MERAFE RESOURCES LIMITED

(“MERAFE”)

RISK MANAGEMENT POLICY & FRAMEWORK

TABLE OF CONTENTS

It should be noted that this framework does not apply to the operations of the Glencore-Merafe Chrome Venture as the Venture has its own ERM policy, framework and processes which are overseen by the Venture's Joint Board. Refer ANNEXURE 5 for more information on the Venture's ERM process.

1. THE EVOLUTION OF RISK MANAGEMENT

"The average company today is a complex enterprise engulfed by rapid technological change and fierce global competition. You have to assess exposure to risk in an ever changing landscape".

Today, risk management is an indispensable element of a corporate governance system in world class organisations. Numerous reasons support the growing importance and profile of risk management, the most likely being the unprecedented levels of business complexity and the impact of globalisation. In addition, the number of high-profile business failures in the last decade has played a significant role in elevating risk management as an important governance process.

Although risk management has risen in prominence in recent years, it is not a new phenomenon. However, it was only about since the mid 1990's that organisations began to realise the value of risk management as an integral component of business operations and an important contributor to the sustainability of organisations and the protection of shareholder value. Until the early 1990s risk management tended to be equated with loss prevention through insurance buying or hedging of financial risk with derivatives.

Since then the focus has shifted to an enterprise-wide risk management ("ERM") approach. This is a holistic, integrated, forward-looking and process-orientated approach to managing all key business risks, not just financial ones, with the intent of maximising shareholder value for the enterprise as a whole. It provides a whole new paradigm on risk management.

2. THE BUSINESS IMPERATIVES FOR ERM

The purpose of an enterprise risk management process is to ensure that all risks that Merafe is exposed to are proactively identified and managed to acceptable levels on a continuous basis. The business imperatives or key drivers to embed such a process within the fabric of Merafe's operations are:

- the achievement of business objectives whilst avoiding unplanned impacts on Merafe's operations and financial results as a consequence of risks that take the company by surprise;
- reduce the impact of Merafe's operations to people and the environment;
- the need to protect Merafe's reputation and image;
- to comply with the requirements of the King Report on Corporate Governance;
- to successfully respond to an ever-changing business environment; and
- to create a more risk aware culture within the company.

3. RISK MANAGEMENT POLICY STATEMENT

The complexity of business transactions, rapid advances in technology, globalisation, speed of product cycles and the overall pace of change continue to increase the volume and complexities of risks facing our company. As a company, we must take risks to create value for our stakeholders. However, we must ensure that we have robust risk management capabilities in place to effectively manage these risks. Sound management of risks will enable the company to anticipate and respond to changes in the external and internal business environment and to take informed decisions in uncertain conditions.

The Board of Directors has committed the company to a risk management approach which is systematic, structured, consistent and continuous and which is aligned with an internationally recognised risk management standard, good practice and the King Report on Governance for South Africa ("King IV"). Risk management must be embedded in, not overlaid upon, every aspect of how we

run our company. Our aim is for risk management to become embedded into the day- to- day activities of the company.

Responsibility and accountability for management of business risks rests with managers and staff. Every employee has an important role to play in the risk management process. The Board of Directors retains overall responsibility for the total process of risk management.

Compliance with this policy and the effectiveness of the company's risk management processes will be monitored by the Board Audit & Risk Committee.

4. BACKGROUND TO MERAFE'S BUSINESS

Merafe Resources Limited (Merafe or the company) is listed on the JSE Limited under the share code MRF in the "General Mining" sector. The main business of Merafe and its wholly-owned subsidiaries is the production and sale of ferrochrome to the stainless steel industry through its 20,5% participation in the earnings before interest, tax, depreciation and amortisation (EBITDA) of the Glencore-Merafe Chrome Venture (the Venture).

The Venture, the largest ferrochrome producer in the world, supplies stainless steel mills in Europe, America and Asia (including China, Japan, Taiwan and Korea).

Merafe and Glencore South Africa (Pty) Ltd (Glencore) (previously Xstrata South Africa (Pty) Ltd) – a wholly-owned subsidiary of Glencore plc (previously Xstrata plc) established the Venture on 1 July 2004. Both parties agreed to pool their chrome operations (while retaining ownership of their assets) and to share in the EBITDA of the Venture.

The Merafe-owned assets that were pooled into the Venture at its inception were the Boshoek ferrochrome plant, Boshoek and Horizon mines and the Kanana UG2 plant. Since then Merafe has increased its ferrochrome interests and its interests in the Venture by acquiring a 50% interest in furnaces 5 and 6 of the Wonderkop ferrochrome plant and Kroondal mine; a 26% interest in Marikana mine and a 20,5% interest in the Lion ferrochrome plant (Phase I and 2), the

Bokamoso pelletising and sintering plant, the Tswelopele, Mototolo and EPL UG2 plants and the Helena and Magareng mines.

The most significant risks that impact Merafe are as follows:

- commodity price volatility
- fluctuation in currency exchange rates
- changes to laws and regulations and non-compliance
- state of global economy
- state of the ferrochrome industry: SA electricity cost and China's dominance
- socio- political climate in SA
- uncertainty regarding empowerment

5. PURPOSE OF THIS FRAMEWORK

The purpose of this framework is to:

- Describe Merafe's risk management philosophy, approach and process;
- Guide the implementation of the risk management process in a uniform manner across the company; and
- Educate managers and employees on the essential tasks of risk management.

6. SCOPE OF APPLICATION

This Framework will be applied to all functions and processes of Merafe and, as such, covers the following broad categories of risk:

Strategic – those risks that have an influence on the viability of Merafe's strategic goals, objectives and business model

Operational – those risks that have an influence on the effective and efficient execution of Merafe's business strategy

Reporting – those risks that have an influence on the integrity of Merafe's financial and other key reports

Compliance – those risks that have an influence on non-compliance with applicable laws and regulations

Non-compliance with this document will be dealt with in accordance with Merafe's disciplinary procedures.

7. INTENDED USERS OF THE FRAMEWORK

The intended users of this framework are everyone in the organisation who is charged with the responsibility and accountability for managing risks. This includes (but not limited to):

- Merafe Board – responsible for the total process of risk management within the organisation and for ensuring that management have implemented an effective and efficient risk management process within the organisation;
- Executive Committee – accountable to the Board for designing, implementing and monitoring the risk management processes;
- Senior Managers – responsible and accountable for effectively managing risks within their respective areas of responsibility; and
- All other managers and employees – responsible for assisting the Managers in executing their responsibility.

8. OTHER RELATED POLICIES

This Framework should be considered in conjunction with these other related policies, inter alia:

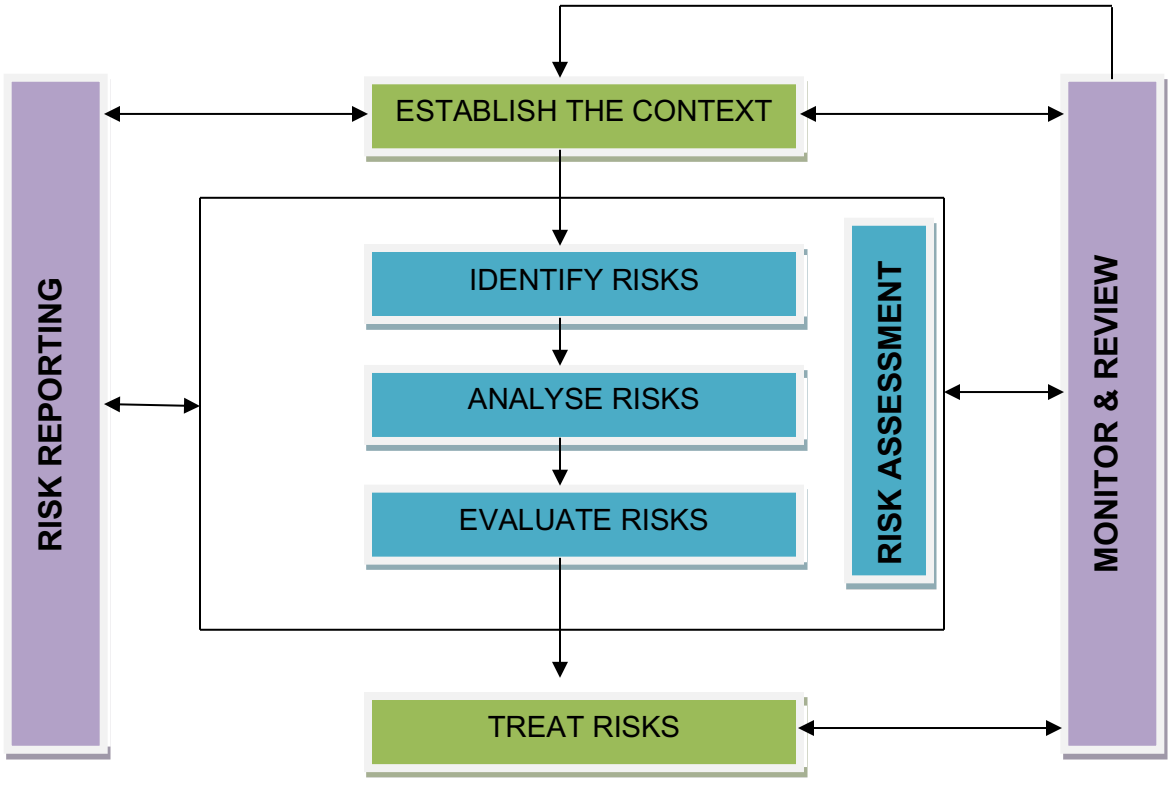
- Code of Ethics
- Fraud and Whistle blowing

9. RISK MANAGEMENT PROCESS

The elements of Merafe's risk management process are set out in the figure below.

At a minimum, the process should be triggered:

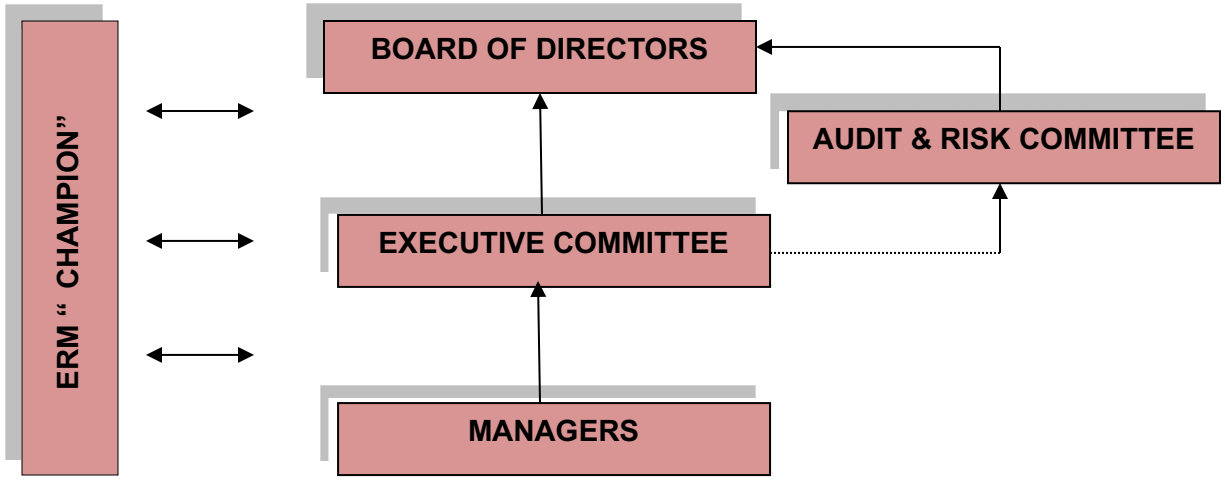
Semi - Annually **OR** **When change events occur**



ANNEXURE 1 provides more detail on each of the elements of the process.

10. RISK GOVERNANCE STRUCTURE

The figure below sets out the structure in place to govern the ERM process at Merafe Limited level.



The responsibilities of each of the elements of the governance structure are set out below.

Element	Responsibilities
Board	• The Board is responsible for the overall governance of risk • The Board should determine the levels of risk tolerance • The Board should delegate responsibilities to management to design, implement and monitor the risk management plan • The Board should ensure that risk assessments are performed on a continuous basis • The Board should ensure that frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks • The Board should ensure that management considers and implements appropriate risk responses • The Board should ensure continual risk monitoring by management • The Board should ensure that there are processes in place which will enable timely, relevant, accurate risk disclosure to stakeholders • The Board should receive assurance regarding the effectiveness of the risk management process
Audit & Risk Committee	• Assists the Board in the execution of its responsibilities regarding risk management • Its risk management responsibilities are set out in its Terms of Reference
Executive Committee	• Ensure that all material risks have been identified and

	are being appropriately managed • Ensure that the total process of risk management is effective and is integrated into the day-to-day activities of the company • Provide adequate and timely risk reports to the Audit & Risk Committee
Manager	• Ensure that the ERM process is properly applied within their respective areas of responsibility • Ensure that material risks are identified and are appropriately managed • Provide adequate and timely risk reports to Risk Champion and EXCO
Risk Champion	• The Risk Champion, as the custodian of the ERM process, is responsible for the following: • Implementing the ERM process across the organisation • Ensuring that departmental risk registers are being maintained • Maintaining the strategic risk register • Continuously improving the risk management process • Preparing risk reports for EXCO and Audit & Risk committee • Liaise with internal audit, external audit and other assurance providers on scope of work and findings • The FD will play the role of risk champion. The merits of this arrangement will be assessed from time to time.

11. REFRENCES

The following were used in the preparation of this Framework:

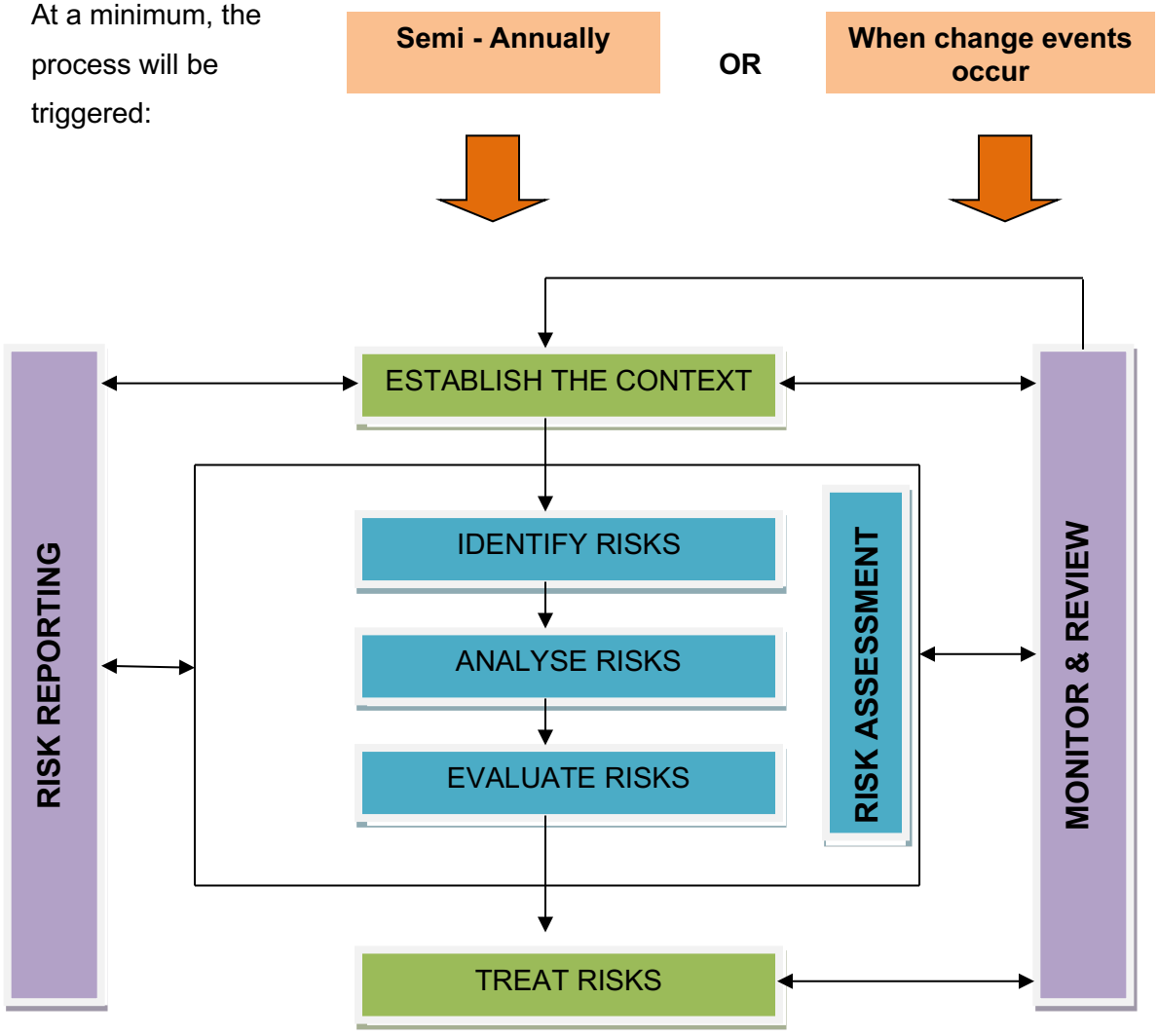
- Australian/New Zealand Standard on Risk Management (AS/NZS 4360: 2004);

- Risk management standard ISO 31000:2009, issued by the International Organisation for Standardisation;
- King Report on Governance for South Africa, ("King IV"); and
- COSO Enterprise Risk Management – Integrated Framework

ANNEXURE 1

A DESCRIPTION OF THE RISK MANAGEMENT PROCESS

At a minimum, the process will be triggered:



At a minimum, the process will be applied across the organisation semi-annually or when certain change events occur. However, notwithstanding the aforegoing,

it is expected that risk management processes will be embedded within the day-to- day activities of everyone within the company.

Examples of change events that may trigger the application of the risk management process within a part of the business or across the entire business are as follows:

- Changes in business strategy
- Legal & regulatory changes
- Restructuring of the business or departments or processes or major changes to people, processes and technology
- Loss of key personnel
- Significant control deficiencies identified by internal and/or external auditors
- Incidences of fraud
- Legal liabilities and challenges
- Changes to business objectives
- Changes to key performance indicators

ESTABLISH THE CONTEXT

Establishing the context is a prerequisite to the process of identifying risks in any given situation. Establishing the context is about placing a boundary around the subject matter that is being subjected to the risk management process. Contexts can be entire businesses, functions, departments, processes, projects, activities, specific business decisions that must be taken and the like. In setting the context, consideration must be given to:

- the business objectives of the subject matter that is being covered;
- the purpose, scope and depth of the risk management process to be applied;
- the time horizon to be covered for risk identification purposes;
- establishing the roles and responsibilities of the various people and parts of the organisation participating in the risk management process;

- subdividing the subject matter into a set of elements in order to provide a logical framework that helps ensure that significant risks are not overlooked; and
- deciding the criteria against which risks will be evaluated

IDENTIFY RISKS

The purpose of risk identification is to identify all risks within the context established above. The aim is to generate a comprehensive list of risks that might have an impact on the achievement of each of the objectives identified in the context phase above. These events might prevent, delay or enhance the achievement of those objectives. Comprehensive identification using a well structured, systematic process and involving the right people is critical, **because a risk not identified at this stage may be excluded from further analysis.** Risk identification should include all risks irrespective of whether or not they are under the control of MERAFE.

It is important that the following aspects are well understood prior to commencing with the risk identification process:

- the external environment
- stakeholder interests and expectations
- relevant business process activities
- relevant business objectives and business strategy

The Risk Universe set out in ANNEXURE 3 could be used to assist in the risk identification process.

Any one or more of the following techniques may be used to identify risks:

- **Facilitated workshops**

This is the most common technique. These workshops typically bring together cross-functional and/or multi-level individuals for the purpose of drawing on the

group's collective knowledge to identify risks based on judgement, past experiences etc.

- **Questionnaires and surveys**

  These can be directed to one or many individuals both within the organisation and external parties.

- **Process flow analysis**

  Involves the diagrammatic representation of a process with the goal of better understanding the interrelationships of its component parts. Once mapped, risks can be identified and considered against the process objectives.

- **Interviews**

  These are one-on-one interviews for purposes of ascertaining the interviewees' knowledge of potential future events.

- **Scenario analysis**

  This is a forward looking methodology for purposes of understanding the range of future uncertainties and testing the robustness of business strategies and evaluating the "what if" impacts.

- **Ongoing event identification**

  Potential risks also need to be identified on an ongoing basis. The table below sets out certain ongoing risk identification mechanisms.

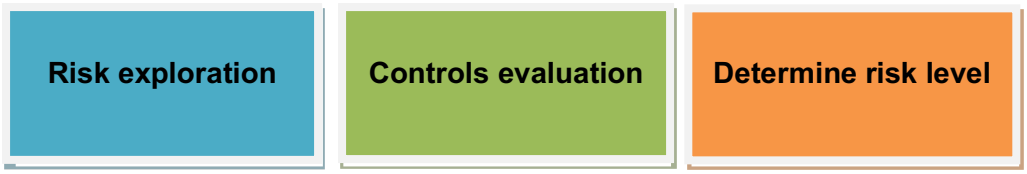
Continuous risk identification mechanisms

Mechanism –Input from	External Factors					Internal Factors			
	Economic	Natural Environment	Political	Social	Technological	Infrastructure	Personnel	Process	Technology
Industry /technical conferences	✓	✓	✓	✓	✓	✓	✓	✓	✓
Peer company website and advertising campaign	✓				✓				
Political lobbyist			✓						
Internal risk management meetings						✓	✓	✓	✓
Benchmarking reports	✓				✓	✓	✓	✓	✓
Key external indices	✓	✓	✓	✓	✓				
Key internal indices/risk & performance measures/scorecards						✓	✓	✓	✓
New legal decisions	✓		✓	✓					
Media reports	✓	✓	✓	✓	✓				
Monthly management reports						✓	✓	✓	✓
Analyst reports	✓		✓	✓					
Electronic bulletin boards and notification services	✓	✓	✓	✓	✓				
Industry, trade, and professional journals	✓	✓	✓	✓	✓				
Real-time feeds of financial market activity	✓								

Source: COSO ERM Framework

ANALYSE RISKS

This phase covers the following elements:



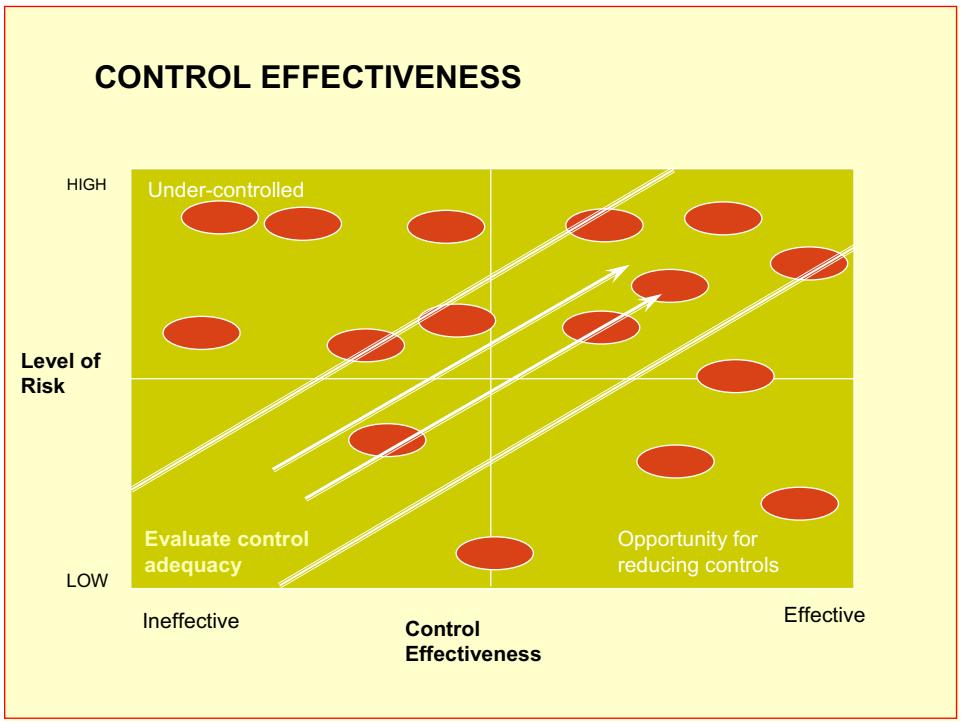
Each of these elements is dealt with below.

- **risk exploration** (understanding the causes and consequences of identified risks)

  The purpose of risk exploration is to understand the causes and consequences of the identified risks. In the absence of a precise understanding of the cause of a risk, one is unable to design effective **preventative** control measures to manage the cause. Similarly, in the absence of a precise understanding of the nature of the consequences of a risk, one is unable to accurately measure the impact that the risk may have nor implement effective **corrective** control measures to manage the impact.

- **controls evaluation** (evaluating existing risk treatment controls)

  This involves obtaining an understanding of the existing preventative and corrective controls currently in place to treat the risk and then assessing the effectiveness of those controls using the table in ANNEXURE 2.
  The figure below provides an overview of the relationship between risk level and control effectiveness:



- **determine risk level** (measuring the impact and likelihood levels of identified risks)

  This phase involves assessing the magnitude of the consequences of a risk, should it occur, and the likelihood of the event occurring. This consequence and likelihood is combined to produce a risk level. The risk assessment matrix and the impact and likelihood rating tables as set out in ANNEXURE 2 will be used to facilitate this process. Based on the matrix, any given risk will be assessed at one of 4 levels.

  Two types of risk assessments could be perfomed, namely qualitative and quantitative.

  Qualitative assessments are used where risks do not lend themselves to quantification or when either sufficient credible data required for a quantitative assessment is not practically available or a quantitative assessment is not cost-

effective. Qualitative assessments are typically based on subjective views of individuals. The following are some of the information sources when performing a qualitative assessment:

- Past incidents and experience;
- Published literature;
- Consultations with stakeholders; and
- Expert judgements

Quantitative techniques involve the use of mathematical models, bring more precision and are typically used in more complex and sophisticated activities to supplement qualitative techniques.

It should be noted that qualitative assessments will suffice for the vast majority of risks.

Risks are normally assessed at an inherent level and at a residual level. It is accepted, however, that in certain contexts the inherent risk assessment will not add value and that only a residual assessment is performed.

The inherent assessment is an assessment of the level of risk before the evaluation of existing risk treatment controls have been considered.

The residual risk assessment is an assessment of the level of risk after risk treatment controls have been evaluated.

EVALUATE RISKS

The purpose of risk evaluation is to make decisions, based on the outcomes of risk analysis, about which risks need treatment as well as well as risk treatment priorities.

Risks assessed as Level 1 risks will receive the highest priority, followed by levels 2 to 4 respectively. Individual risks or an aggregation of common risks at levels 1 and 2 will generally be considered as beyond Merafe's risk tolerance

level and therefore risks at these levels must be considered for further treatment as a matter of urgency.

The following diagram provides an overview of the relationship between risk level and risk treatment:

Risk level	Treatment Action
1	Very urgent action required to develop and implement risk treatment plans to reduce risk exposure
2	Urgent action required to develop and implement risk treatment plans to reduce risk exposure
3	Action to be taken at management's discretion after, amongst other things, assessing the cost of doing so versus the benefit to be derived
4	Risk exposure should be monitored but no immediate action required

TREAT RISKS

Risk treatment involves identifying and evaluating the range of available options for treating a risk and the preparation and implementation of appropriate treatment plans. It should be noted that more than one option may be taken to treat a particular risk.

Available options

Avoidance – Exiting the activities giving rise to the risk.

Mitigation – Action is taken to reduce the impact of the risk or likelihood of the risk occurring, or a combination of both.

Transfer – Reducing risk likelihood or impact by transferring or sharing a portion of the risk with third parties, e.g. buying insurance cover

Acceptance – Accepting the risk at its current exposure level

Selecting the most appropriate response or a combination of responses involves, amongst other things, balancing the costs of implementing the treatment against the benefits to be derived. The cost of managing a risk must be commensurate with the benefits to be derived.

Preparing and implementing risk treatment plans

The purpose of a risk treatment plan is to document how the chosen risk treatment option/s will be implemented. The treatment plans should include:

- proposed actions;
- resource requirements;
- risk owner; and

- timing.

The output from the process elements described above is a risk register.

MONITOR AND REVIEW

Any risk profile will change over time. Risk treatment plans that were once effective may become irrelevant; control activities may become less effective, or no longer be performed; business objectives may change or regulatory requirements may change. This can be due to the arrival of new personnel, changes in the business structure or direction, the introduction of new systems and processes or developments in the external environment. In the face of such changes, management needs to continually monitor the effective functioning of the risk management process. This monitoring should occur in the normal course of management activities.

The following monitoring mechanisms will be implemented:

- **Monitoring of implementation of risk treatment plans**

  Action plans to develop and implement risk treatment plans need to be monitored to ensure that the necessary plans are implemented on schedule and as intended. This monitoring process should be embedded within the normal day to day monitoring processes already in place within the business e.g. departmental meetings, management meetings, Exco meetings etc.

- **Monitoring of ongoing effectiveness of risk treatment controls**

  The effective operation of risk treatment controls must be evaluated on an on-going basis.

  These evaluations may include management reviews, self-assessment reviews and third-party reviews as appropriate.

  Monitoring periods should generally not exceed three monthly periods.

  Key risk indicators are useful risk monitoring tools and should be reflected on the risk registers for each significant risk. They are used to:

-provide timely leading-indicator information about emerging risks

-provide an early warning signal of increasing risk exposures in various areas of the business

- **Monitoring of the effectiveness of the risk management process as a whole**

  The efficacy of the entire risk management process needs to be considered for review on a periodic basis. At the Board's discretion, an independent assurance provider could perform such a review on a periodic basis and provide assurance to the Board that the risk management process has been applied appropriately across the organisation and that all elements of the process are suitable and sufficient.

RISK REPORTING

The essence of risk reporting is that the right people must receive the right risk information at the right time so that corrective action is taken on a timely basis.

The following risk reporting protocols will apply for Merafe:

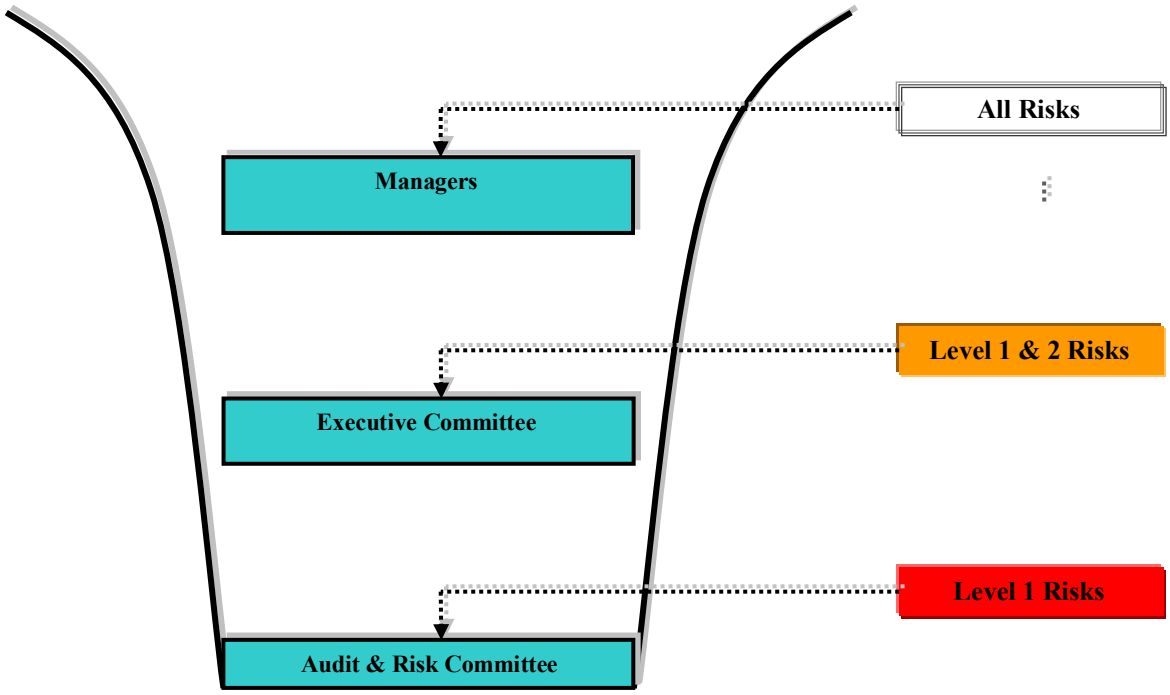
Risks at all levels must be reported internally (formally and informally) within each department on an ongoing basis.

Level 1 & 2 risks will be elevated to and considered by EXCO on a monthly basis.

Level 1 risks will be elevated to and considered by the Board Audit & Risk Committee at each of their scheduled meetings.

Standard risk reporting formats and templates for all levels will be developed.

The risk reporting protocol is depicted in the figure below:


All Risks
Managers
Level 1 & 2 Risks
Executive Committee
Level 1 Risks
Audit & Risk Committee

ANNEXURE 2

RISK ASSESSMENT TABLES

Risk matrix

					Impact descriptor
Level 2 Risk	Level 2 Risk	Level 1 Risk	Level 1 Risk	Level 1 Risk	Catastrophic
Level 3 Risk	Level 3 Risk	Level 2 Risk	Level 2 Risk	Level 1 Risk	Critical
Level 3 Risk	Level 3 Risk	Level 3 Risk	Level 2 Risk	Level 1 Risk	Serious
Level 4 Risk	Level 3 Risk	Level 3 Risk	Level 3 Risk	Level 3 Risk	Moderate
Level 4 Risk	Level 4 Risk	Level 4 Risk	Level 3 Risk	Level 3 Risk	Minor
Rare	Unlikely	Possible	Likely	Almost certain	
Likelihood Measures					

Impact Rating Table

The table below is to be used in assessing the potential impact of a risk

Impact descriptor	Operations	Safety security Health	Legal and regulatory Environmental Reputational	Financial
Catastrophic	Future operations at site seriously affected. Loss of production > 12 weeks	One or more fatalities	Prolonged international, regional and national condemnation Extreme environmental damage (Irreversible incident)	Earnings > 150m Assets > 500m
Critical	Loss of production between 8 and 12 weeks	Critical injury to staff or members of the public (Irreversible impact on health)	International criticism Major environmental damage (reversible over long-term)	Earnings 60m - 150m Assets 300m - 500m
Serious	Loss of production between 4 and 8 weeks	Serious injury to staff or members of the public (reversible impact on health)	Serious negative regional criticism Significant environmental damage (Incident remediable within medium term)	Earnings 40m - 60m Assets 200m -300m
Moderate	Loss of production between 2 and 4 weeks	Lost time injury	Serious negative national criticism Remediable environmental damage (short-term)	Earnings 20m - 40m Assets 100m - 200m
Minor	Loss of production < 2 weeks	First aid cases	Adverse national public attention No material environmental, safety or health impacts	Earnings <20m Assets < 100m

Likelihood Rating Table

The table below is to be used in assessing the likelihood of occurrence of a risk

Category	Criteria
Almost certain	The event is expected to occur or occurs regularly (>75% chance)
Likely	The event will probably occur (>50 % chance)
Possible	The event may occur (15-50% chance)
Unlikely	The event could occur (5-15% chance)
Rare	The event is unlikely to occur (<5% chance)

Control Effectiveness Rating Table

The table below is to be used in assessing the effectiveness of controls in place to treat a risk

Control effectiveness	Criteria	Factor
Unsatisfactory	Controls are non-existent or totally ineffective	0.1
Weak	There are major deficiencies in the control system	0.2
Satisfactory	There is some room for improvement in the control system	0.35
Good	Controls are generally effective to reduce the risk or impact.	0.6
Excellent	Controls could not be more effective	0.8

ANNEXURE 3

RISK UNIVERSE

This risk universe should be used in the risk identification process. It should be noted, however, that the list is not intended to be all-inclusive.

Environment Risks

Competitor
Customer wants

Technological innovation

Stakeholder expectations

Political

Legal

Regulatory

Industry

Financial markets

Natural disasters

Economic

Social

Natural environment

BEE

Process Risks

Financial
Price:
Interest rate
Currency
Commodity
Financial Instruments
Liquidity:
Cash flow
Concentration
Credit:
Default
Concentration
Collateral
Credit rating

Operations
Customer satisfaction
Human resources
Supply chain
Business interruption
Compliance
Health & safety
Environmental
Knowledge & information mgt.
Reputation & Brand
Product/service
Partnering
Cultural
Contract management
Asset management
Capacity
Efficiency
Distribution channels

Governance
Culture
Ethical behavior
Board effectiveness
Succession planning

Integrity
Fraud
Unauthorised use
Illegal acts

Information Technology
Integrity
Access
Availability
Security
Infrastructure
Obsolescence
Integration/interface

Information for decision making risks

Strategic
Business model
Org. structure
Budgeting & Planning
Strategic alignment
Investment valuation
Investment evaluation

Reporting
Financial reporting
Internal controls
Taxation
Pension Fund
Regulatory reporting

ANNEXURE 4

GLOSSARY OF TERMINOLOGY

Term	Definition
Risk	Effect of uncertainty on objectives
Risk management	Coordinated activities to direct and control an organisation with regard to risk
Risk management framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring and continually improving risk management throughout the organisation
Risk management policy	Statement of the overall intentions and direction of an organisation related to risk management
Risk appetite	Amount and type of risk that an organisation is prepared to accept
Risk bearing capacity	The maximum amount that an entity can afford to lose without jeopardising the future viability of the entity
Risk tolerance	Operational metrics in various areas of the business that help ensure that an organisation does not breach its risk appetite
Risk management plan	A plan of risk management activities for the year including the resources required to execute the plan
Risk owner	Person with the accountability and authority to manage the risk
Risk management process	Systematic application of management policies, procedures and practices to the activities of identifying, analyzing, evaluating, treating, monitoring, reviewing and communicating risks
Stakeholder	Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk source	Something which has the potential to give rise to risk
Event	Occurrence of an incident, accident or situation which occurs in a particular place during a particular interval of time. It can have several causes and can result in a range of consequences
Consequence	Outcome of an event affecting objectives
Likelihood	Chance of something happening

Risk profile	Description of any set of risks. The set of risks can relate to the whole organisation or a part of the organisation
Risk register	A formal listing of risks identified, together with the results of the risk assessment and details of risk treatment strategies
Risk analysis	Process to understand the nature of the risk and to determine the level of risk
Level of risk	Magnitude of a risk expressed in terms of the combination of consequences and likelihood
Risk evaluation	Process of determining whether the risk is acceptable or tolerable
Risk treatment	Process of selecting and implementing measures to modify risk. Risk treatment measures include avoidance, transfer, acceptance and mitigation
Residual risk	The level of risk remaining after risk treatment
Key risk indicator	Metrics used by organisations to: -provide timely leading-indicator information about emerging risks -provide an early warning signal of increasing risk exposures in various areas of the business

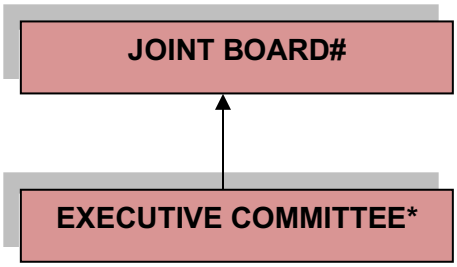
ANNEXURE 5

OVERVIEW OF GLENCORE-MERAFE CHROME VENTURE'S ERM GOVERNANCE STRUCTURE AND PROCESSES

Background

Merafe's main business is its 20,5% interest in the Venture and, thus, ensuring proper governance of the activities of the Venture is very important to the company.

Venture's Governance Structure



* Merafe representation is the same as the Joint Board
# made up of 2 representatives from each company. Merafe is represented by its CEO and FD.

Venture's ERM Processes

"Each operation within the Venture implements and maintains robust and formalised risk management systems and processes. Significant changes to identified and anticipated risks, and actions taken to or being considered to control the risks, are reported to the Venture's Executive Committee and Joint Board on a monthly basis to ensure that management is fully informed on the business risk profile."
"Roles and responsibilities for risk management are clearly defined within the Venture and the internal audit function is responsible for ensuring that operational risk management controls are effective."
In addition, the risks listed in the Venture's risk register are reviewed by Merafe's Audit & Risk Committee at each of its scheduled meetings.