



JULY

2023

# POLICY

ENTERPRISE RISK MANAGEMENT POLICY

GROUP-WIDE





## CONTENTS

<b>1   INTRODUCTION</b>	<b>3</b>
<b>2   APPLICATION</b>	<b>3</b>
<b>3   IMPLEMENTATION</b>	<b>3</b>
<b>4   POLICY PRINCIPLES</b>	<b>4</b>
4.1 PRINCIPLES	4
4.2 OPERATIONALISATION OF THE PRINCIPLES	4
4.3 DISCOVERY LIMITED BOARD STATEMENT	5
4.4 RISK TAXONOMY	6
<b>5   GOVERNANCE STRUCTURES</b>	<b>7</b>
5.1 DISCOVERY LIMITED BOARD	7
<b>6   ROLES &amp; RESPONSIBILITIES</b>	<b>8</b>
6.1 FIRST LINE OF DEFENCE – BUSINESS MANAGEMENT	8
6.2 SECOND LINE OF DEFENCE - OVERSIGHT	8
6.3 THIRD LINE OF DEFENCE - ASSURANCE	9
<b>7   TRAINING AND ATTESTATION</b>	<b>9</b>
7.1 TRAINING	9
7.2 ANNUAL ATTESTATIONS	9
<b>8   COMPLIANCE WITH THIS POLICY</b>	<b>9</b>



## 1 | INTRODUCTION

---

The aim of this Policy is to set out the principles and processes governing enterprise risk management within Discovery Limited and its subsidiaries (the “Group”). The Policy supports and facilitates high quality management of risk exposures appropriate to the nature and scale of the universe of risks faced by the Group.

This Policy is the Group’s overarching Enterprise Risk Management (‘ERM’) Policy and Operational Risk Policy.<sup>1</sup> It enables the Group to establish a comprehensive set of risk management methodologies which align with best practice standards and regulatory requirements in terms of governance and risk management.

The Policy sets out the high-level philosophy and guiding principles for effective risk management to ensure that risks which could significantly impact the ability of the Group to meet its objectives are identified, measured, monitored, managed, priced, mitigated, communicated and reported. It includes the roles and responsibilities of the relevant stakeholders, the governance of and processes for the day-to-day risk and control environment.

## 2 | APPLICATION

---

This Policy applies to Discovery Limited including its South African and international subsidiaries, insurance, and non-insurance entities. This includes:

1. All executive and non-executive directors;
2. All senior managers;
3. Full time, part time or temporary employees;
4. Any independent contractors or consultants under our direct control.

## 3 | IMPLEMENTATION

---

Each entity within the Discovery Group –

1. Must comply with the legislation applicable in that country’s jurisdiction;
2. Must have procedures in place to align its operations with the spirit and purpose of this policy; and
3. May elect to have its own policy in respect of Enterprise Risk Management / Operational Risk, provided that the policy is consistent with this Policy and that the required procedures are in place.

Each directly held intermediate holding company of Discovery Limited must facilitate the adoption of this Policy by the boards of its directly or indirectly held subsidiaries and is responsible for oversight of adherence to this Policy by its direct and indirect subsidiaries.

As there is no intermediate holding company in respect of the South African domiciled subsidiaries that are directly held by Discovery Limited, the CEO of Discovery SA Inc. fulfils the role of oversight and other responsibilities of directly held intermediate holding companies as set out in this Policy.

---

<sup>1</sup> This Policy is intended to meet the legislative requirements for the Group. This includes, but is not limited to:

- The Prudential Standard GOI 3: Risk Management and Internal Controls for Insurers paragraph 6.1 to have a board approved policy addressing operational risk.
- It also meets similar requirements set out in the Prudential Standard GOG: Governance and Operational Standards for Insurance Groups.
- Other risk related Legislative requirements across the Group.



A subsidiary within Discovery may elect to have its own policy considering its nature, scale and complexity, and the legislation under which it operates.

Such a policy must be consistent with this Policy and the Board of Discovery Limited (“Board”) must approve any deviation from this Policy by any of its directly held subsidiaries unless the deviation is necessary to facilitate compliance with legislative and regulatory requirements. In the latter instance, the approval is automatically granted if the board of directors of a subsidiary has communicated the need for such a deviation to the Board.

In respect of indirectly held subsidiaries of Discovery Limited, the board of the relevant intermediate holding company must approve any deviation from this Policy by any of its directly or indirectly held subsidiaries.

## 4 | POLICY PRINCIPLES

---

This section of the policy sets out the overarching ERM principles, the Group’s Board Statement covering their mandate in terms of risks, as well as the high-level risk process and the minimum risk taxonomy to be used across the Group.

### 4.1 PRINCIPLES

The minimum ERM principles (aligned to best practice) to be followed by the Group are set out below.

1. The ERM Policy establishes a consistent, **integrated risk management system** which is an integral part of all organisational activities. The mechanisation of the system is included in the underlying Frameworks and Standards.
2. A **structured and comprehensive approach** to risk management is embedded across the Group which contributes to consistent and comparable results.
3. The risk management system is **customised and proportionate** to the organisation’s external and internal context related to its objectives.
4. Our proactive risk culture is driven by a top-down approach of factoring risk into decision-making, and a bottom-up approach as part of operational activities ensures an **inclusive** system of risk management. Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered which results in improved awareness and informed risk management.
5. The risk management system is **dynamic** to allow for risks that emerge, change or disappear as Discovery’s external and internal context changes. The system anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.
6. The inputs to risk management are based on historical and current information, as well as on future expectations. The risk management system explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information used should be the **best available information** accessible to relevant stakeholders, in a clear and timeous manner.
7. **Human and cultural factors** are taken into consideration for the risk management system as these can significantly influence all aspects of risk management at each level and stage.
8. The risk management system is subject to **continual improvement** through ongoing learning and day-to-day experience.

### 4.2 OPERATIONALISATION OF THE PRINCIPLES

The Group defines risk as the probability of an event materialising which could have a negative or positive impact on achievement of the Group’s objectives. Risks include ‘emerging risks’ which are defined as a condition, situation or trend that develop in a way that could significantly impact the Group’s strategy, financial strength, competitive position or reputation within the next five years. By identifying and proactively addressing these risks and



opportunities, the Group is able to protect and create value for its stakeholders, through greater risk transparency, increased organisational effectiveness and improved business decision making.

ERM provides a framework<sup>2</sup> for managing these risks, which typically involves:

- Identifying particular events or circumstances relevant to the Group's objectives (risks and opportunities);
- Measuring them in terms of impact and likelihood;
- Monitoring the risks against the limits set and capital available;
- Managing risks by developing risk mitigation strategies and action plans where necessary;
- Providing the Discovery Limited Board and Senior Management with oversight of the risks faced by the Group through a regular risk reporting process;
- Applying risk management techniques consistently across the Group; and
- Integrating risk management and measurement into business processes.

The objective of ERM is to align business strategy, risk strategy, capital management, business processes, people and technology in order to evaluate and manage business opportunities, uncertainties and threats in a structured and disciplined manner. By linking risk capital values to the actual risk-taking activities, the Group is able to assess the projected and historical performance of these activities in proportion to the capital required to support them.

This process assists in ensuring that the Group considers risk and capital implications when making strategic and operational decisions. The development of a pro-active approach to risk management (i.e. using risk data to prevent losses rather than continually responding to the negative implications of unforeseen risks that have materialised) provides:

- Increased consistency in the measurement, treatment and communication of risks within the Group;
- Enhanced reporting and analysis of risks faced by the Group;
- Improved focus, attention and perspective to risk data which will be used in the calculation of regulatory and economic capital across the Group;
- Increased alignment to the Group strategy;
- Enhanced quantitative and metrics-based assessment methodology;
- Efficiency and effectiveness of activities related to all assurance matters;
- Cost-effective management and monitoring of risks; and
- Robust risk culture within the Group.

### 4.3 DISCOVERY LIMITED BOARD STATEMENT

The Group is committed to being an organisation with a high-quality ERM capability which covers all its activities and contributes to growth in economic value of shareholder assets and the protection of policyholder and member benefits. This is achieved by:

- Fostering an environment where consideration of risk is embedded in the Group's culture, business planning, decision making and day to day business activities;
- Being risk-conscious, risk-confident and risk-selective. Risks are considered appropriate if they are well understood, generate the required risk adjusted return (either financially or otherwise) and support the Group's objectives. The Group actively seeks to assume appropriate risks, against the background of a clearly articulated risk appetite and business strategy;
- Seeking to treat, tolerate, terminate and/ or transfer those risks for which the Group has little or no appetite or where the expected risk adjusted return is inadequate;
- Seeking to exploit those risks for which the Group has more appetite or where the expected risk adjusted return is adequate;
- Actively communicating the effectiveness and business benefits of risk management to all stakeholders;

---

<sup>2</sup> This is covered in more detail in the Group ERM Framework / entity specific ERM Framework where required.



- Continually developing and enhancing the Group's ERM capability in a manner that yields business benefit;
- Being able to provide reasonable and independent assurance to the Group's Senior Management and the Discovery Limited Board; and
- Ensuring that the various assurance providers are effectively coordinated and integrated to aid effective decision making.

#### 4.4 RISK TAXONOMY

In order to apply the principles described above, the Group has defined a universe of risks (the Discovery Limited Risk Taxonomy) which classifies risks into broad categories. In this structure the broader risk categories are grouped as level one risks. Under these level one risks, are more detailed level 2 risks which may vary by strategic strand and should be approved by each strand's relevant governance committee. The following nine level one risk types have been defined as part of the Discovery Limited ERM Framework:

RISK TYPE	DEFINITION
Business Risk	The risk that the Group will have lower than anticipated profits or experience a loss rather than making a profit. The risk is influenced by numerous factors, including sales volume, unit pricing/ margin, competition and the overall economic climate.
Credit Risk	The risk of loss arising from the failure of counterparties to meet their debt obligations owed to the Group for any reason when due.
Insurance Risk	The risk that an insured event will occur, resulting in the payment of a claim. This risk is influenced by a number of factors including the occurrence of claims, catastrophe events and reinsurance cover.
Liquidity Risk	The risk that the Group, though solvent and profitable on a balance sheet basis, either does not have the cash (or near cash) resources or the ability to liquidate its assets to meet its obligations to policyholders, debtors and/ or capital providers (as they fall due).
Market Risk	The risk that, as a result of market movements, the Group may be exposed to fluctuations in the value of or income from its assets and financial instruments, and the amount of its liabilities relative to expected.
Operational Risk	The risk of loss resulting from inadequate or failed internal processes, people, systems and/ or external events.
Regulatory Risk	The risk of an adverse financial impact, reputational damage, a breakdown of the regulatory relationship or regulatory sanction being imposed as a result of non-compliance to emerging and/ or existing regulatory requirements.
Strategic Risk	The risk of the current and prospective impact on earnings or capital resulting from an inappropriate or defective strategy. The risk arises from the Group's inability to implement appropriate business plans, strategies or decisions. It also relates to the Group's lack of responsiveness to industry changes.
Technology Risk	The risk of governing Technology, Information and Cyber in a way that supports the organisation in setting and achieving its strategic objectives. The risk arises from the increased reliance Business is placing on Technology, Information as well as Security, to enhance and integrate systems and processes to improve efficiencies, remove manual processes, thereby becoming more digitalised and making it more secure.



## 5 | GOVERNANCE STRUCTURES

---

The Group governance structure, including the governance structures of the business entities where the Group has management control, is available from the Company Secretariat. The Discovery Limited Board Charter sets out the scope and responsibilities of the Discovery Limited Board in respect of the business entities within the Group. The requirement is that the most current version should be adhered to.

In instances where a business entity has established separate governance structures in addition to the Group governance structures, the business entity should ensure that the responsibilities defined below are included in the terms of reference of the relevant committee structures.

### 5.1 DISCOVERY LIMITED BOARD

The Discovery Limited Board is ultimately responsible for risk management across the Group. The Discovery Limited Board may delegate some of the activities or tasks associated with its own roles and responsibilities to a delegated committee or senior management within the Group which includes inter alia the following:

- The governance of risk;
- Approval of the levels of the risk appetite and tolerance limits;
- Ensuring an appropriate risk management plan is designed, implemented and monitored;
- Providing oversight in respect of the design and implementation of sound risk management and internal controls systems and functions;
- Ensuring that risk assessments are performed on a continual basis;
- Ensuring risk frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks;
- Ensuring that management considers and implements appropriate risk responses;
- Ensuring continual risk monitoring by management;
- Ensuring that the risk management process is effective by receiving assurance from the first, second and third lines of defence in a coordinated manner; and
- Ensuring there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to relevant stakeholders.

In order to establish adequate governance across the Group, the Discovery Limited Board has established the following sub-committees<sup>3</sup> which have a primary focus on risk:

1. **Discovery Limited Risk and Compliance Committee ('RCC')**, the terms of reference for this committee are defined in the Discovery Limited RCC Terms of Reference (ToR). This committee reviews all material entity and enterprise-wide risk assessments (including business resilience), control evaluations and mitigation plans on a regular basis. Risk assessments and action plans will form part of this broader ERM review.
2. **Discovery Limited Actuarial Committee**, the terms of reference for this Committee are defined in the Discovery Limited Actuarial Committee ToR. This committee reviews all material financial, insurance and actuarial risks.
3. **Discovery Limited Audit Committee**, the terms of reference for this Committee are defined in the Discovery Limited Audit Committee ToR. This Committee reviews the effectiveness of internal controls surrounding the risk management process and the reliability and accuracy of the financial information provided to management and other users of financial information; as well as reporting on significant findings from Group Internal Audit (GIA) reviews and the extent of management implementation of recommendations.

---

<sup>3</sup> Individual entities within the Group may choose to establish a different governance structure to the one illustrated below.



4. **Discovery Limited Treating Customers Fairly (“TCF”) Subcommittee**, the terms of reference for this Committee are defined in the Discovery Limited TCF Subcommittee ToR. This committee primarily reviews risk relating to customer treatment and market conduct.

DISCOVERY LIMITED BOARD		
Discovery Limited Executive Committee Discovery Limited Entity Executive Committees	Discovery Limited Audit Committee Discovery Assurance Risk and Compliance Committee Discovery Assurance Actuarial Committee Discovery Limited Remuneration Committee Discovery Limited Social and Ethics Committee Discovery Limited Technology Working Group	
MANAGEMENT	RISK MONITORING AND ASSURANCE	
<b>First Line of Defence</b> <ul style="list-style-type: none"> <li>Executive Committees</li> <li>Management of Operations</li> </ul>	<b>Second Line of Defence</b> <ul style="list-style-type: none"> <li>Group Risk Management Function</li> <li>Group Actuarial Function</li> <li>Group Compliance Function</li> </ul>	<b>Third Line of Defence</b> <ul style="list-style-type: none"> <li>Group Internal Audit</li> <li>External Audit</li> <li>Other Assurance Providers</li> </ul>

## 6 | ROLES & RESPONSIBILITIES

The Group has adopted the ‘Three Lines of Defence’ governance model. The model clearly separates business management from governance and control structures. A depiction of the ‘Three Lines of Defence’ is shown below. Individual entities within the Group may choose to establish a different governance structure to the one illustrated below. More detail on the structure, roles and responsibilities are included in the underlying frameworks and standards.

The following illustration sets out the overall Group structure:

### 6.1 FIRST LINE OF DEFENCE – BUSINESS MANAGEMENT

The ownership and management of risk is the responsibility of Business Management. This function is responsible for the operational management, management oversight, including strategy implementation, performance measurement, and risk and control management.

This line of defence has direct involvement, as the executing leg, and will therefore offer limited assurance coverage.

### 6.2 SECOND LINE OF DEFENCE - OVERSIGHT

The second line of defence functions comprise of the Risk Management Function, Compliance Function and Actuarial Function (where appropriate). These are functions independent of day-to-day management that provide a level of assurance to the Discovery Limited Board and entity Boards with regard to the adequacy and effectiveness of the overall risk management system. These functions have the authority to communicate with any employee and obtain unrestricted and timeous access to any records required to carry out their responsibilities.



The United Kingdom and Discovery Bank have their own second line of defence functions in place and report to the Group Functions for reporting purposes.

### **6.3 THIRD LINE OF DEFENCE - ASSURANCE**

The Group's Internal Audit Functions (South Africa, United Kingdom and Discovery Bank) and External Audit, make up the third line of defence and are independent assurance functions.

The third line of defence provides feedback on their activities and recommendations for improvement to senior management and Executive Committees, but reports directly to the respective Board(s) through the appropriate Audit Committee(s).

## **7 | TRAINING AND ATTESTATION**

---

### **7.1 TRAINING**

Each subsidiary must develop training programmes for affected employees and contractors and ensure that employees complete such training.

### **7.2 ANNUAL ATTESTATIONS**

Each directly held intermediate holding company of Discovery Limited must provide an annual attestation on the adherence to this policy, including that of its direct and indirect subsidiaries, facilitated by a Discovery Limited platform.

## **8 | COMPLIANCE WITH THIS POLICY**

---

Our policies support our Values and reflect what is important to us. We take breaches of our policies seriously. Depending on the severity of the breach, consequences may range from a warning to termination of employment.

Any breach of, or non-compliance with this policy must be communicated to the Policy owner as soon as reasonably practical. The Policy owner, with input from key stakeholders, will consider the appropriate action(s) required. All instances of non-compliance with this policy will be included within the regular risk and compliance reporting processes and reported to the relevant board committee.



[www.discovery.co.za](http://www.discovery.co.za)

Discovery Ltd is the licensed controlling company of the designated Discovery Insurance Group. Registration number: 1999/007789/06. Companies in the Group are licensed insurers and authorised financial services providers.

