ZIMBABWE ENERGY REGULATORY AUTHORITY

ZERA RISK MANAGEMENT POLICY

Revision 2 2024

Version Control Table

Date	Rev. No.	Reason for Change	Change(s) effected	Originator
January 2024	1	Expiration of the previous policy		Risk Officer

Table of contents

1. Purpose

The purpose of the risk management policy is to provide guidance regarding the management of risk to support the achievement of corporate objectives, protect staff and business assets and ensure financial sustainability. The aim of this policy is to ensure that the organisation makes informed decisions with respect to the activities that it undertakes by appropriately considering both risks and opportunities.

2. Scope

This policy applies to all ZERA activities. It forms part of ZERA governance framework and applies to all employees, service providers, stakeholders, contractors, and students on attachment for all operations undertaken by ZERA. The policy is supported by the ZERA Risk Management Framework.

3. Risk Management and Internal Control objectives.

Risk management objectives in a policy document are set to guide organizations in identifying, evaluating, and effectively managing risks that could potentially impact their operations, assets, reputation, and overall success. These objectives promote a proactive approach towards minimizing negative consequences while enhancing opportunities for growth and achievement. In the case of ZERA, the objective of risk management is to identify risk at an early stage and take the necessary steps or measures to mitigate its harmful effects.

Internal controls are an essential component that are designed to safeguard the organization's assets, ensure the accuracy and reliability of financial information, and promote operational efficiency. Internal controls not only help the organization fulfill its objectives but also safeguard against fraud, errors, and other risks. In reference to ZERA the primary purpose of internal controls is to help safeguard an organization and further its objectives.

Internal Controls employed by ZERA are:

i) Efficient conduct of business:

Controls should be in place to ensure that processes flow smoothly and operations are free from disruptions. This mitigates against the risk of inefficiencies and threats to the creation of value in the organisation.

ii) Safeguarding assets:

Controls should be in place to ensure that assets are deployed for their proper purposes and are not vulnerable to misuse or theft. A comprehensive approach to his objective should consider all assets, including both tangible and intangible assets.

Preventing and detecting fraud and other unlawful acts:

Even small businesses with simple organisation structures may fall victim to these violations, but as organisations increase in size and complexity, the nature of fraudulent practices becomes more diverse, and controls must be capable of addressing these.

iii) Completeness and accuracy of financial records:

An organisation cannot produce accurate financial statements if its financial records are unreliable. Systems should be capable of recording transactions so that the nature of business transacted is properly reflected in the financial accounts.

iv) Timely preparation of financial statements:

Organisations should be able to fulfil their legal obligations to submit their account, accurately and on time. They also have a duty to their shareholders to produce meaningful statements. Internal controls may also be applied to management accounting processes, which are necessary for effective strategic planning, decision taking and monitoring of organisational performance.

3.1 ZERA Control Environment

A control environment, also called "Internal control environment", is the overall attitude, awareness and actions of directors and management regarding the internal control system and its importance to the entity. It is also the atmosphere in which people conduct their activities and carry out their control responsibilities.

The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance oversight responsibilities; the organizational struc-ture and assignment of authority and responsibility; the process for attracting, develop-ing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance.

The organization demonstrates a commitment to integrity and ethical values.

i. The board of directors demonstrates independence from management and exer-cises oversight of the development and performance of internal control.
ii. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
iii. The organization demonstrates a commitment to attract, develop, and retain com-petent individuals in alignment with objectives.
iv. The organization holds individuals accountable for their internal control responsibili-ties in the pursuit of objectives.

4. Risk Governance

The Risk Management Executive Committee Charter is a separate document created in order to define in depth the Committee's objectives, the range of its authority, the scope of its activities and its duties and responsibilities.

Other Key Accountabilities and Responsibilities in ZERA with regards to Risk Governance.

Board	• Ensures an effective risk management framework (including risk appetite and risk tolerance) is established and embedded into the clinical and corporate governance processes of the organisation. • Provide strategic oversight and monitoring of organisation's risk management. • Seek information from the Chief Executive as necessary to satisfy itself that risks are being identified and mitigation strategies are in place and effective.
Risk Committee	• Overseas regular review of risk management activities. • Review and approve Risk Management Framework and Policy. • Review and approve Risk Management Annual Plan. • Review of Risk Management Summary Report. • Review and approve Risk Management Review Reports.
Chief Executive Officer	• Executive owner of Risk Management Framework. • Champions risk management culture within ZERA organisation that includes a focus on continuous improvement and identifying opportunities as well as risks. • Ensures implementation of the Risk Management Plan and that the Risk Register is current. • Ensures appropriate allocation of resources to manage and monitor risk and to implement risk mitigation strategies identified through risk planning activities. • Allocates accountability for managing individual risks at an appropriately senior level to ensure implementation of risk mitigation strategies. • Communicates risk management requirements to management and staff. • Takes appropriate action on risks reported or escalated • Provides the Risk Management Committee and the Board with regular reports on risks and management actions being taken to mitigate these risks • Determines the level of management that will be delegated authority to accept risks • Provides quarterly reports to the ZERA board on the organisation's top 10 risks inclusive of all extreme risks. • Approves the annual Risk Management Attestation Statement.

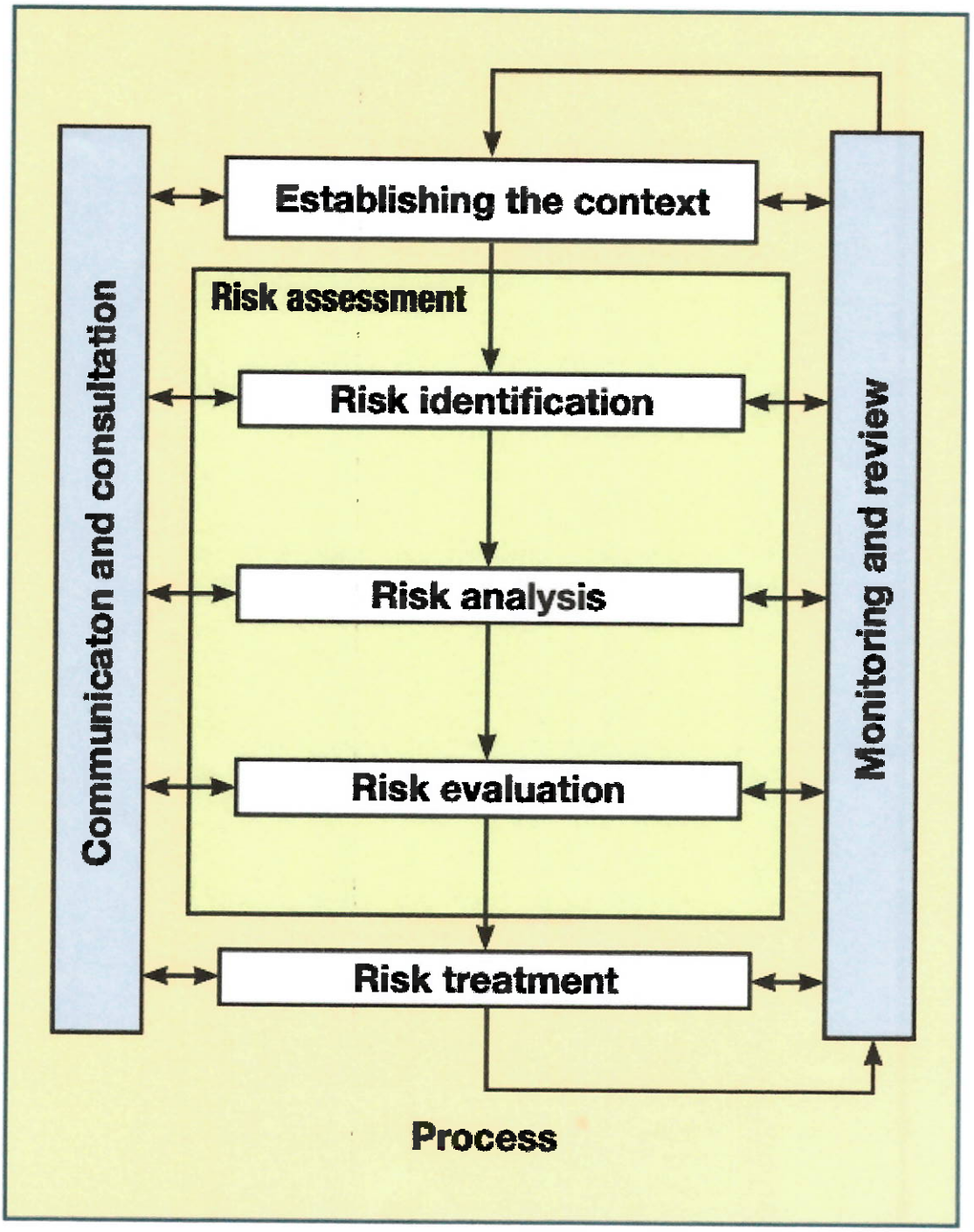
Directors	• Responsible for ensuring that staff understand their responsibilities with respect to operational risk management. • Develop a risk awareness culture within their area of responsibility. • Review of departmental risk register and risk Management objectives. • Risk Management and Compliance sign off. • Integrate Risk management processes into existing business processes. • Manage oversight of strategic, financial, operational and governance risk. • Notify Risk Officer of any changes in risk levels or new initiatives or projects that may exposure the ZERA to risk.
Risk Officer	• Continuously improving risk management policy, strategy and supporting framework. • Prepares and manage Risk Management Annual Plan. • Prepares Risk Management Report to Audit and Risk Management committee. • Reviews Detailed Risk Register and Risk • Management Objectives Profile. • Facilitate Risk Management training program for ZERA staff • Monitor Risk Management Treatment Plans. • Liaise with Internal Audit on outcomes of internal audits and control reviews. • Provide support for any new Risk Management related matters or projects. • Oversee the implementation of the risk management obligations under the Risk management framework.
Senior Managers	• Ensures that staff within their areas, understand their responsibilities with respect to operational risk. • Promote risk management within their areas of responsibility, including communication of requirements to relevant staff. • Accountable for risks and mitigating controls within their area of responsibility and take appropriate action on risks reported or escalated. • Reports on changes and updates to the organisation Risk Register, including updates on risk management strategies, current risk ratings and emerging risks.

Internal Auditor	• Reviews Risk Management Framework and Policy. • Incorporates Risk Management Plan control audit requirements into the Internal Audit plan. • Liaises with Risk Officer on outcomes of internal audits and control reviews. • Ensures audit plans for the organisation include appropriate consideration of risk. • Monitors and reviews risk management attestation compliance and report to the Chief Executive Officer on risk management and control frameworks within the organisation.
Risk Owners	• The departmental Heads are the Risk owners. • Manages the risk, including designing, implementing and monitoring actions to address (or "risk treatments" for) a particular risk. • Assesses the effectiveness of existing controls and design improvements as required. • Escalates the risk for effective management as appropriate to the level of the risk.
Risk Champions	Provides leadership and guidance for their specific teams working alongside the group's risk function.
Staff and Stakeholders	Comply with risk management policies and procedures
Combined Assurance Champion	• It is recommended that the Champion be selected from the 2nd line of defence (Risk Officer). • Obtain quarterly input from assurance providers. • Complete the Combined Assurance Model in terms of risks facing ZERA and identifying the assurance providers.
RMEC	• The purpose is to implement and embed the combined assurance framework principles as approved by the board. • Engage with the Board to determine the desired level of assurance required in each area. • Review all assurance activities on a quarterly basis. • Highlight and review the current areas of concern (emerging and/or existing risks) for management. • Ensures coordination, reporting and communication to stakeholders. • Develop a common view of the risk themes. • Agree on the future assurance activity to ensure broad and efficient coverage. •

5. Risk Management Process

When undertaking a risk management process, ZERA will follow the steps below:

- Establish the context,
- Identify the risk,
- Analyse the risk,
- Evaluate the risk,
- Treat the risk and
- Monitor and review the risk.
- Communication of the risks



6. Risk Rating Methodology

Risk will be assessed and rated based on the risk rating methodology and this considers two elements of risk:

1. Likelihood rating for risk occurring – this is an assessment of the potential frequency of occurrence without reference to known management controls and mitigating processes; and

2. Consequence rating for risk occurring – this is an assessment of the potential people, financial, reputation, compliance or business process/system impact

The level of inherent risk is assessed based on the level of likelihood and consequence.

The mitigating processes and controls associated with the inherent risks are then assessed to determine the control effectiveness rating.
The combined inherent risk rating and control effectiveness are assessed to provide the residual risk rating and treatment plan.

7. Residual Risk Assessment and Treatment Plan

The residual risk is the level of risk that remains within the organisation after consideration of all existing mitigating practices/controls. The residual risk provides guidance on the required level of management attention and when treatment plans are required to be developed to ensure management of the risk.

7.1 Risk Treatment and Response Strategies

Managing risks can involve applying different risk responses to deal with varying types of risk. Not every risk will warrant the same response. The following are strategies which ZERA may adopt in treating risk:

i. Avoiding Risks

Avoidance is an option that works to remove the chance of a risk becoming a reality or posing a threat altogether. If a product or service poses more risks than benefits, then it may behove an organization not to invest in that product or service. If there are geopolitical risks that can threaten an organization's projects, it may be a better choice to avoid those risks and select a different region to launch a project. An avoidance strategy shouldn't necessarily be used with frequency or for longer-term threats. Eventually, this response should be re-evaluated to find other sustainable risk responses that address underlying issues.

ii. Accepting Risks

Sometimes avoidance isn't an appropriate response, and acceptance may be the better practice. When a risk is unlikely to occur or if the impact is minimal, then accepting the risk might be the best response. Timing also plays a role — it could be that a risk doesn't pose any imminent concern, or it won't impact your company's strategic outlook. One example of this might be a change to vendor pricing down the road. This does pose a

financial risk but is nearly unavoidable — vendor prices inevitably increase. It's important to keep re-evaluating these types of risks periodically: their impact on your company and its projects could change.

iii. Mitigating Risks

Mitigating risks is the most commonly discussed risk response — however, it isn't always practical or possible. It may be the best option if a risk poses a real threat or problem, and avoidance or acceptance won't suffice. If a risk creates a negative impact and one that could be costly to your company, employees, vendors, or customers, then that risk should be mitigated. This means identifying the risk, assessing all possible solutions, devising a plan, taking action, and monitoring the results.

iv. Risk Transferring

There are when challenges or issues arise and you or your team may not be able to avoid, accept, or mitigate them. One example may be a lack of expertise or training required to address the risks. In this case, it may be a good idea to outsource or transfer the risk to another party — sometimes in-house, sometimes from an external third or fourth party. Some risk can also be transferred to an insurance company, which may reimburse organizations for certain realized risks.

8. Review And Monitoring of Risks

Through monitoring and review, you can iterate and improve the risk management process through continual improvement and iteration on a periodic and ongoing basis through the activities of planning, gathering, analysing, recording results, and providing feedback on those results.

Key Steps for Monitoring Risk

a. Monitor risk response plans.
b. Identify trigger conditions.
c. Analyze periodically to detect new risks.
d. Evaluate the effectiveness of the risk management plan.

9. Integration with other systems and processes

Risk management is factored into business planning, performance management, audit and assurance, business continuity management and project management.

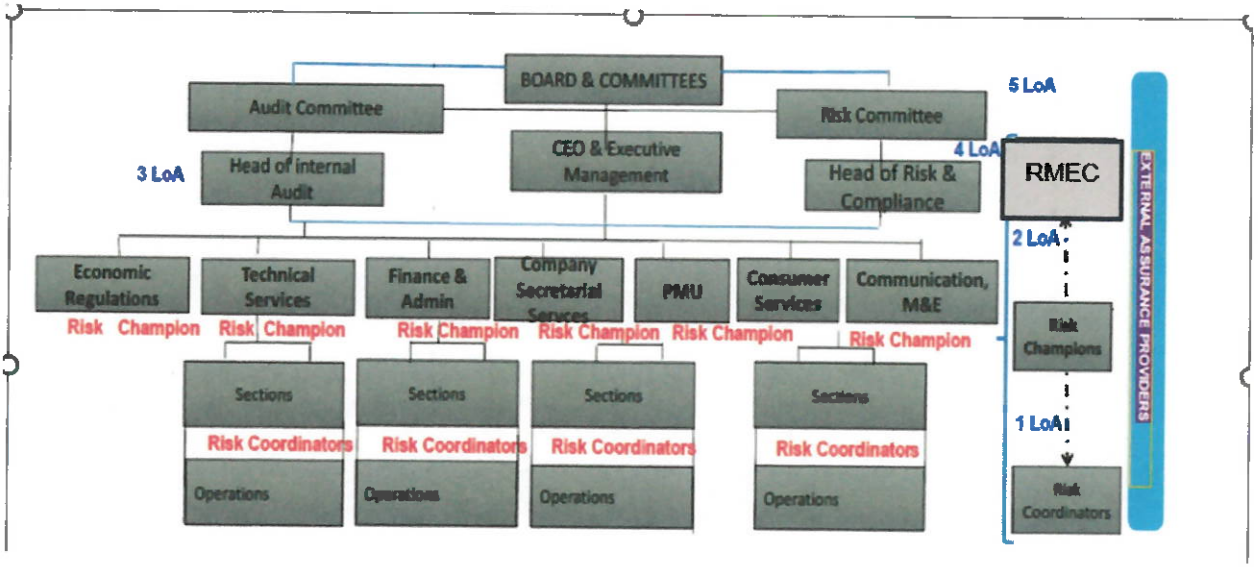
10. Combined Assurance

Combined assurance aims to align assurance processes between Enterprise Risk Management, internal audit and other assurance providers (both internal and external) to deliver deeper insights on governance, risk, and control management to senior management and the board.

A well-executed combined assurance approach helps to standardize messaging, reduce duplicative efforts, provide a common view of risks, and deliver more effective oversight with the ultimate goal of strengthening assurance and collectively adding more value to

the organization. The qualitative and quantitative benefits of increased alignment across assurance providers are clear, but knowing how to get started can be the hardest part.

ZERA Combined Assurance Governance Structure



Key

- 5th line of Assurance -External Audit
- 4th line of Assurance – Board and Committees
- 3rd line of Assurance – Internal audit functions
- 2nd line of Assurance -Risk, Compliance, Legal, Security and specialist functions
- 1st line of Assurance -Operational functions

11. Risk Categories

Risk categories in ZERA will include strategic, financial, environmental, safety, people and reputation.

- Public and Professional Liability responsibilities
- Occupational Health and Safety responsibilities
- Financial Management
- Organisational Management and Operational practices

12. Risk Register

ZERA shall maintain a Risk Register which provides an accurate and complete record of risk assessment and management activities. The Risk Register is to be a "living document", subject to regular review and update as risks are addressed and new risks identified, and strategies for current risks updated.

The Risk Register will include the following core information for each risk:

- An initial risk review date within an appropriate timeframe for example three (3) months of the date a new risk was identified.

- Subsequent risk review dates at minimum three (3) month intervals.
- Current control(s) which clearly define actions / controls that are currently in place.
- Additional control(s) which clearly define actions intended to be taken and a specific officer assigned to implement each additional control.
- A risk assessment to determine the level of risk rating (initial, current and projected) in accordance with Risk Matrix.
- Risk review date updated with each risk review.
- Any additional comments, actions or notes relevant to mitigate the risk.

Risk Owners shall review and moderate risks within their area of responsibility and accountability at minimum three (3) monthly intervals to ensure that the assessment and actions taken are reasonable, acceptable and within the tolerance and level of delegated accountabilities and responsibilities of the risk owner.

13. Risk Reporting

The purpose of risk reporting is to create awareness of key risks, improve accountability for the management of risk and the timely completion of risk treatment plans. The strategic risk register is prepared by the Risk Officer and reviewed by the Risk Management Committee on a quarterly basis.

14. Risk Management Performance

Risk management performance indicators will include the number of risk assessments completed per annum, the number of audit findings accepted in the ERM section, the timeliness of implementation of top risk controls, the reduction in the number of extreme risks in the risk register.

15. Risk Appetite

ZERA follows a prudent risk-taking approach in managing the organization. It defines prudent risks as those seen to contribute to the organization's capacity to better deliver its mandate within a range of consequences that are well understood and appropriately mitigated.

ZERA will manage the organization in a way that will enable it to deliver on its mandate and strategic directions and ensures that it fulfils its mandate and operates as a high-performance organization through effective governance by its Board.

The risk appetite statement for ZERA is a separate document that shows in detail the amount of risk that ZERA is willing to accept.

16. Allocation of appropriate resources to risk management

Risk-based resource allocation: Focusing regulatory and enforcement efforts where they are needed the most. and effectiveness, and most government agencies only loosely focus their efforts in this way. Resource risk management is the process of identifying, assessing, and mitigating risks to the availability,

capacity, and capability of resources required for a project. It involves analysing potential risks that could impact the project's resources and developing strategies to minimize their impact or prevent them from occurring altogether.

Allocation of resources will be based and guided by the risk appetite.

An organization's risk appetite captures the organizational philosophy desired by the board for managing and taking risks. Ideally, this should help to frame and define the organization's expected risk culture and guide overall resource allocation.

17. Review and approval.

The risk management framework and policy will be reviewed one year or earlier in response to an event or as required by a change in circumstances.

18. Policy definitions

consequence	means the outcome of an event;
control	means the measure that is modifying risk;
likelihood	means the chance of something happening;
monitoring	means continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected;
level of risk	means the magnitude of a risk or combination of risks, expressed in terms of the combination of consequence and their likelihood;
residual risk	means the risk remaining after risk treatment;
review	means the activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve the established objectives;
risk	means the effect of uncertainty on objectives;
risk analysis	means the process to comprehend the nature of risk and to determine the level of risk;
risk appetite	means the amount of risk that the organisation is prepared to accept or be exposed to at any point in time;
risk assessment	means the overall process of risk identification, risk analysis and evaluation;
risk evaluation	means the process of comparing risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable;
risk identification	means finding, recognising and describing risks;
risk management framework	is the set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and

	continually improving risk management throughout the organisation;
risk management	means coordinated activities to direct and control an organisation with regard to risk;
risk management plan	means scheme within the risk framework specifying the approach, the management components and resources to be applied to the management of risk;
risk management process	means the systematic application of management policies, framework and practices to the activities of communicating, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk;
risk owner	means the person or entity with the accountability and authority to manage a risk;
risk profile	means the description of any set of risks;
risk rating	means the rating resulting from the application of the organisation's risk assessment matrix on the likelihood and consequence of a risk occurring; and
risk treatment	means the selection and implementation of appropriate options for dealing with risk

Approved by ..... **Chief Executive Officer** ...../...../..... **Date**

Authorised by ..... **Board Chairperson** 17./12./2024 **Date**