



## ENTERPRISE RISK MANAGEMENT POLICY

ERM002

DOCUMENT USERS : Harmony Employees

PERSON RESPONSIBLE FOR KEEPING : ERM MANAGER/ERM TEAM  
DOCUMENT CURRENT

Revision	Prepared	Reviewed	Approved	Date	Description
3	Eben Janse van Rensburg	Exco	Board	July 2019	Finalised for use
4	Eben Janse van Rensburg	Exco	Board	Feb 2021	



---

## CONTENTS

1	Interpretation, Definitions and Abbreviations.....	3
1.1	Definitions .....	3
1.2	Abbreviations .....	5
1.3	Roles and Responsibilities .....	5
2	Introduction .....	6
3	Policy Content.....	7
3.1	Policy Statement.....	7
3.2	Policy Principles and Rules .....	7
4	Supporting Clauses .....	8
4.1	Scope.....	8
4.1.1	Purpose.....	8
4.1.2	Applicability.....	8
4.2	Normative/Informative References .....	8
4.2.1	Normative .....	8
4.2.2	Informative .....	8
5	Appendices .....	8
6	Acceptance .....	9
7	Development Team .....	9
8	Acknowledgements.....	9
9	Record Security and prevention of unauthorised access to records .....	9
10	Compliance.....	9

## 1 Interpretation, Definitions and Abbreviations

### 1.1 Definitions

Term	Definition
<b>Adaptation</b>	In relation to human systems, the process of adjustment to actual or expected climate and its effects, in order to moderate harm or exploit beneficial opportunities; and  In relation to natural systems, the process of adjustment to actual climate and its effects.
<b>Capacity</b>	The positive managerial capabilities of individuals, households and communities to confront the threat of disasters (e.g. through awareness-raising, early warning and preparedness planning).
<b>Climate change</b>	A change in the state of the climate that can be identified by changes in the variability of its properties and that persists for an extended period, typically decades or longer.
<b>Consequence</b>	The expected losses in a given area based on a hazard scenario.
<b>Contingency planning</b>	The forward planning process to anticipate and solve in advance problems that typically arise during a response to an event that may or may not occur.
<b>Critical infrastructure</b>	Critical infrastructure is the assets, systems, and networks that are essential for the functioning of a society and economy. It includes the facilities for emergency services, energy, water, banking, transport and communications to name a few. These networks are also referred to as lifelines.  Disruption in one infrastructure might provoke unexpected failures to others. How to handle interdependencies becomes an important problem.
<b>Disaster</b>	A serious disruption of the functioning of a community or society causing widespread human, material, economic or environmental losses that exceed the ability of the affected community or society to cope using its own resources.
<b>Disaster management</b>	A continuous and integrated multi-sectorial, multi-disciplinary process of planning and implementation of measures aimed at- <ul style="list-style-type: none"> <li>• preventing or reducing the risk of disasters;</li> <li>• mitigating the severity or consequences of disasters;</li> <li>• emergency preparedness;</li> <li>• rapid and effective response to disasters; and</li> <li>• post-disaster recovery and rehabilitation.</li> </ul>
<b>Disaster risk</b>	The probability of harmful consequences, or expected losses (death, injuries, property, livelihood, economic activity disrupted or environmental damage) resulting from

Term	Definition
	interactions between (natural, human-induced or man-made) hazard and vulnerable conditions in a given area and time period.
<b>Emergency preparedness</b>	<p>A state of readiness which enables organs of state and other institutions involved in disaster management, the private sector, communities and individuals to mobilise, organise and provide relief measures to deal with an impending or current disaster or the effects of a disaster; and</p> <p>The knowledge and capacities developed by governments, professional response and recovery organisations, communities and individuals to effectively anticipate, respond to and recover from the impacts of likely, imminent or current hazard events or conditions.</p>
<b>Preparedness</b>	The knowledge and capacities developed by governments, professional response and recovery organisations, communities and individuals to effectively anticipate, respond to, and recover from, the impacts of likely, imminent or current hazard events or conditions.
<b>Resilience</b>	<p>Resilience means the ability to:</p> <ul style="list-style-type: none"> <li>a) Anticipate, identify, and adapt rapidly to threats, vulnerabilities, and opportunities</li> <li>b) Operate under stress without failure for extended periods of time</li> <li>c) Respond appropriately and rapidly to contain the impact (severity/duration) of an incident / threat</li> <li>d) Recover sufficiently and rapidly in a coordinated manner</li> <li>e) Evolve to a higher state of resilience in response to changes in the environment, near misses, and incidents (organisational learning)</li> </ul>
<b>Risk</b>	Effect of uncertainty on objectives
<b>Risk appetite</b>	Amount and type of risk an organisation is prepared to take in order to achieve its objectives
<b>Risk intelligent</b>	<p>Risk intelligent means the ability to:</p> <ul style="list-style-type: none"> <li>a) Think holistically about risk and uncertainty</li> <li>b) Speak a common risk language</li> <li>c) Effectively use forward-thinking risk concepts and tools to make better decisions</li> <li>d) Scan environment and identify emerging risks</li> <li>e) Capitalise on opportunities</li> <li>f) Create lasting value</li> <li>g) Ensure sustainability</li> </ul>

Term	Definition
	h) Pursue continuous learning
<b>Risk tolerance</b>	Organisation's readiness to bear risk after risk treatment, in order to achieve its objectives

## 1.2 Abbreviations

Abbreviation	Explanation
EXCO	Executive Committee (Harmony)
ISO	International Standards Organisation
ER	Enterprise Risk

## 1.3 Roles and Responsibilities

This policy is issued under the authority of the Harmony Board of Directors. The following roles and responsibilities are defined for the oversight and management of risk:

Role	Responsibilities
<b>Audit and Risk Committee of Harmony Board of Directors</b>	The Board empowers the Audit and Risk Committee to give oversight over the effective management of risk in Harmony through: <ul style="list-style-type: none"> <li>a) Approval of Harmony's Enterprise Risk;</li> <li>b) Approval of Harmony's risk appetite;</li> <li>c) Approval of Harmony's top Risks;</li> <li>d) Review of risk management reports submitted to it by management, and</li> <li>e) the integration and embedding of risk management in the business activities and culture of the company.</li> </ul>
<b>Group Chief Executive</b>	Accountable for the overall direction and effective design, implementation and functioning of integrated risk management in Harmony and reports in this regard to the Harmony Board of Directors through the Board Audit and Risk Committee.
<b>Executive assigned the accountability for risk (Enterprise Risk and Investor Relations)</b>	Accountable for shaping, safeguarding and specialised servicing of risk management across Harmony. Specifically, for the following: <ul style="list-style-type: none"> <li>a) The development of Harmony's Risk policy, framework, guideline, processes, procedures and systems;</li> <li>b) Development of the Harmony Risk Plan;</li> <li>c) Reporting to the Board and Exco on the status of risk in Harmony;</li> <li>d) External reporting in compliance with related legislation;</li> </ul>

<b>Role</b>	<b>Responsibilities</b>
<b>Executive Managers</b>	Accountable for effective risk management in their areas of responsibility, including: a) Functional and operational risk management; b) Emergency response structures, incident command systems and situational awareness capabilities;  Accountable for Harmony-wide capabilities related to their functional areas, or as assigned, including: Individual executives accountable as executive sponsors for corporate risks, including establishing Harmony-wide preparedness for specific national disaster priorities.
<b>Group/Regional Resilience Sponsors/RGM's</b>	Responsible for coordinating regional compliance initiatives and reporting.
<b>Enterprise Risk function</b>	Responsible for shaping, safeguarding and specialised servicing of risk management across Harmony.
<b>Risk process experts (champions/HOD's)</b>	Responsible for supporting the execution of risk management in the group/region/sites/functions/subsidiaries/projects.

Specific roles and responsibilities derived from the above are addressed in the relevant Enterprise Risk Management standards, processes and procedures.

## 2 Introduction

- The effective management of risk is essential for Harmony as a company, particularly given the vision, mission and strategic imperatives of Harmony.
- The objective of managing risk is to ensure that Harmony is able to formulate and execute its strategy effectively, to operate its business efficiently with minimum disruption, to proactively leverage opportunities as these arise, and to be able to respond rapidly and recover effectively from disruptions should these occur. It is therefore important that risks and opportunities that impact Harmony's objectives are identified, effectively managed and continuously monitored. It is also important that Harmony has the necessary structures and plans in place to be able to adapt, respond and recover effectively in the event of threats and incidents that affect its people, assets, stakeholders, operations and the environment.
- This policy document sets out the principles, rules and associated responsibilities for managing risk across the group and subsidiaries of Harmony.
- The policy is aligned to governance requirements in King III and IV. It also addresses compliance to the integrated ISO frameworks.

### **3 Policy Content**

#### **3.1 Policy Statement**

Harmony strives to be a leading risk intelligent organisation in support of its mission *to produce safe, profitable ounces and increase our margins*. It does so by embedding good risk management practices in all its governance and delivery processes at a strategic, business and operational level.

#### **3.2 Policy Principles and Rules**

##### **3.2.1 General policy principles**

- Harmony promotes an organisational culture which values effective management of risk through capabilities and measures embedded within its operations, decision-making processes, and the development and implementation of strategy.
- Harmony's governance of risk is aligned with the principles as set out by the King Code on Corporate Governance IV, including the allocation of dedicated time at the Board Audit and Risk Committee to assist it in carrying out its responsibilities in relation to executing its oversight of risk management in the company.
- Harmony drives continued enhancement of its risk management practices, through an annually updated Harmony Risk Management Plan which is prepared by management and approved by the Board Audit and Risk Committee. Harmony is committed to embedding risk management at all levels of the organisation in order to identify the risks and manage them in a consistent and proactive way, prior to events occurring that might prevent us from achieving our objectives.
- Harmony will adopt a structured approach to risk management, using consistent approaches for the assessment, treatment, monitoring and reporting of all types of risk, at all levels and for all activities across the business.
- There will be one guideline for the management of all types of risks that will be consistently applied across Harmony including its subsidiaries and projects.
- Risk Management is primarily the responsibility of line management, regarded as the first line of defence.
- The Harmony Executive Committee (Exco) will monitor and review the organisation's risk management plan, risk management system and the performance of risk management and the management of enterprise risks and report this to the Board Audit and Risk Committee on a quarterly basis.
- The Board Audit and Risk Committee is responsible for providing oversight over the functioning of Combined Assurance activities as the third line of defence. Assurance is provided through Independent reviews on adequacy and effectiveness of risk, control and governance mechanisms, including compliance of Harmony-wide risk management practices and processes.

---

## **4 Supporting Clauses**

### 4.1 Scope

#### **4.1.1 Purpose**

This policy defines a general commitment, direction and intention of enterprise risk management in Harmony in order to promote the creation of a consistent, value adding process that assists the organisation to achieve its objectives as a risk intelligent organisation.

The purpose is to protect Harmony against negative consequences and to maximise opportunities that arise in various areas including finance, people safety, the environment, brand and reputation, legal and compliance and continuity of production.

#### **4.1.2 Applicability**

This policy shall apply throughout Harmony, its regions, subsidiaries, projects, business functions integrated operations at a national and international level, and entities wherein Harmony has a controlling interest.

### 4.2 Normative/Informative References

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

#### **4.2.1 Normative**

- [1] King III Code of Governance Principles of South Africa 2009
- [2] King IV Code of Governance Principles of South Africa 2016
- [3] ISO 22301: Societal Security – Business Continuity Management Systems – Requirements
- [4] ISO 31000: Risk Management: Principles and guidelines
- [5] Harmony Insurance Policy

#### **4.2.2 Informative**

- [1] ISO Guide 73:2009/ARP 070:2009, Risk Management: Vocabulary.
- [2] SABS 0264-1 Terminology and implementation
- [3] The Business Continuity Institute: Good Practice Guidelines.
- [4] ISO 9001 Quality Management Systems.

## **5 Appendices**

Adherence to this policy will be monitored through combined assurance provided by:





- Management oversight and regular reporting to Harmony's governance structures (including Group/Regional governance committees, Exco and the Board and board sub-committees).
- Assessments undertaken and reports prepared by the Enterprise Risk function in Harmony.
- Assessments and audits undertaken by Harmony's Internal Audit and Forensics Departments.
- External independent assurance reviews (external auditors), legislators, regulators and benchmark and maturity assessments.

## 6 Acceptance

This document has been seen and accepted by:

Name	Designation
CEO: Peter Steenkamp	Group Chief Executive
Executive: Boipelo Lekubo	Executive: Financial Director

## 7 Development Team

This policy was developed by the Enterprise Risk Management function.

## 8 Acknowledgements

## 9 Record Security and prevention of unauthorised access to records

- All records shall be identified, classified, retained, stored and protected in such a manner that the evidential value thereof is not compromised in any manner.
- All appointed record custodians shall establish procedures that shall, as far as reasonably possible, prevent the unauthorised access to, copying, removal, destruction or tampering of records by record subjects, third parties or computer viruses. Records must be retained as defined in the Harmony document retention policy, laws and/or regulatory requirements.

## 10 Compliance

- All procedures, policies, etc. must be drafted in accordance with relevant legislation and regulatory requirements.
- Non-compliance with this policy will result in disciplinary action.
- This policy is applicable to all Harmony operations and subsidiaries.



Document No: APR005 Enterprise Risk Policy  
Issue Date:  
Review date:  
Page: 10 of 10

---

*Relevant signatories to be completed here*

---

**Chairman: Board of Directors  
Harmony Gold Mining Company Limited**

---

**Chief Executive Officer  
Harmony Gold Mining Company Limited**