Lebalelo Water User Association

RISK MANAGEMENT POLICY AND FRAMEWORK

A RISK MANAGEMENT PROCESS SUPPORTING MANAGEMENT

VERSION: 2.0

IMPLEMENTATION DATE: JULY 2019
LAST REVISION DATE: MARCH 2020
REFERENCE NUMBER: LWUA-GRC-GOV-RISK

	NAME	POSITION	SIGN OFF	DATE
AUTHOR:	A Collier	GRC-Legal		
PRINCIPAL REVIEWER:	A Collier	GRC		
REVIEWER:	C Taljaard	Projects		
REVIEWER:	S Manyaka	Social		
REVIEWER:	A Britz	Finance		
REVIEWER	T Makhubele	Operations		
REVIEWER	P de Wet	Administration		
RECOMMENDED BY:	J Bierman	CEO		
RECOMMENDED BY:	M Brasler	Chair FINCOM		
RECOMMENDED BY:	M Mashilane	Chair SECOM		
APPROVED BY:	D Pelser	Chair MANCOM		

CONTENTS		PAGE

1	AIM	
2	SCOPE	
3	DEFINITIONS	
4	ABREVIATIONS	
5	RESPONSIBLE FOR REVIEW	
6	RESPONSIBLE FOR IMPLEMENTATION	
7	GENERAL	
8	POLICY / PROCEDURE	
8.1	Introduction	
8.2	Policy and Framework	
8.3	Governance, Roles and Responsibilities	
8.4	Embedding Risk Management in the Association	
8.5	Other	
9	HISTORY OF CHANGES	
10	RECORD CONTROL	
11	REFERENCES	
12	RELATED PROCEDURES	
13	ANNEXURES	

1. AIM

The aim of this policy / procedure is to provide guidance in respect of risks as they apply to the Association.

2. SCOPE

This policy / procedure applies to the Association.

3. DEFINITIONS

TERM	DEFINITION
Assurance	Any activity, internal or external, which evaluates performance of internal control activities and identifies deficiencies in control effectiveness.
Combined assurance	Integrating and aligning assurance processes in a company to maximise risk and governance oversight and control efficiencies, and optimise overall assurance to the Board Risk Committee, considering the company's risk appetite.
Compliance	Adhering to the obligations of laws, industry and organisational standards and codes, principles of good governance and accepted ethical standards.
Compliance Management	A series of activities that when combined are intended to achieve compliance.
Compliance Requirement	A law, regulation, government directive, standard, contract or internal policy/procedure that has been adopted by the company.
Control	The measure that is modifying risk. • Controls include any process, policy, device, practice, or other actions which modify risk. • Controls may not always exert the intended or assumed modifying effect.
Control effectiveness assessment	An assessment of the effectiveness of the control activities implemented in achieving the desired risk treatment. The assessment can be completed by management or the assurance providers.
Desired residual risk (Target risk)	The level of risk that can be tolerated for each identified risk. Where residual risk is assessed at a higher level than the desired residual risk there should be actions to mitigate the risk to the desired level.
Event	An incident or occurrence, from sources internal or external that could affect the implementation of the strategy or the achievement of objectives.
Event identification	An ERM component which is designed to develop a consistent and sustainable approach to identify events that could impact, positively or negatively, on LWUA's ability to achieve its corporate strategy and objectives
Impact	Result or effect on an event
Inherent risk	The risk the organisation is exposed to in absolute terms, i.e. in the absence of any management actions (including control activities) management might take (or have taken) to alter either the risk's likelihood of occurrence or impact.
Internal environment	Encompasses the tone of the organisation, influencing the risk consciousness of its people, and is the foundation for all other components of enterprise risk management, providing discipline and structure. Includes the risk management philosophy; the risk appetite and culture; oversight by the Management Committee; the integrity, ethical values and competence of employees; management's philosophy and operating style; and the way management assigns authority and responsibility and organises and develops its people.
Likelihood	The chance of something happening. 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 mathematical terms (such as a probability or a frequency over a given time period).
Monitoring	The continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.
Obligation	Specific actions that the organisation must undertake in order to comply with the corresponding compliance requirement.
Opportunity	Positive effect of uncertainty on the Association
Reporting	Formal processes of informing key stakeholders of the results of the ERM initiative and its effectiveness
Residual risk	The risk remaining after risk treatment. Residual risk can contain unidentified risk.
Residual risk gap	The difference between the current level of residual risk and the desired level of residual risk
Risk	Risk is the effect of uncertainty on objectives. • An effect is a deviation from the expected – positive and/or negative. • Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). • Risk is often characterized by reference to potential events and consequences, or a combination of these. • 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. • Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.
Risk appetite	The broad-based level of risk that the Association is willing to accept in pursuing its corporate goals and its strategic imperatives.
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk profile	A description of any set of risks. The set of risks can contain those that relate to the whole organisation, part of the organisation, or as otherwise defined.
Risk treatment	An ERM component which relates to the policies, procedures, processes and controls implemented by management to avoid, reduce, share or accept risks associated with specified future event taking into account the risk tolerances of the organisation and the cost versus benefit including the effect on event likelihood and impact.
Risk tolerance	The acceptable level of variation relative to the achievement of objectives, usually expressed as desired residual risk.
Stakeholders	Parties that are affected by the Association, such as the MANCOM, FINCOM, SECOM, OPSCOM, employees, customers, authorities, regulatory bodies, community and suppliers.

4. ABBREVIATIONS

All abbreviations used in the document which are generally used in daily communications and need no explanation, are unnecessary. Abbreviations of an unfamiliar nature are explained in this paragraph in alphabetical order. Within the contents of this policy / procedure, reference is often made to phrases and/or terms that are unique to this policy / procedure. The meaning of the phrases and/or terms shall be as follows:

ABBREVIATION	EXPLANATION
Association	Lebalelo Water User Association
CEO	The Chief Executive Officer of the Association
COSO	Committee of Sponsoring Organizations of the Treadway Commission

ERM	Enterprise risk management is a continuous, proactive and systematic process, effected by the Association's personnel, applied in strategic planning and across the organisation, designed to identify potential events that may affect the organisation, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of objectives.
ERM system	The data repository used to capture all risk data, generate risk reports for management and monitor the presence and effectiveness of the ERM framework and process over a period of time.
FINCOM	Finance Committee
GRC-Legal	Governance Risk and Compliance - Legal
ISO	International Organization for Standardization
King IV™	King IV Report on Corporate Governance for South Africa 2016
KRI	Key Risk Indicators
KPI	Key Performance Indicators
MANCOM	Management Committee
OPSCOM	Operations Committee
SECOM	Social and Ethics Committee

5. REPONSIBLE FOR REVIEW

GRC-Legal shall be responsible to review this procedure on an annual basis, or as and when changes are required.

6. RESPONSIBLE FOR IMPLEMENTATION

The persons responsible for the implementation of this policy / procedure are:

- The CEO is responsible for implementation.
- Any Association employee or contractor that is requested to assist with the policy / procedure.
- The various Managers of the Association to make all relevant people mentioned in this procedure aware of their roles and responsibilities.

7. GENERAL

7.1 Compliance

Adherence to policy and procedure:

- It is the responsibility of the MANCOM, FINCOM and SECOM, in conjunction with executive management, to make appropriate provision for establishing controls to ensure adherence to this policy.
- Deviation to this policy shall not be permitted. Any incident where this policy is breached must be reported to the FINCOM.
- Any disciplinary action taken in terms of non-compliance with this policy will be in accordance with the disciplinary procedures of the Association.

7.2 Distribution

HARD COPY #	DISTRIBUTED TO	MASTER REFERENCE	ELECTRONIC REFERENCE
1	Legal -GRC	Central Policies & Procedures Library	Lebalelo Management SharePoint
2	CEO		
3	Management Committee		

8. POLICY / PROCEDURE

The following should be followed by Association employees.

8.1 Introduction

Risk management is an enabling process that supports management and MANCOM in meeting its strategic & business objectives in pursuit of value creation and protection. Strategic choices and the implementation thereof require risk taking. The risk management process is therefore an integral part of strategy setting and management as the information produced through it, along with other sources of information informs management decisions.

A Risk Management Policy and Framework, which is constituted of the following elements, is required to ensure that the risk management process is executed in a systematic, integrated and coordinated manner:

- Governance framework: Roles & responsibilities across the three lines of defense.
- Risk strategy and risk policies: How much risk should be taken in pursuit of profit & the minimum standards to be followed?
- Risk and Compliance methodologies: Processes to identify, assess, manage & monitor risks.
- Tools: System, templates and guidance to formalise and standardise risk & compliance management processes.
- Reporting and communication: Periodic reporting to management and the Board on risks, the control environment and mitigating actions taken.

The Risk Management Policy and Framework has been developed applying the ISO31000:2018 Risk Management Principles which should provide assurance to Management and the MANCOM that:

- The risk management framework applied is “fit for purpose”;
- All material risks are identified and prioritized;
- The control environment is effective to mitigate risks;
- The effort of assurance providers across the three lines of defense is optimized; and
- Gaps in the assurance plan are highlighted.

Furthermore, it also contributes to:

- A defined risk management philosophy and policy;
- An overview of the risk and compliance management process and consistent application;
- The communication of the key risk management principles;
- A common risk language across the organisation;
- Clear governance structures, roles and responsibilities in relation to risk management;
- Standardised risk & compliance reporting aligned with the organisation’s value drivers;
- Strengthening of the organisation’s processes to improve its resilience; and
- Identification of opportunities to be leveraged whilst providing comfort that the required reward is achieved.

In an environment of change and uncertainty, risk management is a critical success factor for achieving the Association’s strategic and business objectives. Embedding risk and compliance management into existing organisational processes is essential to making informed decisions and proactively planning for possible future events stemming from internal as well as external sources.

The implementation of an effective Risk Management Policy and Framework is a strategic imperative that has the full support of the Association’s MANCOM, Executive Management, Line Management and staff.

Risk and compliance management is everyone’s responsibility. The Risk Management Policy and Framework provides a systematic and integrated approach to risk and compliance management. The principles outlined in this document are the foundation for the risk and compliance philosophy and initiative.

8.2 Policy and Framework

8.2.1 Introduction

In terms of Principle 11, 12, 13 and 15 of the King IV Report on Corporate Governance for South Africa 2016 (“King IV™”), issued by the Institute of Directors in Southern Africa, the Association’s MANCOM and Executive Management have adopted a Risk Management Policy and Framework that is based on best practices which

includes the COSO II Risk Management Framework (as revised 2017) and the ISO 31000:2018 Risk Management Principles..

The purpose of the Risk Management Policy and Framework is to establish and formalise the requirement for implementing and maintaining effective risk management within the Association.

This Risk Management Policy and Framework aims to promote a robust and comprehensive risk management programme that is embedded throughout the Association – to identify, understand (assess) and manage risks, provide greater certainty and confidence to the Association's stakeholders, employees, customers, suppliers, and the communities in which the Association operates in order for the Association to be successful in achieving its strategic objectives

This approach to managing risk will facilitate the integration, coordination, and alignment of the Association and compliance risk management and assurance processes that exist within the Association, to optimise and maximise the level of assurance, governance and control oversight over the risk and regulatory landscape.

Combined assurance provided by internal and external assurance providers as well as line management should contribute toward satisfying the MANCOM, FINCOM and SECOM that significant risk areas, compliance requirements and mitigating controls identified through assessment processes are managed in a structured and coordinated way. It supports their governance and leadership role, informed decision-making and meeting oversight and fiduciary responsibilities.

8.2.2 Key principles embedded in the Risk Management Policy and Framework

The Policy and Framework is designed to support the Association in meeting its objectives and provides guidance on the following key principles:

- Integrated approach: An integrated approach to risk management is adopted i.e. a holistic approach to identifying, assessing, managing and reporting on the risks of the organisation.
- Culture: The Association accepts that taking risk is inherent in doing business and therefore recognises that the risk management and internal control system is important in the process of value creation and protection and that risk management is everyone's responsibility.
- Legal Mandate: The association is committed to best practice risk management and standards as embodied in this document. Adherence to these standards will demonstrate compliance with corporate governance guidelines.
- Governance structures: Accountability for a "fit for purpose" Risk management Policy and Framework lies with the MANCOM who is supported by the FINCOM who reviews the Risk Management Policy and Framework and the information produced by it. Management have the responsibility to design and implement this Policy and Framework and periodically report to the Management Committee.
- Risk appetite & tolerance: A certain level of risk is inherent in the operations of the Association; it is therefore necessary for the MANCOM and Executive Management to determine an acceptable level of risk in the pursuit of value creation and protection.
- Assess risk and monitor controls: Risk will be identified, assessed and controlled by line management and monitored and reported on an ongoing basis.
- Risk reporting: Risk reports will be periodically generated and represent inputs from all three lines of defense. In particular risks associated with the Association value drivers will be reported to the FINCOM and SECOM and ultimately a combined view will be presented to the MANCOM.
- Roles and responsibilities: There are different role players across the three lines of defense all with a defined set of responsibilities to give effect to the Risk Management Policy and Framework.

8.2.3. Policy implementation

The risk and compliance management function (second line of defence) will facilitate the risk management process. This will ensure an inclusive team-based approach for effective application across the Association.

The risk and compliance management process is the accountability of the MANCOM. The MANCOM is responsible for publishing an assessment of the state of risk and compliance, combined assurance and internal controls on the recommendations of the FINCOM in the Integrated Annual Report.

The MANCOM approves the risk management plan and the strategic, operational and compliance risk profiles while the FINCOM and SECOM will be responsible for oversight and monitoring of the risks allocated to them based on the value drivers of the Association.
The FINCOM will provide the MANCOM with a written assessment on the maturity and effectiveness of business and compliance risk management processes. The Governance, Risk and Compliance – Legal Manager is responsible to the MANCOM for the design, implementation and monitoring of risk and compliance processes.

8.2.4 Minimum Standards

To achieve the purpose of this policy the Risk Management Policy and Framework provides a common understanding, language and methodology for identifying, assessing, treating, monitoring and reporting risks and compliance commitments which provides executive management and the MANCOM with the assurance that key risks are being identified and managed. To ensure adherence to the Risk Management Policy and Framework, the following minimum standards will apply:

- The risk and compliance process will be embedded into critical business activities, functions and processes through applying a combined assurance (three lines of defence) approach. Risk understanding and tolerance for risk will be a key consideration in decision making.
- At a minimum, a workshop should be conducted with the FINCOM, the Chairperson of the MANCOM and executive management to establish the risk appetite and tolerance levels and consider the strategic risk and it delegates responsibility for the day-to-day management of risks to executive management.
- The OPSCOM provides oversight over the Association's assurance providers to ensure that the MANCOM, FINCOM and SECOM receives sufficient assurance that risks are being managed within the set risk appetite and tolerance levels and that the Association operates within the confines of its legislative environment.
- Risk controls will be designed and implemented to ensure that Association's strategic and operational objectives are met. The effectiveness of these controls will be systematically and frequently reviewed, where necessary, and improved.
- Risk management performance will be monitored, reviewed and reported. An independent assessment on the effectiveness of Association's risk and compliance process may be conducted at least every three years by an independent risk assurance function.
- Each area/ function in the Association is responsible for implementing and managing appropriate control systems and processes within their functional areas / operations. Progress against plans, significant changes in the business and the compliance risk profile and actions taken to address risk and various actions for risk treatment will be reported quarterly to management, bi-annually to the FINCOM and SECOM, and at least annually to the MANCOM. The GRC – Legal Manager maintains the risk and compliance management systems, processes and procedures.
- A common reporting framework will be utilised to report on the material risks, its mitigation and the control environment by the different assurance providers. The content in risk reports must adhere to the risk management process and standards as set out in this document
- No amendment(s) may be made to any section of this policy that does not form part of the standard Association governance processes.

8.3 Governance, Roles and Responsibilities

8.3.1 The Association's Risk Management Governance Principles

This section sets out the guiding principles for risk management (Based on the King IV Code of Good Governance™ and other best practices such as the revised COSO II: 2017 and ISO 31000:2018) underlying the organisation's Risk Management Policy and Framework. The Association has defined the following principles, which relate to the responsibilities for the governance of risk management, and which should be adopted by those involved in the risk management process:

- The Associations Executive Management is accountable to the MANCOM for the identification and management of the risk, both transversal risks and risks relating to legal and regulatory compliance that impact on their activities. The CEO of the Association has ultimate responsibility to the MANCOM to ensure that risks are appropriately managed and that regulations are complied with.

- The MANCOM, through its FINCOM and SECOM, is responsible for ensuring that management executes their risk, legal and regulatory responsibilities.
- A continuous improvement/learning culture is promoted at all levels while risks and compliance requirements will be reported on across the Association on a consistent basis.
- Where appropriate, risk and regulatory compliance requirements are identified and quantified in financial terms using a consistent approach in order to quantify exposures and allocate capital charges as appropriate.

8.3.2 Roles and Responsibilities

In order to implement and maintain an effective system of risk management at the Association, the process will be managed using a combined assurance approach which defines three lines of defence, namely:

- Line 1: Management and staff - The definition of "management" includes all levels of management;
- Line 2: The Governance, Risk and Compliance Function (independent from the operations) perform key functions to provide a second line of assurance to the MANCOM;
- Line 3: Independent internal and external assurance providers made up by risk assurance, external audit, and occasionally external regulators and any other external assurance provider such as verification and / or certification agencies. These structures are largely independent of the operational activities of the Association and provide assurance to the FINCOM, SECOM and MANCOM.

Before assurance responsibility can be allocated the assurance providers within each line of defence must be defined. Each line of defence may have multiple assurance providers. However, the acceptance of an assurance provider and its line of defence classification must be approved by the CEO before it may be included and used as such.

The criteria for the classification of assurance providers are as follows:

- Line 1 Classification Criteria: Executive management, management committees, line management and staff within the Association, responsible for various parts of business and control processes. This primary classification of management and staff responsibility should be used to define the individuals and teams that will make up the 1st line of defence.
- Line 2 Classification Criteria - For assurances by internal assurance providers to be regarded as credible each assurance provider may be assessed for quality against, at least the following criteria:

Criteria	Description
Independent / Objective	Sufficiently independent from the process / operation.
Skill and experience	Appropriately skilled and experienced.
Qualification	Be appropriately qualified.
Assurance methodology	Results formally reported.
Assurance body / registration	May be accredited or registered at a recognised accreditation body.

- Line 3 Classification Criteria - In order for assurance by Independent Assurance Providers both internally and externally to be regarded as credible, the following criteria must be met:

Criteria	Description
Independent / Objective	Independent from the operation, no direct reporting line to process owners, or involvement and / or work done in the process to be reviewed.
Conflict of interest	Free of any conflict of interest in relation to the process and operation under review and its results.
Skill and experience	Sufficiently and appropriately skilled and experienced.
Qualification	Appropriate qualifications.
Assurance methodology	Apply sound and formal methodologies. Formal reporting supported by working papers / audit trails.

Assurance body / registration	Accredited or registered at a recognised professional body.

8.3.3 First Line Responsibilities

8.3.3.1 Association Staff

All staff members of the Association will be responsible for the following:

- Employees must be aware of and understand the risks associated with their actions and comply with the Association's policy, processes, supporting guidance and procedures.
- Employees ensure the identification of new risks to their areas of accountability and responsibility and manage and/or escalate those risks to management, as appropriate.
- Employees should report significant risk matters, including deficient policies and procedures, to their line or executive management.

8.3.3.2 Operations Committee and Risk Owners

The OPSCOM consists of Executive Management and are in most cases the Risk Owners of the identified risks. These individuals will be responsible for:

- Ensuring that risks affecting the strategy of the Association are identified, assessed, managed, monitored and reported effectively, through implementing policies, processes, supporting guidance and procedures.
- Designing and implementing processes that will enable the Association to manage risk effectively within their defined risk appetites.
- Ensuring that process controls are documented and regularly reviewed and updated.
- Report on the status of risks and the management of risk.
- Managing the implementation of the Risk Management Policy and Framework.
- Provide support and assistance to the Association where required, in embedding risk management.
- Ensure that the risk process, from risk identification, measurement, management and reporting to optimisation, is occurring efficiently and effectively at programme level and provides input, where necessary.
- Provide oversight for risk management activities across the Association, ensuring that the Association's policies and procedures are adhered to.
- Ensure risk reports are produced and provided to MANCOM, FINCOM and SECOM in line with the risk management process.
- Ensuring synergy and a common approach to risk management is applied throughout the Association.
- Raising the awareness and understanding of risk management within the Association.
- Obtaining the commitment from line management for the effective implementation of risk management.
- Ensuring the Association's business plans take account of/incorporate the information in the risk register.
- Reviewing the risk register to ensure it incorporates all key/significant business risks.
- Ensuring all key business risks are properly managed and reported to the risk management function.
- Escalating instances where the risk management efforts are stifled.
- Updating the risk information.
- Provide guidance and support to manage "problematic" risks and risks of a transversal nature.
- Providing assurance regarding controls,
- Implementation of action plans for the risk.
- Reporting on developments regarding the risk.

8.3.4 Second Line Responsibilities

8.3.4.1 Governance, Risk & Compliance Management Function

The governance, risk management and compliance function should maintain a level of independence from the operations and management to ensure that a consistent approach is applied and to be able to challenge and analyse the risk profiles developed and reported. This independence is obtained primarily through organisational status and objectivity. While administratively, the Governance, Risk and Compliance reports to the CEO, the risk and compliance function should not assume operating responsibilities and should report functionally to the MANCOM, FINCOM and SECOM. The responsibilities of the Governance, Risk and Compliance Function include the following:

- Research, design, recommend and facilitate the overall risk management process.

- Oversee, monitor and communicate the status of implementation of risk management.
- Update and maintain the risk register with the assistance of Executive - and Line management.
- Analyse and report on risks to the MANCOM, FINCOM and SECOM.
- Facilitate and co-ordinate the implementation, maintenance and monitoring of the overall risk management and combined assurance process.
- Operate under the guidance of, and work closely with the MANCOM, FINCOM, SECOM and OPSCOM with regards to risk management.
- Provides guidance to the MANCOM, FINCOM and SECOM on overall leadership, vision and direction for risk management.
- Develops their risk management policy and framework in accordance with the Association's risk appetite and tolerance levels.

8.3.5 Third Line Responsibilities

8.3.5.1 Risk Assurance Function

When required, the association may choose to appoint an independent Risk Assurance service provider to provide assurance on the risk management process. The responsibilities of this service provider may include, amongst others, the following:

- To provide independent assurance on internal controls, risk mitigation strategies or process assurance.
- To review the risk management effectiveness, including the overall understanding of the risk profile and risk management effectiveness assessment.

The scope and mandates of the activities of the assurance providers will be established in line with the Risk Management Policy and Framework.

8.3.5.2 MANCOM, FINCOM and SECOM

The responsibilities of the MANCOM, FINCOM and SECOM pertaining to risk management and monitoring have been outlined in the Charters of these Committees. This Policy and Framework should therefore be read in conjunction with these Charters as they elaborate on the roles and responsibilities reflected in the Charters. A summary of the responsibilities for each of these committees have been reflected below:

Management Committee

- Adopt and oversee the effective implementation of policies and processes necessary to ensure the integrity of the internal controls and risk management, so that decision-making capability and the accuracy of its reporting are maintained at a high level at all times.
- Ensure development, implementation and ongoing maintenance of an effective Risk Management Framework and Plan.
- Monitor the key risks relating to the value drivers indicated as the responsibility of the Management Committee.
- Ensure compliance with all relevant laws, regulations and codes of best business practice and should receive regular updates on changes in the Regulatory Environment.
- Assigning assurance responsibility to assurance providers across the three lines of defence in line with the requirements as set out in this document.
- Ensuring that the FINCOM and SECOM provide risk assurance oversight in respect of the risks relating to their area of governance.

8.3.5.3 Finance Committee

- Perform a regular review of the adequacy and effectiveness of the Association's risk management policy and framework to ensure alignment to the key objectives of the Association.
- Evaluate and agree the nature and extent of the risks that the Association is willing to take in pursuit of its strategic objectives. The committee will recommend the risk appetite and the limit of the potential loss that the Association has the capacity to tolerate.
- Ensure that the risk appetite and risk tolerance are adequately defined and regularly reviewed.
- Ensure that appropriate risk metrics are developed and applied to monitor compliance with the risk appetite and tolerance limits established for the Association.
- Ensure "that it results in:

- An assessment of risks and opportunities emanating from the triple context in which the Association operates and the capitals that the Association uses and affects;
- An assessment of the potential upside, or opportunity, presented by risks with potentially negative effects on achieving organisational objectives;
- An assessment of the Association's dependency on resources and relationships as represented by the various forms of capital;
- The design and implementation of appropriate risk responses;
- The establishment and implementation of business continuity arrangements that allow the Association to operate under conditions of volatility and to withstand and recover from acute shocks; and
- The integration and embedding of risk management in the business activities and culture of the Association". (King IV™ Part 5.4, Principle 11,)

• Ensure that risk assessments are performed on an, at least annual basis.
• Monitor the key risks and actions taken to mitigate these risks for each of the value drivers indicated as the responsibility of the Committee.
• Disclose in a report to the MANCOM, for inclusion in the Integrated Report, the following in relation to risk:

- An overview of the arrangements for governing and managing risk;
- Key areas of focus during the reporting period, including objectives, the key risks that the organisation faces, as well as undue, unexpected or unusual risks and risks taken outside of risk tolerance levels;
- Actions taken to monitor the effectiveness of risk management and how the outcomes were addressed; and
- Planned areas of future focus. (King IV™ Part 5.4, Principle 11)

8.3.5.4 Social and Ethics Committee

• Monitor the key risks relating to safe operating conditions and a healthy workforce, environmental management, social mandate, sound brand, reputation and ethics and social stakeholder engagement and management as outlined by the value drivers of the Association, coupled with ensuring appropriate assurance is obtained, as necessary.

8.4 Embedding Risk Management in the Association

Risk awareness is embedded throughout the Association, which requires that:

• Risk management is integrated into all core business processes by applying a combined assurance approach.
• An organisational structure exists that supports the risk management and combined assurance policy and framework, particularly ensuring that there is clear ownership and communication of risk.
• Clear business & functional goals/objectives exist to assist with risk identification and to assist with mapping to risk appetite and tolerance levels set for the Association.
• Clear processes are in place for risk escalation and compliance incident reporting.
• Risk management (incl. compliance with legislation and regulatory requirements) and combined assurance be included as part of the personal performance management system for relevant personnel.
• Appropriate training in risk management at all levels.
• A fraud prevention policy and plan should be incorporated as part of the risk management and combined assurance to ensure that risk related to fraudulent and corrupt practices are identified and effectively managed.

8.4.1 Risk Appetite / Tolerance

Risk appetite is the amount of risk, on a MANCOM level, the Association is willing to accept in pursuit of value. The Association pursues various objectives to add value and should broadly understand the amount/level of risk it is willing to undertake in doing so. The Association must consider its risk appetite at the same time it decides which goals or operational tactics to pursue. To determine risk appetite, Executive Management, together with MANCOM and FINCOM review and concurrence, should undertake the following three steps:

• Develop risk appetite - Developing risk appetite does not mean the Association shuns risk as part of its strategic initiatives. Just as organisations set different objectives, they will develop different risk appetites. There is no standard or universal risk appetite statement that applies to all organisations, nor is there a "right" risk appetite. Rather, Executive Management and the MANCOM and FINCOM must make choices in setting risk appetite,

understanding the trade-offs involved in having higher or lower risk appetites. The choices made are formalised in qualitative or quantitative measures for the different types of risk that the Association is exposed to.

- Communicate risk appetite - Several common approaches are used to communicate risk appetite. The first is to create an overall risk appetite statement that is broad enough yet descriptive enough for organisational units to manage their risks consistently within it. The second is to communicate risk appetite for each major class of organisational objectives. The third is to communicate risk appetite for different categories of risk.
- Monitor and update risk appetite - Once risk appetite is communicated, Executive Management, with the MANCOM and FINCOM support, needs to revisit and reinforce it. Risk appetite cannot be set once and then left alone, rather, it should be reviewed in relation to how the Association operates, especially if the entity's business model changes. Management should monitor activities for consistency with risk appetite through a combination of ongoing monitoring and separate evaluations. In addition, the Association, when monitoring risk appetite, should focus on creating a culture that is risk-aware and that has organisational goals consistent with the MANCOM.
- Risk tolerance - refers to the acceptable levels of variation from risk appetite that the Association is willing to tolerate. Risk tolerance is defined as:

- The acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as those used to measure the related objective;
- In setting risk tolerance, Executive Management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Operating within risk tolerances helps ensure that the entity remains within its risk appetite and, in turn, that the entity will achieve its objectives; and
- Risk tolerance, guides the Association as it implements risk appetite within its sphere of operation. Risk tolerances communicate a degree of flexibility, while risk appetite sets a limit beyond which additional risk should not be taken.

- A Key Risk Indicator (KRI) is a measure used to indicate how risky an activity is. Key risk indicators are metrics used by the Association to provide an early signal of increasing risk exposures in various areas of the business. It differs from a key performance indicator (KPI) in that the latter is meant as a measure of how well something is being done while the former is an indicator of the possibility of future adverse impact. KRIs give an early warning to identify potential event that may harm continuity of the activity/project. Key risk indicators are linked directly to the Association's risk appetite and tolerance levels and therefore, each key risk indicator would have a set appetite level and tolerance level.

The first stage in the risk management process is to establish a benchmark of what the Association's acceptable level of risk is (Risk Appetite or Risk Tolerance) for each of the principal risks that the Association is exposed to, these can be defined in qualitative or quantitative terms. The Association MANCOM, FINCOM and Executive Management, through their risk review processes are responsible for identifying and assessing the risks and comparing these to the risk appetite limits/tolerances for each risk.

Risk appetite and tolerance levels are determined through an assessment of the inherent risk values and an assessment of the control environment to establish the residual risk levels/exposure. The residual risk level is compared to the risk appetite and tolerance level set for that risk and if it is too high, additional actions and controls have to be developed and implemented to reduce the risk exposure so that it is below the risk appetite for that risk. Any breaches of risk appetite limit for a risk type should immediately be escalated to GRC – Legal and ultimately to the FINCOM and MANCOM.

8.4.2 Risk Management and Combined Assurance Process

The risk management and combined assurance process consists of five (5) phases:

•The scope, context and criteria.
•Risk Identification.
•Risk Analysis.
•Risk Evaluation.
•Risk Treatment (combined assurance).

8.4.2.1 Establishing the Context

The risk assessment scope, context and criteria shall be set prior to risk identification to define the parameters within which risks will be assessed and to set the scope of risk management. The context shall include consideration of the Association's external and internal environments and the interface with strategic objectives, goals and objectives, as well as business plans and project deliverables.

Internal Environment: The Association's control environment is the foundation of risk and compliance management, providing discipline and structure to the risk management process. The effectiveness of the control environment is influenced by both the internal environment and external environment. The objective of evaluating the internal environment is to understand the factors that contribute to risk and therefore informs controls which should be in place to effectively manage the risks of the Association. The internal and external environment provides context and is about placing the risk assessment into perspective to ensure that the assessment is focused on and extracts risks that are pertinent to strategic and business objectives. In general, the context for risk assessments would consider the following relative to the internal environment:

- Consideration of value drivers, strategic and business objectives in combination with the Business plan.
- Expectations and requirements of key stakeholders inclusive of regulators.
- Understanding of value creation processes.
- Mapping of risk strategy to the business strategy.
- Understanding of key business processes and core competencies required to execute the Business plan.
- Organisation structure and its role in supporting the above.
- Risk management philosophy, process and culture.
- Commitment to complying with laws, regulations, codes of best practices and international standards.
- Oversight by the MANCOM and FINCOM of Audit and Risk.
- Integrity and ethical values of internal stakeholders.
- Assignment of authority and responsibility.
- Capabilities, in terms of resources and knowledge.

External environment: Evaluating the external environment is important in order to understand the external factors that influence the achievement of the Association's strategic and business objectives. These are generally factors over which the Association has no direct control but still needs to consider evaluating the ongoing relevance of its business strategies and risks that threaten its achievability.

The following elements should be key considerations as part of this evaluation:

- Economic – Understanding movements and trends in the macro-economy and its impact on the Association.
- Natural Environment – Considering risks like natural disasters, drought, floods, fires, earthquakes and sustainable development and the Association's preparedness to deal with those in the event that they occur.
- Political – Considering policy formulation and developments at national and regional levels and potential impact on the Association.
- Social – Considerations include changing demographics, shifts in societal values, social trends e.g. consumerism.
- Technological – Evolving, new and disruptive technologies

8.4.2.2 Risk Identification

Risk identification is the first step in the risk assessment process. The definition of risk can be summarised as the risk of an uncertain future event that could influence the achievement of an entity's objectives. A risk has two components to it:

- Probability – the likelihood that the risk will materialize.
- Impact – the magnitude or effect on the Association should the risk materialize.

Risks can therefore be either a threat or opportunity to the Association to achieve its objectives and successfully execute its strategies.

Types of risks (also referred to as principal risks) categorise the risks that could occur into groupings that share similar attributes even though the risk events are described differently. Risk appetite statements will, at a minimum be developed at a risk category level. The major categories are:

- Strategic risk – The risk of incorrect discretionary decisions regarding strategies, operating model, markets to operate in, services and products, capabilities and enablers, capital allocation, gearing and key stakeholders and responses to external developments. Excluded from this risk category is the execution of these decisions which is typically included in operational risk.

- Reputational risk – Risks relating to the Associations' perceived trustworthiness, dealings with third parties, fairness and good market practices and ethical conduct.
- Business risk – Risks related to variations in expected volumes of new business, margins, product mix and inflexible cost structures, mostly due to external conditions such as macro-economy, competition, political developments and environmental conditions.
- Operational risk – The risk of loss resulting from failures human, process and system failures or from external events. This risk includes breaches of contractual conditions as well as regulatory and compliance breaches.

During this process, risks with a potential impact on objectives are examined. An understanding of the risk is developed and involves a consideration of the causes (factors in the internal and external environment that increase the probability that the risk may occur) and sources of the risk, and their positive and negative consequences.
The objective of risk event identification is to develop a consistent and sustainable approach to identify all potential events that could impact the Association's ability to achieve its strategies and objectives. Risks or events can only be analysed and responded to if they are identified.
The risk identification process is outlined in Annexure A of this policy and framework.

8.4.2.3 Risk Analysis

Risk analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and the risk treatment response. Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur.
The risk description should include the elements below illustrated by a simple example:
- Risk event: Fire in the building (describing the potential event).
- Root cause: Arson, Electrical faults, Sabotage. (Describing the factors that could give rise to the event, note there could be more than one factor.)
- Consequence: Loss of life, Loss of information and systems, Loss of facilities.

Compliance risks require an analysis of the applicable laws, regulations, and codes of best practice or international standards in order to understand the compliance obligations on the Association. The results of the compliance analysis should be recorded in a compliance risk management plan and should cover at least the following elements:
- Applicable commitment: Applicable laws, regulations, codes of best practice or international standards.
- Requirements, sections, subsections: obligations, requirements and provisions identified through the analysis.
- Impact on the business: Potential sanctions, penalties, disruptions in operations and impact on the Association's reputation in the event of non-compliance

8.4.2.4 Risk Evaluation

The purpose of risk evaluation is to assist with the prioritisation of risks and to determine a risk treatment response. Risk evaluation involves comparing the level of risk (probability and impact) found during the analysis process with risk criteria established when the context was considered.
Risks are evaluated at the inherent and residual levels where impact, likelihood of occurrence and risk mitigation effectiveness are evaluated.
Executive Management may assess how risks correlate, where sequences of events combine and interact to create significantly different probabilities or impacts. While the impact of a single risk might be slight, a sequence or combination of events within or across the Association might have more significant impact.

8.4.2.5 Risk Treatment

The objective of risk treatment is to determine an appropriate response to the risk considering the nature of the risk, cost involved to implement controls and/or mitigating actions, and current level of residual risk compared to the risk appetite and tolerance level of the associated risk. Risk treatment involves a cyclical process to evaluate whether the chosen actions have been implemented and are effective in mitigating the risk.
Various response strategies are available for responding to a given event and associated risks. After the inherent risk is calculated, Executive Management must develop a response to the risks identified. These responses have been categorised as:

- Avoid – Action is taken to terminate or avoid the activities giving rise to risk because they are not manageable, or effective controls may be too expensive to implement. Risk avoidance could involve discontinuing a product, declining expansion into a new geographical market, or selling a division.
- Share – Action is taken to reduce risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Common risk-sharing techniques include purchasing insurance products, risk financing (where financial instruments are used to completely or partially mitigate the impact of the risk by, for example, 'hedging' through the use of instruments such as derivatives and swaps) or outsourcing an activity.
- Accept – A conscious decision to assume this risk and then take no action against its impact on the basis of a cost/benefit analysis.
- Mitigate – Recognition and active management of the risk through management control to reduce the likelihood of the risk occurring or its potential impact. For example, by the use of management controls, policies and procedures.

In selecting the treatment, an evaluation of the costs and benefits of the response is performed and an approach selected that brings the expected likelihood and impact within the desired risk tolerances. These will vary over time according to specific business objectives and will be reassessed when changes to strategic and operational objectives are affected. Risk treatment will always consider the existing control activities and its effectiveness.
Control activities can typically be categorised into:

- Preventative controls - These affect the likelihood of a particular risk occurring. The primary advantage of a preventative control is that the effort required to prevent a risk from occurring can be significantly lower than dealing with the consequences. For example, regular maintenance in a manufacturing plant is much more efficient than allowing equipment to break down, which incurs both replacement costs, along with operational downtime. Regular pre-emptive maintenance, training and skills development, separation of duties, and credit-worthiness checks are examples of preventative controls.
- Detective Controls - Detective controls identify events that have already happened, but which have not necessarily affected the operational ability of the Association (and hence may have gone unnoticed). They are useful as they allow the Association to institute corrective or mitigating actions early enough so that further deviation from objectives might be prevented. They also help ensure that corrective controls are being implemented properly. Examples includes inspection of equipment or facilities, regular internal and external audits and the use of leading and lagging safety indicators are examples of detective controls.
- Corrective Controls - These affect the severity or consequences of a risk, either minimising harm or optimising benefits. The main advantage of corrective controls is that they enable the continued operation of the Association or activity, helping to maintain continuity in delivering services or products to the Association's stakeholders, and value to its shareholders. Examples of corrective controls include insurance, product stockpiles, emergency response plans and teams, force majeure contracts and back-up power generators.

8.4.2.6 Combined Assurance

Executive Management, FINCOM, SECOM and the MANCOM rely on the risk management process and its outputs to make informed decisions and to assist with their oversight and fiduciary responsibilities. As such it needs to obtain periodic assurance from the various assurance providers across the three lines of defence that the risk management system is "fit for purpose", that it has been correctly applied and that the results produced by it are accurate and complete.

The combined assurance approach therefore needs to be conducted in a co-ordinated manner across the three lines of defence to ensure that optimal assurance is provided given the resources available and that assurance is provided where most relevant and that gaps in assurance are also highlighted.
Combined Assurance provides the following additional benefits:

- A common view of the risk types across the Association.
- Minimised business/operational disruptions by eliminating duplication of efforts and / or assurance activities.
- Comprehensive and prioritised tracking of remedial action on identified improvement opportunities/weaknesses.
- Improved reporting to the MANCOM, FINCOM and SECOM, including reducing the repetition of reports being reviewed by the different committees.
- Identification of areas of potential assurance gaps and facilitates the implementation and management of improvement plans for the gaps identified.

- An improved, more efficient focus on critical business and regulatory risk areas by the assurance providers.
- Better co-ordination of assurance providers reduces the business and regulatory risk of assurance "fatigue". Identifies areas of duplication and creates opportunities for cost savings.
- The use of Combined Assurance supports the FINCO and the MANCO in making their control statements in the integrated report.

The Risk Management Policy and Framework should therefore be read in conjunction with the Combined Assurance Policy and Framework.

8.4.2.7 Risk Reporting and Escalation

It is important to keep the MANCOM, FINCOM, SECOM and Executive Management abreast of key risks and the actions resulting from risk management activities. This component of the Risk Management Policy and Framework outlines the process to report risk management information to Executive Management and the MANCOM on a consistent and timely basis.

Key risks, along with emerging risks and risk response information, shall be reported to the MANCOM at least bi-annually.

The objective of risk reporting is to keep the MANCOM and Executive Management abreast of:

- Material risks and the effectiveness of risk treatment actions associated with it.
- Effectiveness of the control environment.
- Effectiveness of the Risk Management Policy and Framework and process.
- Breaches of risk appetite.
- Adherence to policy requirements.
- Material risk events.
- Escalations of risk matters.
- Combined assurance results.

The GRC Function is responsible for co-ordinating the periodic risk reporting to Executive Management, the FINCOM and SECOM. The reporting will be based on the responsibilities outlined in the Charters of these Committees and linked to the approved year-plan.

8.4.2.8 Risk Monitoring and Review

Monitoring is an ongoing process performed by all functions across the three lines of defence to verify the effectiveness of the risk management policy and framework and combined assurance process and evaluation of its results and risk mitigating actions taken. Monitoring will assist to:

- Identify risk trends, risk appetite breaches, material events, policy breaches and other matters that require escalation to Executive Management and the MANCOM.
- Ensure the consistent application of the Risk Management Policy and Framework across the Association.
- Identify weaknesses/enhancements and develop corrective action plans.

The process to monitor the risk management policy and framework takes two (2) distinct forms:

- Ongoing risk management monitoring activities - Ongoing monitoring activities are built into the normal, recurring operating activities across the Association. Employees are responsible for identifying and escalating potential risk management policy and framework weaknesses or enhancements.
- Independent risk management evaluations - Independent risk management and combined assurance evaluations performed by individuals not involved with the risk management and combined assurance processes will provide an independent appraisal of the effectiveness of the risk management policy and framework and process.

Executive Management is required to make a quarterly attestation that all potential risks, including any new emerging risks, have been identified and are recorded and that the controls have been reviewed for effectiveness and action plans prepared, where appropriate. Key controls and the overall risk environment is subject to ongoing monitoring to assess the adequacy of risk management activities through the OPSCOM, FINCOM, SECOM and MANCOM.

8.4.2.9 Communication and Consultation

Effective communication and consultation are key components to successfully implementing a risk management program. Communication is necessary to increase the awareness of the risk management program. Various mechanisms such as awareness campaigns, training and education sessions, newsletters, etc. will be considered to ensure that the communication is effective and reaches every employee throughout the Association. An effective communication and consultation approach will increase the level of risk management awareness and understanding at all levels of the Association and establish an Association wide risk aware culture.

8.5 Other

8.5.1 Regulatory Compliance

Management of Regulatory Compliance is directly linked to the risk management practices outlined in this Risk Management Policy and Framework.

The Regulatory Compliance process are outlined in the Regulatory Compliance Policy and Framework document. As part of this process legal compliance risk will be considered and will consist of the following two (2) elements:

- Regulatory risk is the risk that the Association does not comply with applicable laws and regulations or supervisory requirements or the exclusion of provisions of relevant legislation from operational procedures.
- Reputational risk is the risk that the Association might be exposed to negative publicity due to the contravention of applicable statutory, regulatory and supervisory requirements by the entity as well as staff members during the conduct of business.

Once the Regulatory Universe has been identified, as part of the Regulatory Compliance process, the legislative items on this Regulatory Universe should be risk assessed and ranked based on the impact which non-compliance will have on the Association. The process of risk assessing and ranking these legislative items will be based on the risk assessment process outlined in Annexure A of this Policy and Framework.

8.5.2 Risk Management Tools

The risk database is owned by the Association and access to the tool and data will be granted, restricted and controlled by the application owner. Logical Access to the data will be restricted to the OPSCOM and MANCOM. The data housed in the risk database and used to record, monitor and evaluate risks, will be backed up as per the information security policy of the Association.

GRC – Legal is the custodian of the risk data.

8.5.3 Record Keeping

The risk database is subject to the guidelines outlined in the Document Retention Policy.

9. HISTORY OF CHANGES

Reasons for Change - Index

A	As a result of incidents
B	As a result of audit findings
C.	Changes in Operating Procedures
D.	Changes in Legislation/Structures
E.	Changes in Technology
F.	Changes in Machinery/Equipment
G.	Results of risk assessments
H.	Change in training requirements
I.	New procedure format
J.	Change due to spelling or grammatical error
K.	To integrate a special instruction into the document control system
L.	Other reasons

Date of change	Revised Item (Paragraph number) - include a reference if it is applicable	Reason	Name of reviewer
July 2019	I	New procedure	A Collier
March 2020	L	Annual Review	A Collier

10. RECORD OF CONTROL

Records to be maintained in accordance with this policy / procedure:

Identification	Reference number	Responsible for filing	Responsible for maintenance	Location of storage area	Retention period	Method of disposal
Dealing with Policy	LWUA-GRC-GOV-POL	Legal -GEC	CEO	Association Offices and Share Point	Duration of document life	Shredding
Policy audit reports and findings				Office / Operations		
Corrective actions of the related findings or correspondences to the Policy				Office / Operations		

11. REFERENCES

Applicable Legislation

12. RELATED PROCEDURES

Document number	Document Title
LWUA-BM-GOV-POL	Association Governance Documentation Management Procedure

13. ANNEXURES

Annexure	Name
Annexure A	Risk Assessment Process and Score sheets

ANNEXURE A

Risk Assessment Process and Score sheets

Introduction

This document summarises the approach used to perform the risk assessments for the Association executive management. It is a qualitative assessment that has been created to perform comparative risk assessments across the Association. The approach is designed to be able to distinguish and report on events that are significant at a MANCOM, FINCOM or SECOM level, linked to the value drivers for the Association.

Calculating Inherent Risk Exposure

The risk that a potential event occurs is estimated from two perspectives: likelihood and impact. Inherent risk is the risk to an entity in the absence of any actions management may take to alter the risk's impact or likelihood. To calculate the inherent risk rating, we have used a qualitative scale that is aligned with the agreed risk assessment process (i.e. a 100 basis points).

1. Impact

Impact can be defined as the consequence or outcome of an event / risk affecting objectives. A risk can have both tangible and intangible consequences / impacts on the objectives of the Association.

To facilitate the impact assessment, we have utilised an impact matrix as indicated below:

Exposure Description	Financial	Reputation Credibility	People	Health and Safety – Injury Damage	Impact on Assets	Environment	Quality	Legal
Level 1 Minor	Less than R3,500,000	Internal Review	Manager and staff turnover less than 1% pa. Vacancy rate less than1%. Complaints or dissatisfaction amongst workforce.	Minor medical treatment by trained first aider. Near miss.	Insignificant infrastructure damage. Infrastructure still in good working condition posing no risk	Environmental near miss. No ecological damage. No impact on the community. Impact is limited to the footprint of the activity.	Affects quality of the process / product / service or affects the productivity, which is detected internally. No lost production. Doesn't affect customer or surplus. Isolated to a specific incident / project, once off.	On the spot fine. Technical non-compliance. Prosecution unlikely.

Exposure Description	Financial	Reputation Credibility	People	Health and Safety – Injury Damage	Impact on Assets	Environment	Quality	Legal
Level 2 Significant	Between R3,5 million & R7,0 million	Scrutiny required by internal committees or internal audit to prevent escalation. Localised media coverage	Manager and staff turnover over 2% pa. Vacancy rate over 2%. Isolated employee grievances.	Minor injuries with minor medical treatment required by trained medical personnel without lost time. Reversible health condition.	Minor infrastructure damage, equipment still operational and require minor repairs, no time loss.	Minor environ-mental incidents. Contained within the site. Short-term ecological damage, the impact is limited to the immediate surroundings. Nuisance to the community.	Affects quality of process/ product / service to the customer, but customer accepts / can accept, process / product / service. No production loss. Customer complaints with no financial impact.	Transgression of policy requirements. Breaches of letter of the law. A report to the authorities may be required

Exposure Description	Financial	Reputation Credibility	People	Health and Safety – Injury Damage	Impact on Assets	Environment	Quality	Legal
Level 3 Serious	Between R7,0 million & R15,0 million	Scrutiny required by external committees. Local / regional media coverage	Manager and staff turnover over 3% pa. Vacancy rate over 3%. Disputes / marches / organised stay away. Strike at one facility.	Major medical treatment by medical personnel resulting in lost time, restricted work.	Significant infrastructure damage, infrastructure require major repairs.	Reportable environmental incidents. Impact extends beyond the site boundary. Short -term ecological disturbance and/or significant impacts on the community. The impact is reversible with significant financial input	Affects quality of process / product / service to the customer. Several customer complaints and withheld payment. Short-term production loss	Breach of legislation that may lead to an enquiry by the authorities. A report must be issued to the authorities. An investigation by the authorities is likely.

Exposure Descrip-tion	Finan-cial	Reputation Credibility	People	Health and Safety – Injury Damage	Impact on Assets	Environment	Quality	Legal
Level 4 Critical	Between R15,0 million & R35,0 million	Intense public, political and national media scrutiny e.g. front-page headlines, TV, etc. Negative impact on the credibility of the organisation.	Manager and staff turnover over 5% pa. Vacancy rate over 5%. Strikes at several facilities. Difficulty in attracting qualified staff. Long term deterioration of employee morale.	Major medical treatment by medical personnel resulting in permanent disability/capacity. Irreversible occupational disease cases	Widespread, serious infrastructure loss. Infrastructure need replacement.	Reportable environmental incidents. Long-term ecological damage and / or widespread permanent impacts on the community. Impact is almost irreversible. The cost to reverse the impact exceeds realistic financial levels.	Affects quality of process/ product/ service to the customer. Medium term production loss. Product delivered at own costs resulting in financial loss	Violation of the law that could lead to prosecution and/or major fines. An investigation by the authorities is definite. Temporary suspension of licenses / permits to operate.

Exposure Descrip-tion	Finan-cial	Reputation Credibility	People	Health and Safety – Injury Damage	Impact on Assets	Environment	Quality	Legal
Level 5 Catastrophic	Greater than R35,0 million	Intense public, political and media scrutiny and regulatory intervention e.g. front-page headlines, TV, etc. Long term impact on the credibility of the organisation.	Manager and staff turnover over 7% pa. Vacancy rate over 7%. National Strikes. Inability in attracting qualified staff. Deterioration of employee morale for the foreseeable future.	Fatality or permanent incapacity where recovery is not possible. Fatality as result of occupational disease.	Devastating infrastructure loss. Need major capital replacement and results in major production loss	Environmental disaster. Irreversible ecological damage and / or extensive permanent impacts on the community. The impact is irreversible, and it is not possible to mitigate, even with significant financial input.	Affects quality of process/ product/ service to the customer. Significant damages/ loss to client due to non-fulfilment of contract and damages to client. Long-term loss of production	Violation of the law which could lead to imprisonment of Directors / RGM's / responsible staff / decision makers. Loss of licenses / permits to operate

2 Likelihood

Likelihood can be defined as the probability of something happening. 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).

Likelihood is assessed using a scale of 1– 5. The assessment of inherent exposure is done on the basis that the control environment in place is not considered. The assessment criteria in the table below is to be used to assess the probability of a specific risk materialising:

Description Probability	Level – 1 Rare	Level – 2 Unlikely	Level – 3 Possible	Level – 4 Likely	Level – 5 Almost Certain
Historical Trend	The risk has occurred in the last 24 months	The risk has occurred in the last 12 months	The risk has occurred in the last six (6) months.	The risk has occurred in the last three (3) months.	Monthly
Future Potential	The risk is highly unlikely to occur in the next five (5) years of more.	The risk may occur in the next five (5) years	The risk may occur in the next 16 to 30 months.	The risk may occur in the next seven (7) to 15 months.	The risk is currently occurring or could occur in the next six (6) months.

3 Inherent Risk Exposure

The ratings selected for the inherent impact and inherent likelihood of the risk generate the inherent risk exposure. The risk register will automatically calculate the exposure level. This exposure description and its corresponding exposure factor are illustrated in the table below, which is based on the assessment of the risk's impact and likelihood.

The risk evaluation matrix or heat map below, facilitates the evaluation of the risk assessment results. It allows us to easily distinguish between high, medium and low risks.

SCALE		LIKELIHOOD				
		LEVEL 1 Rare	LEVEL 2 Unlikely	LEVEL 3 Occasional / Possible	LEVEL 4 Regular / Likely	LEVEL 5 Frequent / Almost Certain
LEVEL 5	Catastrophic	5	10	15	20	25
LEVEL 4	Critical	4	8	12	16	20
LEVEL 3	Serious	3	6	9	12	15
LEVEL 2	Marginal / Significant	2	4	6	8	10
LEVEL 1	Negligible / Minor	1	2	3	4	5

Legend

	Urgent action is required to mitigate or eliminate the risk associated with a particular activity, product or service. All high risks are to be placed on a management programme and objectives and targets set to minimise the risk.
	Efforts must be made to minimise the risk, and as far as practicable without major expenditure using various control mechanisms.
	Risks are managed within acceptable levels. Continuous monitoring of risk mitigation strategies and key risk indicators to ensure that risks are managed within acceptable levels.

4 Control Effectiveness

To assess the effectiveness of the risk responses, we identify the control activities used by management to ensure that the risk responses are carried out. The most cost-effective way of mitigating a risk is usually by implementing process controls and risk monitoring in business processes.

During the strategic risk assessment process and our engagement with risk owners, we assessed the effectiveness of the control environment of each risk at risk level. To facilitate the process the below scales for current control effectiveness are used.

LEVEL	DECRIPTION	FACTOR
VERY GOOD	Controls are effectively implemented to mitigate the risk.	1
GOOD	Risk is substantially controlled and mitigated.	2
SATISFACTORY	The control system is somewhat effective but there is room for improvement.	3
WEAK	Some of the risk is controlled but there are major deficiencies.	4
UNSATISFACTORY	Risk does not appear to be controlled and the control system is ineffective.	5

5 Residual Risk Rating

This is the level of risk remaining after the relevant controls have been applied by management to reduce the risk. Residual risk represents the actual level of exposure that LWUA faces. The residual risk is rated as High, Medium or Low depending on management's view of the risk left over / not covered / managed.