THE GBVF RESPONSE FUND1

NPC Reg. No. 2021/359277/08

Contact Details: info@gbvfresponsefund1.org

Enterprise Risk Management Policy and Framework

September 2021

SIGN OFF AND REVIEW

		Date
Reviewed by	Audit and Risk Committee	20 September 2021
Approved by	Board of Directors	01 October 2021

Document No	Revision	Date
GBVF/RPF/001	01	2021/09/21

1. Preamble

1.1 This Policy and Framework are paramount to the good governance of the Fund and its effective and efficient management. To achieve the intended outcomes the Fund has integrated the following four key elements, namely having the right quality individuals in the Board and management, implementing strong processes and controls and having a robust independent oversight and assurance over all processes and controls.

2. Introduction

2.1 The GBVF Response Fund1 (the Fund) was established as part of the national response to the scourge of gender-based violence in South Africa. The Fund exists to co-ordinate financial resources to support relevant programmes and campaigns to eradicate GBVF as articulated in the South African National Government National Strategic Plan (NSP), by serving as a vehicle through which individuals and organisations are able to pledge their support, by making donations to the Fund and / or specific initiatives which are supported by the Fund.

2.2 In today's business environment, change and uncertainty are constants. Organisations face external and internal factors that give rise to uncertainty on whether or not organisations will achieve their objectives. Change and uncertainty create both threats (risks) and opportunities, which may either erode or enhance value for an organisation.

2.3 The Fund is committed to the optimal, effective management of risk in order to achieve their strategic goals in a sustainable manner. Risk management is integrated into the culture of the Fund and includes the mandate, leadership and commitment from the Board. This Enterprise Risk Policy and Framework aim to promote a robust and comprehensive risk management programme which will ensure that the Fund understands the risks and opportunities to which it is exposed and deals with them in an informed, proactive manner in the interests of all stakeholders.

3. Purpose and scope

3.1 The purpose of this Policy is to articulate the Fund's risk management philosophy and implementation framework. The Fund recognises that risk management is a systematic and formalised process. The objectives of the enterprise risk management are to:

3.1.1. Increase the likelihood that strategic objectives will be realised, and value preserved and enhanced;

3.1.2. Embed a culture that allows for responsible risk-taking while ensuring legitimate precautions are taken to protect the public interest, maintain public trust and ensure due diligence;

3.1.3. Ensure that the Board establishes the risk appetite within which the Fund needs to operate and to govern the Fund accordingly;

3.1.4. Provide guidance to the Chief Executive Officer, executive management and staff when overseeing or implementing the processes, systems and techniques for managing risk which are appropriate to the context of the Fund; and

3.1.5. Provide a comprehensive approach to better integrate risk management into strategic decision making.

3.2 This policy applies to all of the Fund's management, staff and directors, volunteers, contractors. The policy should be considered in all dealings with donors and beneficiaries who should understand how the Fund will apply risk management in the respective interactions.

4. Definitions

4.1 Enterprise Risk Management (ERM) refers to a process, affected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the organisation, designed to identify potential events that may affect the organisation, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of Fund's objectives.

4.2 The Institute of Risk Management defines risk as "the uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of consequences of impact and likelihood".

4.3 The International Standardization Organisation, ISO 31000 defines risk as the "effect of uncertainty on objectives".

5. Policy/Framework Objectives

5.1 The Policy and Framework has been developed to:

5.1.1 Clarify organisational roles and responsibilities with regard to ERM.

5.1.2 Facilitate the overall integration of ERM into the Funds activities.

5.1.3 Communicate formally the overall intentions and direction of ERM.

5.1.4 Establish robust ERM principles which are consistently applied throughout the Fund.

5.1.5 Align risk management with the Fund objectives, strategy and culture.

5.1.6 Define common risk management terminology.

5.1.7 Define the Funds risk categories and set risk appetite per risk category.

5.1.8 Escalation actions to be taken iro residual risk levels.

5.1.9 Provide guidance related to the key components of an effective risk management initiative.

5.1.10 Provide a customisable yet consistent approach to exploit opportunities through strategy and management risk.

5.1.11 Ensure that the risk management, regulatory compliance and strategic planning and execution are integrated.

5.1.12 Improve risk awareness.

5.2 This framework has been developed applying the ISO31000:2018 Risk Management Principles.

6. Policy and framework implementation

6.1 The Executive Management are accountable to the Audit and Risk Committee to design, implement and monitor the risk management process and ensure risks are managed within the agreed risk appetite as set by the Board and report on risks that are outside of the appetite and to document and / or seek approval for where risks have been accepted.

6.2 The risk management process is the responsibility of the Board. The Board is responsible for ensuring that there is a risk management policy and framework and setting the Funds risk appetite as well as publishing an assessment of the state of risk and internal controls on the recommendations of the Audit and Risk Committee in the Integrated Annual Report.

6.3 The Audit and Risk Committee recommends for approval to the Board the risk management plan and the strategic, operational and compliance risk profiles as well as provides oversight and monitors the assurance process at a strategic and operational level, as well as the reporting thereon. The Audit and Risk Committee is responsible to regularly review the risk register and for the oversight of the risks outside the risk appetite,

management plans to bring risks within appetite and risk acceptance. The Audit and Risk Committee recommends to the Board for approval the assurance scope and coverage and consider the assurance provided.

6.4 The Audit and Risk Committee will provide the Board with a written assessment of the maturity and effectiveness of the risk management process based on an assessment by management and independently assured by Internal/External Audit.

7. ERM Principles

7.1 An effective and efficient risk management practice promotes value creation and protection throughout the organization. This can be facilitated by adopting a set of principles which are considered a necessity for a strong foundation. Those principles which are adopted by the Fund are explained below.

7.1.1 Integrated: risk management is integrated with significant Fund activities.

7.1.2 Structured and comprehensive: a structured and comprehensive approach to risk management contributes to consistent results.

7.1.3 Customized: the risk management framework and activities are customized and proportionate to the Fund's external and internal context.

7.1.4 Inclusive: appropriate and timely involvement of stakeholders enables their knowledge, views, and perceptions to be considered. This results in improved awareness and informed risk management.

7.1.5 Dynamic: risks can emerge, change or disappear as the Fund's external and internal context changes. The organization anticipates, detects, acknowledges and , and responds to those changes and events appropriately and timely.

7.1.6 Best available information: Information should be timely, clear and available to relevant stakeholders.

7.1.7 Human and cultural factors: human behaviour and culture are taken into consideration throughout the risk management cycle.

7.1.8 Continual improvement: risk management is continually improved through learning and experience.

8. Benefits of Enterprise Risk Management

8.1 ERM is designed to strengthen management practices, decision-making and priority setting to better respond to stakeholder needs. The Fund's ERM process is expected to

provide the following benefits:

8.1.1 Consideration of risk during strategy and objective setting;

8.1.2 Understanding the proactive management of critical risks impacting objectives throughout the organisation;

8.1.3 Provide clarity on the level of risk that the Fund is prepared to take and the management of various risks of the Fund within this appetite. Identification and implementation of cost effective, integrated responses to multiple risks;

8.1.4 Enabling the Board and management to have a portfolio view of risks across the entire Fund, thereby creating reasonable assurance to the Board;

8.1.5 Reduction in operational surprises;

8.1.6 Informed decision-making;

8.1.7 Reporting with greater confidence, increasing business confidence;

8.1.8 Support governance responsibilities and satisfy legal and regulatory requirements;

8.1.9 Enhanced corporate governance processes;

8.1.10 Clearly defined roles, responsibilities and accountability;

8.1.11 Increased internal and external transparency;

8.1.12 Alignment of internal audit focus with the risk profile of the organisation.

9. Roles and Responsibilities

9.1 Board of Directors

9.1.1 Responsible to ensure that the Fund has a risk management policy and framework.

9.1.2 Assumes ultimate responsibility for risk management oversight.

9.1.3 Provides guidance (where necessary) during the identification of the top risks for the Fund.

9.1.4 Approve the risk appetite per risk category of the Fund.

9.1.5 Takes decisions (where appropriate) to accept key risks for the Fund.

9.1.6 Approve the risk appetite statements as recommended by management and Audit and Risk Committee.

9.1.7 Other roles and responsibilities as specified in Fund's delegation of authority.

9.2 Audit and Risk Committee

9.2.1 Assists the Board of Directors in providing oversight on risk management process including in respect of risks outside of risk appetite, management plans to bring risks within appetite and risk acceptance.

9.2.2 Reviews the management of enterprise risks.

9.2.3 Regularly review the Fund's risk register.

9.2.4 Escalate to the Board any issues in respect of risk management.

9.2.5 Oversees the adequacy and effectiveness of the Fund's policies and processes to identify and assess key risks and the systems to monitor and manage these risks.

9.2.6 Advises management to rectify exceptions in the implementation of risk treatment plans for the Fund's top risks.

9.2.7 Other roles and responsibilities as specified in Committees Terms of Reference.

9.3 Executive Management

9.3.1 Cultivates the desired risk culture and ensures robust accountability across the Fund.

9.3.2 Manage risks within the agreed risk appetite as set by Board, to report on risks that are outside of appetite and to document and/or seek approval for where risks have been accepted.

9.3.3 Perform the required risk escalation actions as outlined in Annexure B.

9.3.4 Reviews and deliberates (where necessary) on ERM reports on a periodic basis prior to presenting them to the Audit and Risk Committee and Board.

9.3.5 Challenges the selected risk treatment plans (where necessary), especially for the Fund's top risks.

9.3.6 Monitors the implementation status of risk treatment plans for the Fund's top risks and addresses exceptions.

9.3.7 Identify, assess and treat risks under their areas of responsibility in a dynamic and continuous manner.

9.3.8 Update the risk registers in a dynamic and continuous manner.

9.3.9 Cultivates ERM capabilities throughout the Fund.

9.3.10 Establishes, maintains and communicates (as appropriate) Fund ERM policy / framework / appetite / templates.

10. The Fund's ERM Framework

10.1 The Fund's ERM framework provides guidance to implement a consistent, efficient and economical approach to identify, evaluate and respond to key risks that may impact the Fund's overall strategic objectives. This framework is based on the principles embodied in the International Standard: Risk Management - Guidelines (ISO 31000:2018) and the King Code on Corporate Governance Principles (King IV).

10.2 Risk Appetite / Tolerance

10.2.1 The first stage in the risk management process is to establish a benchmark of what the Fund's acceptable level of risk is (Risk Appetite or Risk Tolerance). The Board and management, through their risk review processes are responsible for determining and rating the risks and controls.

10.2.2 Risk appetite and tolerance levels are determined through an assessment of the inherent risk values, an assessment of the control environment to establish the residual risk levels and establishing desired control effectiveness levels to determine the risk appetite and tolerance levels.

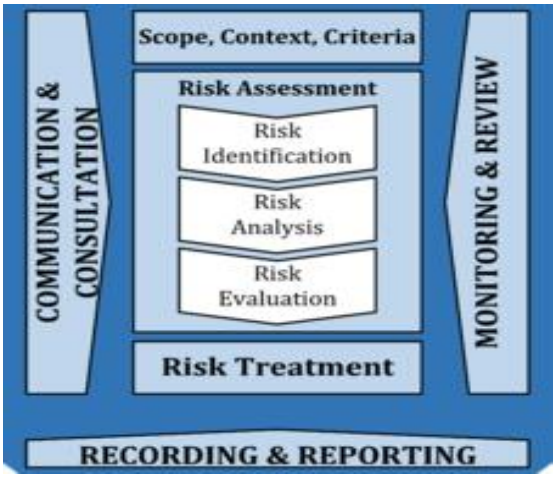
10.2.3 The residual risk should be assessed by the business and action agreed to mitigate the risk further if necessary or accepting the residual risk. The acceptance of risk should be within the organisations risk tolerance level.

10.2.4 Annexure A includes the detailed approach the Fund will apply to determine and set risk appetite and tolerance.

10.3 Risk Management Process

10.3.1 The risk process is a systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk and regulatory compliance requirements.

10.3.2 The risk management process consists of seven phases as detailed in the diagram below:



10.4 Risk Assessment

10.4.1 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. Operational, technical, financial, legal, s social, environmental, strategic, reputational, informational, stakeholder and other such criteria against which the threats or opportunities are to be evaluated shall be determined. The context shall include consideration of the Fund's external and internal environments and the interface with strategic objectives, goals and objectives, as well as business plans and project deliverables.

10.5 Establishing the context

10.5.1 Establishing the context is about placing the risk assessment into perspective to ensure that the assessment is focused and extracts risks that are pertinent to the business objectives. In general, the context for risk assessments would be one of the following four kinds of risk categories:

10.5.1.1 *Strategic:* risks that have the potential to impact, either positively or negatively on delivery of strategy;

10.5.1.2 *Reputation:* risks that have the potential to negatively impact the reputation of the Fund;

10.5.1.3 *Financial:* risks that have the potential to affect the financial viability of the Fund;

10.5.1.4 *Operational:* risks that have the potential to impact, either positively or negatively: delivery on the business plan; and

10.5.1.5 *Projects/Initiatives*: risks that have the potential to impact, either positively or negatively on the Fund's project and initiatives.

10.5.2 The context shall include consideration of the Fund's internal and external environments and the interface with strategic objectives, goals and objectives, as well as business plans and project deliverables.

10.5.3 Internal environment: The Fund's control environment is the foundation of risk and compliance management, providing discipline and structure. The objective of the internal environment component is to establish the "tone at the top" with regards to risk management and regulatory compliance. The control environment influences how strategy and objectives are established, business unit activities are structured, and risks and regulatory requirements are identified, assessed and acted upon. It influences

the design and functioning of control activities, information and communication systems, and monitoring activities and incorporates, but is not limited to, the following aspects:

10.5.3.1 The risk management philosophy and culture;

10.5.3.2 Commitment to complying with laws, regulations, codes of best practices and international standards;

10.5.3.3 Oversight by the Board and the Audit and Risk Committees;

10.5.3.4 Integrity and ethical values of internal stakeholders;

10.5.3.5 A commitment to competence;

10.5.3.6 Organisational structure;

10.5.3.7 Assignment of authority and responsibility; and

10.5.3.8 Capabilities, in terms of resources and knowledge.

10.5.4 External environment: Understanding the external environment is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing the terms of reference against which the significance of a risk is evaluated. The external environment can include, but is not limited to:

10.5.4.1 The social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment;

10.5.4.2 Key drivers and trends having impact on the objectives of the organisation; and

10.5.4.3 Relationships with perceptions and values of external stakeholders.

10.5.4.4 The external context entails the external environment in which the organisation seeks to achieve its objectives, and over which it has no direct influence. Describing the external context is important in order to understand the market forces (e.g. political, technological, legal, economic, etc.) and the social and environmental forces that will affect the Fund's operating and strategic capabilities.

10.5.5 The Chief Executive Officer (CEO) must establish the risk appetite document for the Fund which must be ultimately approved by the Board.

10.5.6 The Chief Financial Officer (CFO) must establish the risk assessment matrix which must be approved by CEO.

10.6 Risk Identification

10.6.1 Risk identification is the first step in the risk assessment process. A systematic and documented approach should be adopted for risk identification to determine what, how, where and when events could happen that could impact on the achievement of objectives.

10.6.2 Management shall identify risks with a potential impact on objectives systematically, iteratively, dynamically and collaboratively, drawing on the knowledge and views of stakeholders.

10.6.3 Risk identification must use the best available information, supplemented by further enquiry as necessary.

10.6.4 Risks must be clearly articulated to facilitate subsequent analysis and evaluation.

10.6.5 The following factors could be considered during risk identification for the Fund (not exhaustive):

10.6.5.1 Threats and opportunities.

10.6.5.2 Weaknesses and strengths.

10.6.6 Even risks which are not under the full control of the Fund must be highlighted during the risk identification cycle.

10.7 Risk Analysis

10.7.1 Risk analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur.

10.7.2 Management shall consider the following factors for each risk during risk analysis:

10.7.2.1 The residual likelihood of risk consequences.

10.7.2.2 The residual nature and magnitude of risk consequences.

10.7.2.3 Existing controls.

10.8 Risk Evaluation

10.8.1 The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

10.8.2 During risk evaluation, management makes decisions about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

10.8.3 Risks are evaluated at the inherent and residual levels where impact, likelihood of occurrence and risk mitigation effectiveness are evaluated.

10.8.4 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 business units might have more significant impact. Where risks are likely to occur within multiple business units, management may assess and organisation identified events into common categories.

10.8.5 Management shall evaluate risks with the guidance of the Risk Assessment process (Annexure B) and risk appetite (Annexure A).

10.9 Risk Treatment

10.9.1 The objective of risk treatment is to determine how the Fund will respond to events and associated risks. Risk treatment involves a cyclical process of assessing a risk treatment, deciding whether residual risk levels are tolerable, if not tolerable, generating a new risk treatment and assessing the effectiveness of that treatment. Refer to Annexure B where more detail on the risk treatment process has been defined.

10.9.2 The decision to implement a response will be based on risk tolerances, the effect the response will have on the impact and likelihood ratings and the results of the cost

versus benefit evaluation. Once a risk treatment is implemented, the Fund will develop ongoing mechanisms to monitor the implementation and effectiveness of the risk treatment.

10.9.3 Risk treatment relates to the risk response strategies, policies, procedures, processes and controls implemented to respond to specified future events. Risk treatment involves a cyclical process of:

10.9.3.1 Assessing a risk treatment;

10.9.3.2 Deciding whether residual risk levels are tolerable;

10.9.3.3 If not tolerable, generating a new risk treatment; and

10.9.3.4 Assessing the effectiveness of that treatment.

10.9.4 Various response strategies are available for responding to a given event and associated risks. After the inherent risk is calculated, management must develop a response to the risks identified. These responses have been categorised as:

10.9.4.1 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 not pursuing a certain initiative.

10.9.4.2 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 or outsourcing an activity.

10.9.4.3 Accept – A conscious decision to assume this risk and then take no action against its impact on the basis of a cost/benefit analysis.

10.9.4.4 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.

10.9.5 Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:

10.9.5.1 Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

10.9.5.2 Taking or increasing the risk in order to pursue an opportunity;

10.9.5.3 Removing the risk source;

10.9.5.4 Changing the likelihood;

10.9.5.5 Changing the consequences;

10.9.5.6 Sharing the risk with another party or parties (including contracts and risk financing); and

10.9.5.7 Retaining the risk by informed decision.

10.9.6 Taking risks is a part of the ordinary course of business. It is not the intent in all cases to minimise, avoid or eliminate all risks that are identified. However, it is the intent that the Fund understands the significant events that may impact business strategies and set guidelines to address the associated risks. This is achieved by establishing a standard and consistent process for developing an acceptable response.

10.9.7 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.

10.9.8 Risk treatments serve to focus attention on control activities needed to help ensure that the risk treatments are carried out properly and in a timely manner. Control activities are the policies and procedures that help ensure risk management strategies are properly executed. They occur throughout the organisation, at all levels and in all functions and usually involve two elements: a policy establishing what should be done and procedures to give effect to the policy.

10.9.9 In selecting control activities, management considers how the control activities are related to one another. In certain instances, a single control activity addresses multiple risk treatments, while in others, multiple control activities are needed for one risk treatment. The selection or review of control activities should include consideration of their relevance and appropriateness to the risk treatment and related objective. The ultimate goal is to bring the residual risk (after management actions and/or controls) to a level that is at or below the acceptable risk tolerance levels defined by management i.e. the desired residual risk/target risk. Controls can be divided into three groups according to how they influence risk – preventing, detecting or correcting.

10.9.10 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, training and skills development, separation of duties, and credit-worthiness

checks are examples of preventative controls.

10.9.11 Detective Controls - Detective controls identify events that have already happened, but which have not necessarily affected the operational ability of the Fund (and hence may have gone unnoticed). They are useful as they allow the Fund 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 regular internal and external audits and the use of leading and lagging indicators are examples of detective controls.

10.9.12 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 organisation or activity, helping to maintain continuity. Examples of corrective controls include insurance, emergency response plans and teams, force majeure contracts and back-up power generators.

10.10 Recording and Reporting

10.10.1 It is important to keep the Board, Audit and Risk Committees and management abreast of key risks and the actions resulting from risk management activities including identifying and reporting on risk events. This component of the risk management framework outlines the process to report risk management information to management and the Board on a consistent and timely basis.

10.10.2 Risk management activities should be traceable. Accurate and up-to-date risk information and performance shall be reported and communicated vertically and laterally across the Fund as appropriate. Key risks, along with emerging risks and risk response information, shall be reported to the Board at least quarterly.

10.10.2.1 The objective of risk reporting is to keep the Board and management abreast of:

10.10.2.2 Key events and associated risks especially where risks or control breakdowns happen, or where there are near misses. This reporting should be separate from the risk register and need to be reported on regularly to the Audit and Risk Committee, and significant matters to Board. This should also include a root cause assessment etc.as to why the risk occurred or the control broke down;

10.10.2.3 Current plans to address the key risks; and

10.10.2.4 Effectiveness of the Risk Management Framework and process.

10.10.3 The CFO must record risks with the necessary information to understand, analyse and evaluate them. The information requirements are established within the risk register template/s.

10.10.4 Risk reporting shall take into consideration:

10.10.4.1 Differing stakeholders and their specific information needs and requirements.

10.10.4.2 Cost, channel, frequency and timeliness of reporting.

10.10.4.3 Relevance of information to the Funds objectives and decision-making.

10.11 Communication and Consultation

10.11.1 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. exist to ensure that the communication is effective and reaches every employee throughout the organisation. An effective communication and consultation approach will increase the level of risk management awareness and understanding at all levels of the organisation and establish an organisation wide risk aware culture.

10.11.2 Communication and consultation with appropriate external and internal stakeholders must take place within the risk management cycle. This might include (but not limited to):

10.11.2.1 Sessions and workshops with risk owners and the Board

10.11.2.2 Discussions with auditors.

10.11.2.3 Sessions and workshops with Board Sub Committees

10.12 Monitoring and Review

10.12.1 Monitoring is a process that assesses the effectiveness of the risk management framework and process over a period of time.

10.12.2 Monitoring and review shall take place within the risk management cycle as required. This includes (but not limited to):

10.12.2.1 Risk treatment plans.

10.12.2.2 Control weaknesses

10.12.2.3 Audit observations.

10.12.2.4 Incidents.

11 Compliance and adoption of policy and framework implementation

11.1 Compliance with this policy and framework is essential to ensure that the Fund's risks are monitored and managed on a continuous basis in order to maximise potential opportunities and minimize the adverse effects of risk as well as increasing the likelihood that the Funds strategic and operational objectives will be achieved.

11.2 This policy and framework will be socialised with all employees through a formal workshop and for new employees as part of the onboarding pack.

12 Policy and Framework Review

12.1 The Risk Management Policy and Framework will be reviewed annually to ensure it remains current and relevant.

Appendix A: Risk Appetite and Tolerance

1. Introduction

1.1 The Risk Appetite and Tolerance Framework sets out the levels of risk that an organisation is willing to assume in pursuit of its business objectives and forms part of the organisation's Enterprise Risk Management system, which is governed by the Board.

1.2 This Risk Appetite and Risk Tolerance Framework is aligned to the Risk Management Standards and takes into consideration the principles outlined in King IV and ISO 31000. The King IV report specifically requires organisations to establish what would constitute excess risk taking and accordingly the Board is required to set levels of risk appetite and tolerance.

1.3 The methodology outlined in this annexure sets out the Fund's approach to risk appetite and risk tolerance, as well as an approach to assist operations and functions to respond appropriately to specific risk or opportunity issues.

1.4 The framework addresses specific responsibilities and accountabilities for the risk appetite and risk tolerance processes.

1.5 The use of risk appetite and risk tolerances shall become an aspect of the Fund's pro-active culture and shall be integrated into day-to-day business activities.

1.6 This framework supports the Enterprise Risk Management Framework and describes the structured approach to determine the Fund's risk appetite and tolerance levels using a consistent industry recognised approach.

2 Objective

2.1 The objective of the Risk Appetite and Risk Tolerance Framework is to provide a clearly defined and documented mandatory approach for decision making against a framework of calculated risk appetite and tolerances, i.e. to ensure that the Fund is not exposed to more risk than it is willing and able to assume. It is expected that the company shall embed this in all business activities, systems and processes so that risks are identified and managed on a consistent and holistic basis before events occur that might affect the achievement of the strategic objectives.

3 Definitions and Abbreviations

3.1 **Risk Appetite -** The level of risk that an organisation is willing to take in pursuit of its goals and objectives. It is also defined as the variability in results that an entity and its senior executives are prepared to accept in support of a stated strategy.

3.2 **Risk Tolerance -** Maximum risk that an organisation is willing to take regarding each specific risk.

3.3 **Key Risk Indicators (KRIs) -** Measures that provide insight into potential events.

4 Benefits of Establishing a Risk Appetite and Tolerance Framework

4.1 The risk appetite and risk tolerance process serve as an early warning mechanism to alert the Fund when adverse risk trends reach unacceptable limits. It is imperative, therefore, that management tracks risk and indicator trends to understand the direction in which risks are heading. This shall reduce the likelihood of the risk materialising and/or the impact it shall have on the Fund.

4.2 The process enables the Board and Management to decide whether they are comfortable with the Fund's risk exposure versus its risk capacity.

4.3 The risk appetite statements and tolerances shall enable better communication, consensus and decision-making in response to risk and opportunity.

5 Components of Risk Appetite and Tolerance Framework

5.1 Risk Appetite and Tolerance process flow

5.2 The process followed in setting risk appetite and tolerances and ensuring integration with the management of risks is summarised below.

5.3 Risk appetite can be defined as the total impact an organisation is prepared to accept, retain or pursue in achieving its strategic objectives. Risk appetite defines the boundary between acceptable and unacceptable levels of risk. Risk appetite forms the cornerstone of an effective risk management framework and sets the 'tone form the top' and the basic

foundation for the organisation's risk culture. Setting risk appetite enables an organisation to increase its rewards by optimising risk taking and accepting calculated risks within an appropriate level of authority. Risk appetite sets clear strategic directions and sets tolerance limits around controls.

5.4 The Fund's Board will define the risk appetite in terms of the level of risk that is acceptable to the organisation. Risks with unacceptable exposure will be addressed in an appropriate manner by management. It is essential that the Board and EXCO are kept informed with accurate and up-to-date information regarding the risks that the Fund is exposed to at any given time.

5.5 Risk tolerance refers to the acceptable levels' deviation risk from risk appetite that the Fund 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, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Operating within risk tolerances helps ensure that the Fund remains within its risk appetite and, in turn, that the entity will achieve its objectives; and
- Risk tolerances guides management as they implement risk appetite within their sphere of operation. Risk tolerances communicate a degree of flexibility, while risk appetite sets a limit beyond which additional risk should not be taken.

5.6 Risk tolerances and limits will be defined and approved by the Audit and Risk Committee to ensure the ongoing monitoring and management of risks are within acceptable risk limits, in line with the overall risk appetite statement.

5.7 Risk threshold is the maximum period which the Fund can afford to be without a critical function or process. The Risk appetite, risk tolerance levels, and risk thresholds will be reviewed on a regular basis and aligned accordingly.

6 Risk Appetite Statements

6.1 For each of the Risk Categories a Risk Appetite Statement will be crafted which sets out the inherent constraints that shall be considered when deciding how much risk to assume, and which risks the Fund is committed to take in order to achieve its strategic objectives

6.2 Risk appetite is determined qualitatively or quantitatively.

6.3 The amount of risk that the Fund can accept shall vary over time as circumstances change. The Fund's appetite for risk therefore needs to be evaluated regularly.

6.4 The Board shall set limits to determine the levels of risk the Fund is able to tolerate in pursuit of its objectives/value drivers. The Board considers the risk appetite of the Fund along with its tolerance limits.

Appendix B: Risk Assessment Process

1. Introduction

This annexure summarises the approach used to perform the risk assessments. It is a qualitative assessment that has been created to perform comparative risk assessments across the Fund.

The approach is designed to be able to distinguish and report on events that are significant at a Board level (critical risks), from those significant at the different managerial levels (high risks) or lower.

2. 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 action's management may take to alter the risk's impact or likelihood.

2.1. Impact

Impact: the potential effect on the business should the risk materialise, rated on a scale of 1 to 5 from minor to extreme.

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

Impact category	General
Extreme – 5	A risk event that, if it occurs will have a severe impact on the achievement of desired results, to the extent that one or more of its critical outcome objectives will not be achieved.
Critical – 4	A risk event that, if it occurs will have a significant impact on the achievement of desired results, to the extent that one or more of its stated outcome objectives will fall below acceptable levels.
Serious – 3	A risk event that, if it occurs will have a moderate impact on the achievement of desired results, to the extent that one or more of its stated outcome objectives will fall below goals but above minimum acceptable levels.
Significant – 2	A risk event that, if it occurs will have a minor impact on the achievement of desired results, to the extent that one or more of its stated outcome objectives will fall below goals but well above minimum acceptable levels.
Minor – 1	A risk event that, if it occurs will have little to no impact on the achievement of outcome objectives

2.2. Likelihood

Likelihood: the inherent probability that a risk will occur without any risk mitigation or control measures in place. Environmental factors that influence the risk should be considered when assessing likelihood. 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:

Descriptor	Historical Trend	Future Outlook
Frequent – 5	Daily / Weekly / Monthly.	The risk is currently occurring or could occur in the next 3 months.
Regular – 4	The risk has occurred in the last 3 months.	The risk may occur in the next 6 to 12 months.
Occasional – 3	The risk has occurred in the last 6 months.	The risk may occur in the next 12 to 24 months.
Unlikely / Uncommon - 2	The risk has occurred in the last 12 months.	The risk may occur in the next 3 years.
Rare – 1	The risk has occurred in the last 24 months.	The risk is highly unlikely to occur in the next 3 years of more.

2.3. 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.

Inherent Risk Heat Map						
Impact	Extreme - 5	5	10	15	20	25
	Critical - 4	4	8	12	16	20
	Serious - 3	3	6	9	12	15
	Significant - 2	2	4	6	8	10
	Minor - 1	1	2	3	4	5
		Rare – 1	Unlikely – 2	Occasional – 3	Regular – 4	Frequent - 5
		Likelihood				

2.4. Inherent risk escalation

The colour coded table below, illustrates the escalation of inherent risk based on the assessed inherent risk exposure.

Exposure description	Suggested action	Approval authority
Extreme	This risk must be shared, terminated or controlled	Board
Critical	This risk will typically be shared or controlled	Audit and Risk Committee
Serious	This risk will normally be controlled (treated)	CEO
Significant	Management will make an informed decision as to whether this risk must be controlled or absorbed by the business unit.	CFO
Minor	This risk is within the accepted appetite. Cost of losses will be absorbed by the operating unit	CFO

2.5. Control Effectiveness

Effectiveness factor	Qualification criteria	Rating
Very Good	Controls evaluated are adequate, appropriate and effective to provide reasonable assurance that risks are being managed and objectives should be met.	90%
Satisfactory	A few control weaknesses were identified, however existing controls are considered to be generally adequate, appropriate and effective to provide reasonable assurance that risks are being managed and objectives are being met.	65%
Weak	Control weaknesses were identified, which if not appropriately addressed could in the future result in the entity not achieving its objectives.	40%
Unsatisfactory	Numerous control weaknesses were noted. Controls evaluated are unlikely to provide reasonable assurance that risks are being managed and objectives are met.	20%

2.6. Residual risk rating escalation

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 the Fund faces. The residual risk is rated as Extreme, Serious, Moderate, within appetite and Acceptable depending on management's view of the risk left over / not covered / managed.

Residual Risk Rating	Residual Risk	
Extreme	15.6 - 20	Immediate escalation and action: Management must immediately escalate to Audit Committee and Board. Immediate remediation plans must be instituted.
Serious	11.6 -15.5	Urgent Action: Management must immediately escalate to Audit Committee and remediation plans must be identified and implemented.
Moderate	7.6 -11.5	Action: Management must plan and implement action to reduce the exposure further.
Within appetite	3.6 - 7.5	Tolerate - within acceptable limits. Management to monitor exposure level.
Acceptable	0.1 - 3.5	Observe - within acceptable limits. Management to continue to observe exposure level.

Appendix C – Key definitions

Term	Definition
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.
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.
Enterprise risk management (ERM)	Enterprise-wide risk management is a continuous, proactive and systematic process, effected by an organisation'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.
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 an organisation'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 Board of Directors; 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.

Term	Definition
Opportunity	Positive effect of uncertainty on
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 an organisation 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 management	Coordinated activities to direct and control an organization with regard to risk
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 an organisation, such as the Board, employees, customers, authorities, regulatory bodies, community and suppliers.
Assurance	Any activity, internal or external, which evaluates performance of internal control activities and identifies deficiencies in control effectiveness.