Enterprise Risk Management Policy and Framework

ERM Policy and Framework

TABLE OF CONTENTS

ERM Policy and Framework

1 PURPOSE AND OBJECTIVES

This document sets out the policy and framework on the management of risk at all levels of Telkom SA SOC Limited (hereinafter referred to as "the Organisation"). As the field of risk management is dynamic, this policy document is expected to change over time.

This policy confirms the commitment of the Organisation's executive and senior management, in support of the board's accountability for Enterprise Risk Management (hereafter referred to as ERM) towards conducting healthy business practices which is beyond reproach, through the application of ERM principles to stimulate business growth and sustainability

2 APPLICABILITY AND SCOPE

The ERM policy and framework apply to all employees and is aimed at establishing the principles of and commitment to the management of enterprise-wide risks the Organisation and thus establishing and reinforcing a risk management culture within the Organisation. All employees must be conversant with this policy and sections of the framework.

The objective of the framework is to ensure that there is a standard approach to managing risks across the Organisation. The framework will instil consistency and serve as a key enabler in the deliverance of the strategic intent, thus ensuring that objectives are achieved, namely:

I. Instil a culture of risk management and risk ownership practiced as everyone's responsibility, including integrating risk management into the way business is run and applying a more rigorous basis for decision-making and planning.

II. Identifying negative and positive risk circumstances and assessing risks regarding likelihood and magnitude of impact.

III. Creating a response strategy and monitoring it, whilst creating value for stakeholders, employees, customers, regulators, and society at large.

IV. To assist management in achieving our objectives by proactively de-risking business plans and through business continuity management preparedness, ensure business readiness before, during and after a disruption or disaster.

3 CONTEXTUAL BACKGROUND

The Organisation has established an independent ERM function that identifies, assesses, advises on, monitors and reports on the enterprise-wide risks in the Organisation, including all business units and subsidiaries. ERM sets out to achieve the following key objectives:

I. Oversight: All critical risks and opportunities are identified, managed and monitored under a holistic approach as per the risk committee approved risk appetite statement.

II. Ownership and responsibility: The risk ownership is assigned to management individuals who are responsible for identifying, evaluating, mitigating, and reporting risk exposures.

III. Assurance: The board, risk committee, organisation executive and management have reasonable assurance that all risks and opportunities are being appropriately managed/explored within defined levels to bring value to the organisation.

The board has committed the Organisation to a process of ERM that is aligned to the principles of the King IV Report on Corporate Governance, the COSO Integrated ERM Framework as well

as ISO 31000 Risk management – Guidelines. Business units and subsidiaries, supporting functions, processes, and controlled entities will be subject to the ERM Policy and Framework.

4 RESPONSIBLE PERSONS AND DUTIES

Certain individuals and groups across the Organisation have specific responsibilities they are expected to undertake as set out in the ERM Policy. These are summarised below:

4.1 Board of Directors

The board of directors has the ultimate responsibility for overseeing the management of risk management. The broader duties and responsibilities are based on good corporate governance (King IV) practices. The board must ensure that governing documents are in place: ERM Policy and Framework, Enterprise Risk Strategy and Plan, ERM systems and processes.

4.2 Risk Committee

The risk committee has an independent role and makes recommendations to the board for consideration and approval, including overseeing management's actions in the management and reporting of material business risks and overseeing the ERM Policy and Framework.

4.3 Group Chief Executive Officer

The Group Chief Executive Officer (GCEO) is responsible for maintaining an effective and comprehensive, fully integrated ERM process to safeguard and protect the assets.

4.4 Integrated Governance, Risk and Compliance Forum (IGRCF)

The forum is an internal structure, which will conduct the final assessment of the risks and risk opportunities identified to be reported to the board and its sub-committees.

4.5 Executive Committee

The board delegates responsibility for the implementation of the ERM policy to the GCEO and through the GCEO to the Executive Committee (Exco) ream. Key responsibilities of Exco in relation to enterprise risk management include:

IV. Implementing and monitoring of the processes required for risk identification and assessment and ensuring risks owners are effectively managing and monitoring key risks.

V. Ensuring that systems and processes to manage risk are operating effectively in accordance with the organisation's Enterprise Risk Management policy and framework.

VI. Regular reporting to the GCEO on the effectiveness of managing material strategic and operational risks and periodic review of the risk profile, fostering a risk-aware culture.

4.6 Group/Managing Executives and Executives

Executive management is responsible for the effective ERM, and ensuring that all instances of non-compliance with the ERM policy & framework are managed and reported appropriately.

4.7 Senior Management and all other employees

Senior Management and other employees across the company are responsible for the effective identification, management, reporting and control of risk within their area of responsibility, and for developing and promoting a risk-aware culture.

4.8   General Management

Specific responsibilities for managing enterprise risk include:

I.   Promoting a culture of risk management and control in their area of responsibility and assigning risk and control owners as per the risk management processes.

II.   Ensuring staff are adequately trained in enterprise risk management requirements relating to their position and that training is up to date and that risk management is factored into job descriptions and performance management agreements.

III.   Ensuring risk management capabilities are factored into contracts with external customers and suppliers as well as reporting and resolving non-compliance instances.

4.9   Business Assurance Forum

The Business Assurance Forum is authorised by the Exco to carry out any activity within its terms of reference, including the following duties:

I.   Implements ERM strategies and a sustainable process of enterprise risk management.

II.   Monitors risk appetite and produces risk reports and provides oversight on risks.

III.   Integrates, coordinates and aligns risk management and assurance processes and coordinates assurance activities at a business unit level.

4.10   Enterprise Risk Management unit

I.   Develop, implement and maintain an enterprise risk governance framework, policies, and processes for all categories of risk (preventable, strategic and external risks).

II.   In conjunction with Exco, determine and propose the risk appetite and ensure that the ERM framework integrates with organisation strategy formulation and business planning.

III.   Monitor compliance with the ERM framework through the provision of reporting, that ensures effective and efficient risk management for the organisation.

IV.   Create, promote and maintain a culture of risk awareness and accountability in business through appropriate forums, communications and education.

V.   Draft, review and edit ERM management reports, discuss the reports with appropriate management, evaluate responses and schedule follow-up projects to be performed.

VI.   Identify, assess and prioritise risks for the organisation, including monitoring and analysing risks and risk trends, followed by the development of control mitigation within all business units and subsidiaries.

VII.   Plan execute and report to the risk committee on the progress on the ERM plan and report directly to the risk committee at board level on ERM activities. This report must include significant risk exposures and mitigating strategy issues, corporate governance issues and all ERM matters needed or requested by the board and management.

VIII. Provide, annually, an assessment on the adequacy and effectiveness of the organisation's processes for mitigating risks.

4.11   Internal Audit

Internal Audit is responsible for providing an independent and objective assurance to the board on the effectiveness of enterprise risk management across the company.

5   RISK APPRAOCH

5.1   Enterprise Risk Management Integrated Approach: Our integrated approach on risk and compliance governance is based on the approved ERM governance structure, that considers nine principles of the Integrated Governance, Risk and Compliance (IGRC) framework for building an intelligent risk organisation.

5.2   Enterprise Risk Management Governance Structure: The board of directors through the risk committee, is responsible for the total process of risk management. The Organisation's business operations, subsidiaries, business units, joint ventures and any other functional areas are responsible for implementing and reporting on the policies, frameworks, and requirements of the ERM function.

Each business unit and subsidiary performs ongoing risk exposure analysis in consultation with the ERM function who in turn produces a risk profile report, demonstrating the management of key risks and opportunities identified.

6   ENTERPRISE RISK MANAGEMENT PROCESS

The ERM process is driven by a series of activities and events designed to integrate ERM within business processes across the enterprise and ensure that there is standardisation and common elements across all these occurrences.

ERM is a multidirectional, iterative process in which almost any component can and does influence another. We ensure that ERM processes and risks are re-evaluated and updated on an ongoing basis to reflect new information and experiences so that all significant risks are appropriately identified, addressed and that any material opportunities are not overlooked.

In linking the ERM process steps to the execution in business, the process is guided by several activities indicated to the right of the diagram below:
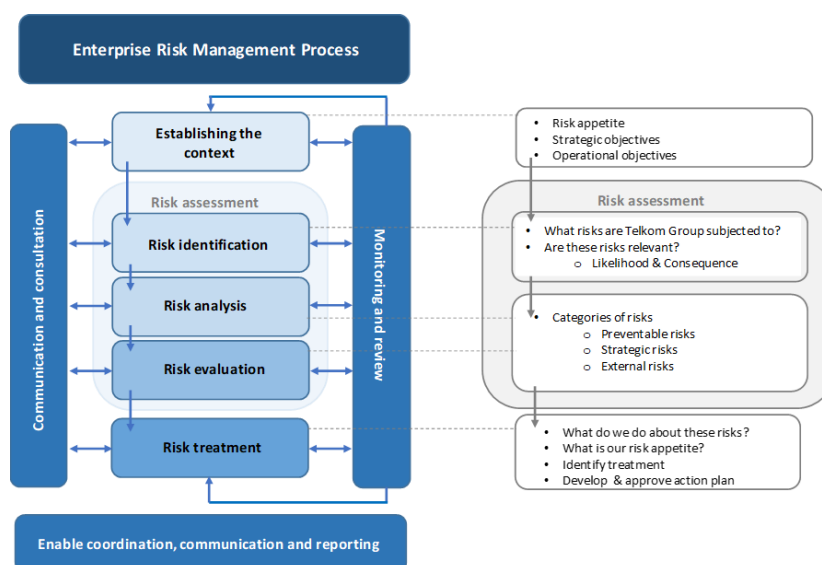
7   ESTABLISHING THE CONTEXT

7.1   Establishing context is crucial in the implementation of enterprise risk management. Context includes the following:

I.   External context: Consideration of the following areas form part of the external context: legal, regulatory, socio-economic, financial, and perceptions of external stakeholders.

II.   Internal context: Factors to be considered when making decisions and addressing the uncertain outlook include company's strategic objectives and direction, organisational chart, SOPs (Standard Operating Procedures), resources and culture.

7.2   Areas considered include, but is not limited to risk appetite, performance metrics and risk tolerance levels, risk profiling as well as reporting and control.

Creating a risk culture is one way of reinforcing overall risk appetite. Our approach is best used when the organisation has a well-communicated risk appetite and associated risk tolerances, to the point at which the following outcomes exist:

I.   Consistent implementation across units and effective monitoring and communication of risk and changes in risk appetite.

II.   Consistent understanding of risk appetite and tolerances for each organisational unit as well as consistency between risk appetite, objectives and relevant reward systems.

This approach draws on ongoing and separate evaluations conducted as part of the Organisation's monitoring. Any variation from the stated (or desired) risk appetite is then reported to management and the board as part of the normal internal reporting process.

7.3   Strategic Objective Setting

Establishing objectives which are aligned with the Organisation's mission, vision, goals and values, is the reference point for identifying and assessing risks. Thus, the objective setting is a pre-condition to any risk management process. Objectives are aligned with the Organisation's risk appetite, which drives the risk tolerance levels.

8   RISK ASSESSMENT

The ERM process is driven by a series of activities and events designed to integrate ERM within business processes across the enterprise and ensure that there are standardisation and common elements across all these occurrences. Risk assessment activities include: risk identification, risk analysis and evaluation, control effectiveness and risk prioritisation.

Business value benefits considered during the risk prioritisation process refer to benefits to the target market (existing customers and/or prospective customers), increased profitability, shareholder value and improved customer experience.

9   RISK AND OPPORTUNITY RESPONSES

In considering its response, management considers costs and benefits and select a response that brings expected likelihood and impact within the desired risk tolerance, thus reducing the risk to an acceptable level. The diagram illustrates the risk response (strategy) concepts:
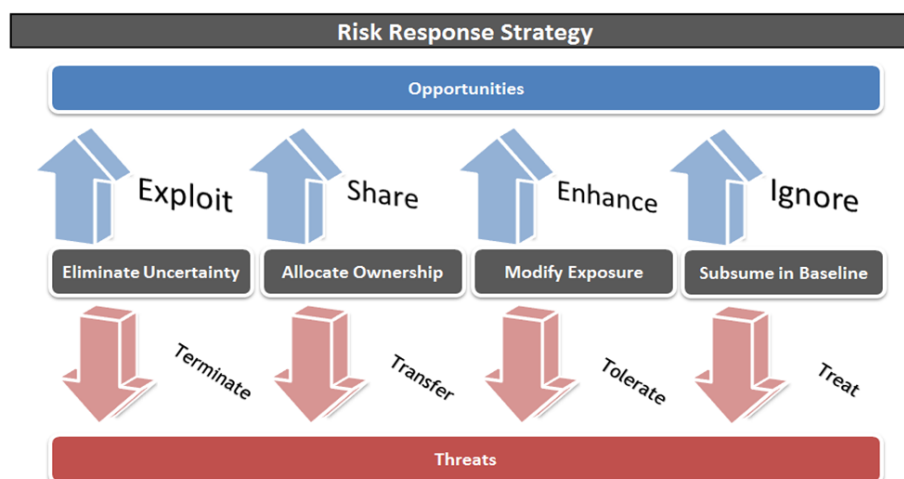
10   MONITORING AND REVIEW

Monitoring of the risk and assurance process is performed on an ongoing basis through the constitution and convening of various committees, through interaction with management and the combined assurance process. The purpose of the monitoring and review process is to:

I.   Provide assurance that risks are being managed as regularly as expected.

II.   Assess whether the risk response plans remain relevant.

III.   Ensure that the risk profile of the company anticipates and reflects changed circumstances and new exposures.

Further to this, the risk exposure is monitored on an ongoing basis through the identification and analysis of appropriate key risk indicators. Key Risk Indicators (KRI's) act as early warning signals by providing the capability to indicate changes to the Organisation's risk profile

11   RISK REPORTING

The primary purpose of risk reporting and disclosure is to provide stakeholders with confidence in the strategy, tactics, and operations of the Organisation.

In the ERM policy, the board has established how and when it shall receive information about risks and risk management. The periodic recurring risk reporting is designed to provide reliable, current, complete, and timely information to the recipients, reflecting the nature of different risk types as well as market developments. The board, risk committee, and various forums, receive regular reports on the status of risks and risk management.

In addition, reporting on risks in the integrated report serves the purpose of holding the directors to account to ensure they are managing both internal and external factors which could destroy value and threaten the viability of the Organisation.

ERM Policy and Framework

12   ANNEXURE A: DEFINITIONS, ACRONYMS, LAWS & REGULATIONS

12.1   Definitions

Definitions	Description
Risk	Risks are uncertain future events that could influence the achievement of Organisation's strategic objectives. This includes both negative and positive events.
Enterprise Risk Management Policy	Articulates the commitment of the board to the process of enterprise risk management and defines roles and responsibilities for managing risks across the Organisation
Risk Management	Risk management is a consistent approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues and opportunities.
Enterprise Risk Management	Is a process, affected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
Risk Management Culture	Culture of shared values, beliefs, assumptions and behaviours that characterises the Organisation, especially in relation to risk management requirements.

12.2   Acronyms

Acronyms and Abbreviations	Description
Board	Board of Directors
Exco	Executive Committee
GCEO	Group Chief Executive Officer
ERM	Enterprise Risk Management

12.3   Laws and Regulations

    I.   Companies Act 71 of 2008

    II.   King IV Code on Corporate Governance 2016^{TM}

    III.   COSO (Committee of Sponsoring Organizations of the Treadway Commission) Integrated Enterprise Risk Management Framework

    IV.   ISO 31000: Risk management – Guidelines