Risk in the fulfilment of their duties. These persons can have an alternative reporting line to the CRO or report directly to the CRO .
Internal Audit	an independent assurance function authorised to assess the control environment within the organisation in accordance with definition for internal audit
Objectives	Goals that management have set for the company or a department to achieve.

**ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026**

11. KEY RISK MANAGEMENT VOCABULARY	
Cost of Risk	Costs associated with: • Insurance premiums • Self-retained losses (incurred loss) • Loss control expenses including safety, security, property conservation, quality control programs, etc. • Administrative costs (internal and external) including risk management department, internal claims staff, fees paid to brokers, risk management consultants, outside claims and loss control services, plus your time as risk manager and / or claims administrator.
General Risk Management Terms	

ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026

	11. KEY RISK MANAGEMENT VOCABULARY
Risk	Risk is an effect of uncertainty on objectives (outcomes): Note 1: An effect is a deviation from the expected — positive and/or negative. Note 2: Objectives can have different aspects (such as financial, health and safety and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product and process). Note 3: Risk is often characterized by reference to potential events and consequences or a combination of these. Note 4: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. Note 5: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.

ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026

11. KEY RISK MANAGEMENT VOCABULARY	
Risk Management Framework/Strategy	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. Note 1: The foundations include the policy, objectives, mandate and commitment to manage risk. Note 2: The organisational arrangements include plans, relationships, accountabilities, resources, processes and activities. Note 3: The risk management framework is embedded within the organisation's overall strategic and operational policies and practices.
Risk Management Policy	Statement of the overall intentions and direction of an organisation related to risk management.
Risk Management Implementation Plan	Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk. Note 1: Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities. Note 2: The risk management plan can be applied to a particular product, process and project, and part or whole of the organisation.
Risk Management Process Terms	

**ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026**

	11. KEY RISK MANAGEMENT VOCABULARY
Risk Management Process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.
Step 1: Communication and Consultation	
Communication and Consultation	- Continual and iterative processes that an organisation conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk. Note 1: The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of the management of risk. Note 2: Consultation is a two-way process of informed communication between an organisation and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is: • a process which impacts on a decision through influence rather than power; • An input to decision making, not joint decision making.
Interested Party	- Person or group having an interest in the performance or success of an organisation. Example: Customers, owners, people in an organisation, suppliers, bankers, unions, partners or society, regulators and government.
Stakeholder	- Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
Risk Perception	- Stakeholder's view on a risk. Note 1: Risk perception reflects the stakeholder's needs, issues, knowledge, belief and values.

ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026

11. KEY RISK MANAGEMENT VOCABULARY	
Step 2: Establishing the Context	
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.
External Context	- This is external environment in which the organisation seeks to achieve its objectives. Note 1: External context can include: • the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; • key drivers and trends having impact on the objectives of the organisation; and • relationships with, and perceptions and values of external stakeholders

ENTERPRISE – WIDE RISK MANAGEMENT POLICY 2026

11. KEY RISK MANAGEMENT VOCABULARY	
Internal Context	- Internal environment in which the organisation seeks to achieve its objectives. Note 1: Internal context can include: • governance, organisational structure, roles and accountabilities; • policies, objectives, and the strategies that are in place to achieve them; • the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies); • information systems, information flows and decision-making processes (both formal and informal); • relationships with, and perceptions and values of internal stakeholders; • the organisation's culture; • standards, guidelines and models adopted by the organisation; • Form and extent of contractual relationships.
Risk Criteria	- Terms of reference against which the significance of a risk is evaluated. Note 1: Risk criteria are based on organisational objectives, and external and internal context. Note 2: Risk criteria can be derived from standards, laws, policies and other requirements.
Step 3-5: Risk Assessment	
Risk Assessment	- Overall process of risk identification, risk analysis and risk evaluation.
Step 3: Risk Identification	

ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026

	11. KEY RISK MANAGEMENT VOCABULARY
Risk Identification	- Process of finding, recognising and describing risks. Note 1: Risk identification involves the identification of risk sources, events, their causes and their potential consequences Note 2: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.
Risk Description	- Structured statement of risk usually containing four elements: sources, events, causes and consequences.
Risk Source	- Element which alone or in combination has the intrinsic potential to give rise to risk. Note 1: A risk source can be tangible or intangible.
Event	- Occurrence or change of a particular set of circumstances. Note 1: An event can be one or more occurrences and can have several causes. Note 2: An event can consist of something not happening. Note 3: An event can sometimes be referred to as an “incident” or “accident”. Note 4: An event without consequences (3.6.1.3) can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.
Hazard	- Source of potential harm. Note 1: Hazard can be a risk source.
Key Risks	- Identifying risks which the organisation perceives to be its most significant risks.
Risk Owner	- Person or entity with the accountability and authority to manage a risk.

**ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026**

Step 4: Risk Analysis	
Risk Analysis	- Process to comprehend the nature of risk and to determine the level of risk. Note 1: Risk analysis provides the basis for risk evaluation and decisions about risk treatment. Note 2: Risk analysis includes risk estimation.
Likelihood / Probability	- Chance of something happening. Note 1: In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically [such as a probability or a frequency over a given time period. Note 2: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.
Exposure	- Extent to which an organisation and/or stakeholder is subject to an event.
Consequence / Impact / Severity	- Outcome of an event affecting objectives. Note 1: An event can lead to a range of consequences. Note 2: A consequence can be certain or uncertain and can have positive or negative effects on objectives. Note 3: Consequences can be expressed qualitatively or quantitatively. Note 4: Initial consequences can escalate through knock-on effects.

ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026

Probability as a Measure	- Measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty.
Frequency	- Number of events or outcomes per defined unit of time. Note 1: Frequency can be applied to past events or to potential future events, where it can be used as a measure of likelihood / probability.
Vulnerability	- Intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence.
Risk Matrix	- Tool for ranking and displaying risks by defining ranges for consequence (impact) and likelihood (probability).
Level of Risk	- Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood.
Inherent Risk	- The product of the impact of the risk on the objective and the likelihood of the risk occurring, should no management actions/controls be in place to mitigate the risk.
Step 5: Risk Evaluation	
Risk Evaluation	- Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Note 1: Risk evaluation assists in the decision about risk treatment.
Risk Attitude	- Organisation's approach to assess and eventually pursue, retain, take or turn away from risk.
Risk Appetite	- Amount and type of risk that an organisation is willing to pursue or retain.
Risk Tolerance	- Organisation's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives. Note 1: Risk tolerance can be influenced by legal or regulatory requirements.

**ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026**

Risk Aversion	- Attitude to turn away from risk.
Risk Aggregation	- Combination of a number of risks into one risk to develop a more complete understanding of the overall risk.
Step 6: Risk Treatment (also called Risk Response)	
Risk Treatment	- Process of selection and implementation of measures to modify risk. Note 1: Risk treatment can involve: • avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; • taking or increasing risk in order to pursue an opportunity; • removing the risk source; • changing the likelihood; • changing the consequences; • sharing the risk with another party or parties [including contracts and risk financing]; • Retaining the risk by informed decision. Note 2: Risk treatments that deal with negative consequences are sometimes referred to as «risk mitigation», «risk elimination», «risk prevention» and «risk reduction». Note 3: Risk treatment can create new risks or modify existing risks.
Risk Controls	- Actions taken and implemented by management to treat risks and enhance the likelihood that established objectives and goals will be achieved. Note 1: Controls include any process, policy, device, practice, or other actions which modify risk. Note 2: Controls may not always exert the intended or assumed modifying effect.

**ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026**

Risk Acceptance / Risk Retention	- Informed decision to take a particular risk. Note 1: Risk acceptance can occur without risk treatment or during the process of risk treatment. Note 2: Accepted risks are subject to monitoring and review.
Risk Retention / Risk Acceptance	- Acceptance of the potential benefit of gain, or burden of loss, from a particular risk. Note 1: Risk retention includes the acceptance of residual risks. Note 2: The level of risk retained can depend on risk criteria.
Risk Avoidance / Risk Termination	- Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk. Note 1: Risk avoidance can be based on the result of risk evaluation and/or legal and regulatory obligations.
Risk Transfer / Risk Sharing	Sharing with another party the burden of loss, or benefit of gain, of a risk. Note 1: Legal or statutory requirements can limit, prohibit or mandate the transfer of certain risk. Note 2: Risk transfer can be carried out through insurance or other agreements. Note 3: Risk transfer can create new risks or modify existing risk. Note 4: Relocation of the source is not risk transfer.
Risk Financing	- Form of risk treatment involving contingent arrangements for the provision of funds to meet or modify the financial consequences should they occur.
Residual Risk	- Risk remaining after risk treatment. Note 1: Residual risk can contain unidentified risk. Note 2: Residual risk can also be known as «retained risk».
Resilience	- Adaptive capacity of an organisation in a complex and changing environment.

**ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026**

Action Plans	- Tasks/projects that management commit to implementing, after identifying unacceptable risk exposures, in order to return the exposure to within acceptable parameters. Each action plan must have a due date and a resource allocated.
Key Risk Indicators	- Symptoms/signs/events by which key risks can be easily identified.

ENTERPRISE – WIDE RISK MANAGEMENT POLICY
2026

Step 7: Monitoring and Review	
Monitoring	- Continual checking, supervising, critically observing or determining the status of risks in order to identify change from the performance level required or expected. Note 1: Monitoring can be applied to a risk management framework, risk management process, risk or control.
Review	- Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. Note 1: Review can be applied to a risk management framework, risk management process, risk or control.
Risk Reporting	- Form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management.
Risk Register	- Record of information about identified risks. Note 1: The term risk log” is sometimes used instead of «risk register».
Risk Profile	- Description of any set of risks. Note 1: The set of risks can contain those that relate to the whole organisation, part of the organisation, or as otherwise defined.
Risk Management Audit	Systematic, independent and documented process for obtaining evidence and evaluating it objectively to determine the extent to which the risk management framework, or any selected part of it, is adequate and effective.

