"Z7"

EOH

EOH Enterprise Risk Management Implementation Guideline

EOH 000 GRC GDL 04

Contents

EOH Enterprise Risk Management Implementation Guideline

EOH 000 GRC GDL 04

1. Introduction

The EOH Enterprise Risk Management (ERM) Implementation Guideline supports the implementation of the EOH ERM Policy.

Effective management of risk is central to the success of EOH. EOH philosophies form the foundation of the EOH ERM objective set. The deployment of the ERM policy is based on a multi-layer responsibility level of responsibility within EOH. The EOH ERM program has distinct structures with defined roles and responsibilities for the centre, division, cluster and business unit.

EOH's ERM Implementation philosophy is

- Best People
- Partner for Life
- Right First Time
- Sustainable Transformation
- Lead and Grow

EOH ERM is a collaborated endeavour to identify risks and to put in place actions, processes and / or measures to mitigate the probability of such risks materialising.

EOH ERM system is sponsored by the EOH Board, EOH Risk Committee and EOH EXCO.

2. Risk Management Policy

EOH's risk management policy is to ensure the consistent application of the ERM framework, ensuring a standardised, consolidated and transparent ERM System Framework, approach and process for organisational Enterprise Risk Management to ensure the management of all types of risks across EOH.

The core objectives of EOH's risk policy are:

1. To protect shareholder value by understanding and minimising the impact of uncertain future events;
2. To maintain EOH Group ERM framework;
3. To provide an information platform for more effective Group strategic and operational planning;
4. To enhance organisational resilience by maintaining an embedded enterprise risk management culture;
5. To provide an information system to deal more effectively with potential business disruptions thereby minimising the financial impact on the organisation; and
6. To provide a structure and systematic process to learn from loss events and to put the necessary controls in place to prevent the recurrence of such incidents.

3. Implementation of Risk Policy

EOH will adopt a structured approach to risk management to ensure a consistent approach to the assessment and treatment of all types of risk, at all levels, and for all significant activities throughout the organisation.

Enterprise Risk Management (ERM) needs to be embedded into all of EOH's critical business processes to prevent an event that might affect EOH achieving its objectives. To achieve this, risks will be identified and managed in a consistent, proactive manner. Similarly, after an event has occurred, EOH will use systematic processes to learn from such occurrences and put the necessary preventative measures in place to prevent the recurrence of such incidents. In this way EOH will drive towards Right 1st Time operational excellence.

ERM is the responsibility of line management in all of EOH's Business Units, Clusters, Divisions and at Group level. Those responsible for the management of risks are also accountable for ensuring that the necessary measures to mitigate remain in place and are effective.

Good corporate governance will be achieved through the regular review, measurement, reporting and communication of risks.

EOH's EXCO will monitor and review the organisation's risk management framework ensuring compliance with applicable standards and best practice and report its findings to the EOH Risk Committee and EOH Board on a regular basis.

4. Purpose of the ERM Implementation Guideline

This guideline directs EOH management and staff regarding the principles and minimum requirements of the ERM system and is aligned to the organisational obligations as set out in the Companies Act and recommendations of King III on ERM.

EOH ERM will consistently apply the EOH ERM framework for the management of all types of risks across EOH within the Risk Tolerance levels of the organisation. This amount is set at 10% of net profit after tax.

5. EOH ERM Principles

The EOH ERM principles are:

- A clear mandate and obligation regarding ERM and ensuring management accountability for risk management.
- An overarching set of ERM standards that set the performance requirements for risk management throughout EOH.
- Supporting guidelines that provide a consistent, generic tool kit of best practice methods to satisfy the requirements of the EOH ERM standards.
- A common approach to risk analysis and risk prioritisation.
- A common language for risk management.
- The use of one risk management information system, BarnOwl to support and drive consistency.

- Enterprise-wide requirements to gather and report risk information for governance purposes.
- An active program to share good risk management practice and learn.
- EOH businesses are accountable for the implementation of the risk management policy and standards and are required to create and maintain risk management plans to ensure compliance

6. EOH ERM Framework

The EOH ERM Framework seeks to position the operational risk identification and response program with the right focus, at the right level, namely:

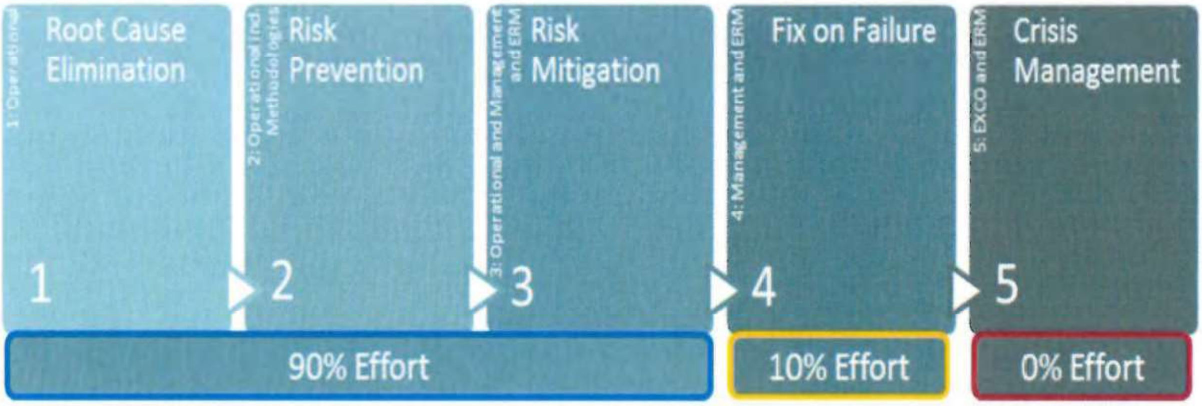


Fig 01: EOH ERM Framework

The core of the process is an ongoing and systematic, business-wide risk assessment process which supports EOH's ERM philosophy. This ensures that risks and opportunities are not only adequately identified, evaluated and managed at the appropriate level in each division, but also that their individual and joint impact on EOH as a whole is taken into consideration.

The EOH ERM process is divided in two streams, namely the 'strategic process' and the 'tactical process'. The strategic process is about policy, overall communication, overall roles and responsibilities and the measurement and review of the program, whereas the tactical process is about the actual identification, registration and treatment of risks.

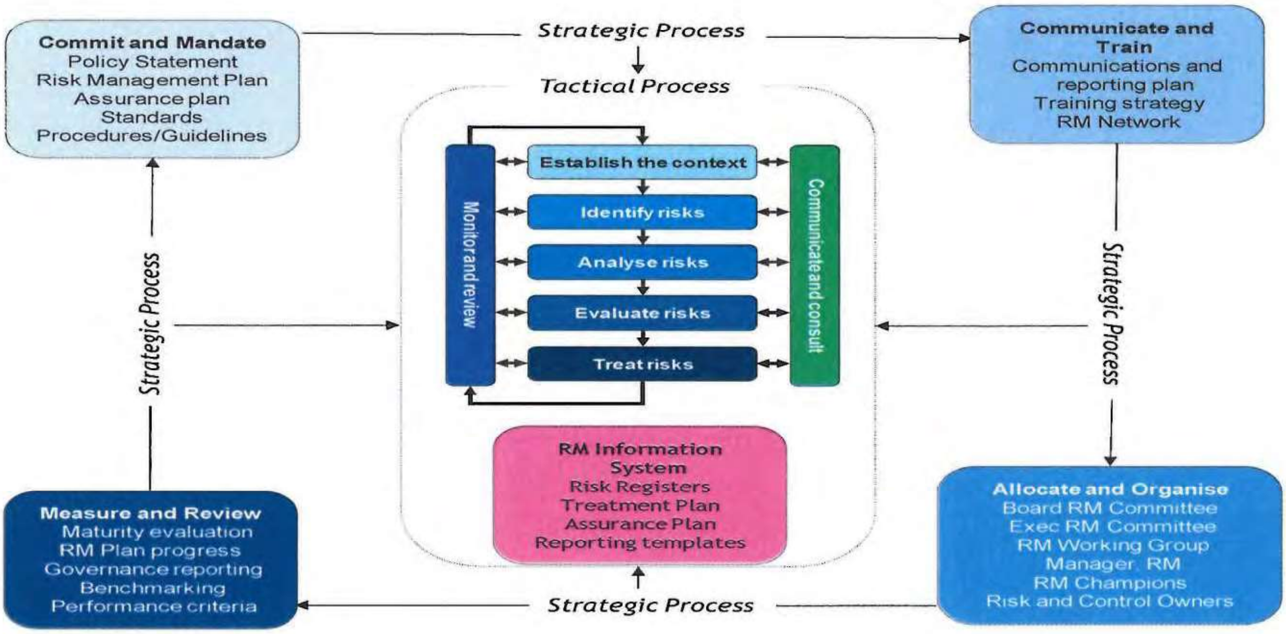


Fig 02: EOH ERM Process

Operational Business Unit Managers, as well as the Group IT, Finance, Strategic Sales and HR functions carry out regular self-assessments of risk. This process identifies critical business strategic, commercial, operational, and financial and compliance exposures facing the group and the adequacy and effectiveness of control factors at all levels. The assessment methodology takes into account the severity and probability of occurrence and applies a rating based on the quality of control, thereby ranking risks and setting priorities. The top risks, elevated at group level, are addressed through action plans put in place with responsibilities assigned to the appropriate people.

The tactical process can be further explained as follows:

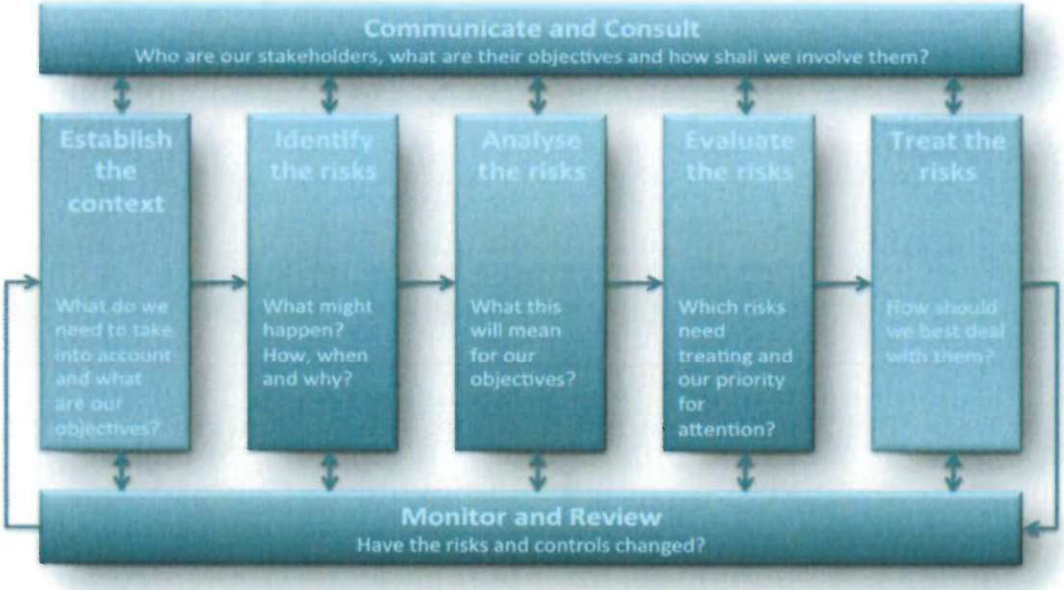

Communicate and Consult
Who are our stakeholders, what are their objectives and how shall we involve them?
Establish the context
What do we need to take into account and what are our objectives?
Identify the risks
What might happen? How, when and why?
Analyse the risks
What this will mean for our objectives?
Evaluate the risks
Which risks need treating and our priority for attention?
Treat the risks
How should we best deal with them?
Monitor and Review
Have the risks and controls changed?

Fig 03: EOH ERM - Tactical Process

The EOH Risk Officer oversees the process from the perspective of strategic direction, ongoing improvement in methodology and process.

By integrating the risk management process with EOH's strategic direction, the risk-return trade-off is optimised. This enhances competitive advantage, growth and the employment of capital.

The ERM Framework supports the EOH Board Risk Committee in a resultant 3 Line defence strategy:

First line – Divisional Management (levels 1-3)

The Group's first line of defense is the senior executives and business unit managers who are directly responsible for EOH's business operations. They are accountable for:

- Managing the day-to-day risk exposures by applying appropriate procedures, internal controls and Group policies;
- The effectiveness of risk management and risk outcomes;
- Allocating resources to execute risk management activities;
- Tracking risk events and losses;
- Identifying occurrences and implementing remedial actions to address these occurrences; and
- Reporting and escalating material risks and issues to the Chief Risk Officer and Risk Committee.

Second line – Group Risk function (level 3-4)

The Chief Risk Officer is a member of the EOH Executive Committee and is accountable for the effectiveness of the risk management function. The Chief Risk Officer reports to the Group CEO and has direct and unrestricted access to the Risk Committee Chairman. The Chief Risk Officer is responsible for developing Group-wide risk management policies, overseeing their implementation and reporting on risk issues to the EOH Executive Committee.

Third line – Assurance (level 4-5)

The third line of defense comprises the Group's independent assurance functions that provide an independent and balanced view of all aspects of risk management (both first and second line of defense) across the Group to the various governance bodies within the Group.

7. EOH ERM System

The EOH ERM System (Annexure 1) clarifies the risk terminology used and BarnOwl system process to be followed in support of the ERM Framework.

The summarised EOH ERM System process is explained in the EOH ERM Dictionary. The EOH ERM Dictionary is aligned to the EOH ERM BarnOwl system requirements and risk management best practice.

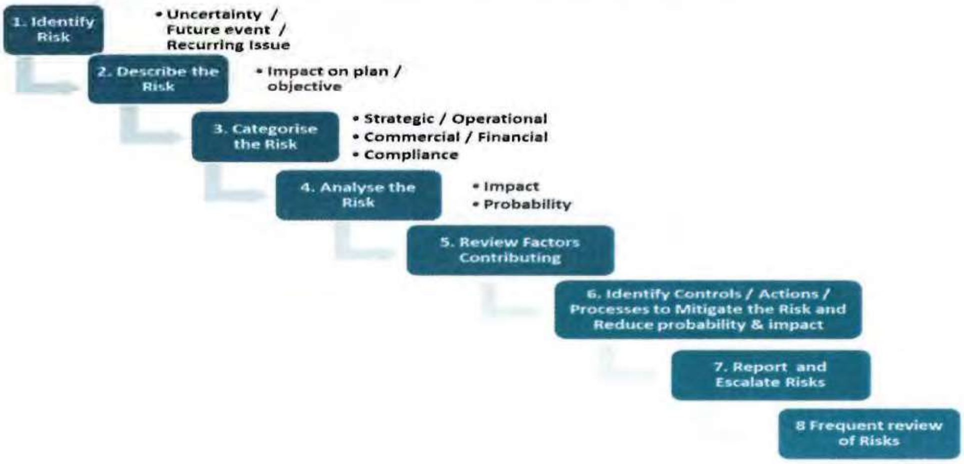
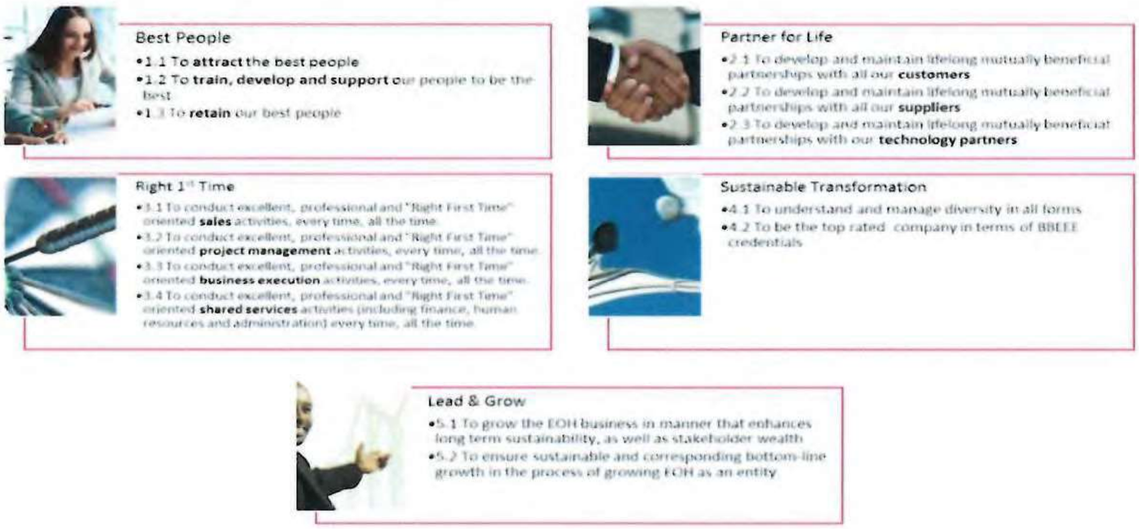

1. Identify Risk
• Uncertainty / Future event / Recurring Issue
2. Describe the Risk
• Impact on plan / objective
3. Categorise the Risk
• Strategic / Operational
• Commercial / Financial
• Compliance
4. Analyse the Risk
• Impact
• Probability
5. Review Factors Contributing
6. Identify Controls / Actions / Processes to Mitigate the Risk and Reduce probability & impact
7. Report and Escalate Risks
8 Frequent review of Risks

Fig 04: EOH ERM System Process

EOH implemented the integrated BarnOwl ERM system in 2012. The BarnOwl System is the reporting portal of choice for EOH ERM for the EOH Board Risk Committee, EOH Executive Committee and EOH Divisional Exco's in support of the Integrated Annual Reporting requirements.

8. EOH ERM Risk Model and Risk Categories

The ERM Risk Model has its foundation in the following risk objectives based on the EOH Philosophies.



Best People

- 1.1 To **attract** the best people
- 1.2 To **train, develop and support** our people to be the best
- 1.3 To **retain** our best people

Partner for Life

- 2.1 To develop and maintain lifelong mutually beneficial partnerships with all our **customers**
- 2.2 To develop and maintain lifelong mutually beneficial partnerships with all our **suppliers**
- 2.3 To develop and maintain lifelong mutually beneficial partnerships with our **technology partners**

Right 1st Time

- 3.1 To conduct excellent, professional and "Right First Time" oriented **sales** activities, every time, all the time
- 3.2 To conduct excellent, professional and "Right First Time" oriented **project management** activities, every time, all the time
- 3.3 To conduct excellent, professional and "Right First Time" oriented **business execution** activities, every time, all the time
- 3.4 To conduct excellent, professional and "Right First Time" oriented **shared services** activities (including finance, human resources and administration) every time, all the time

Sustainable Transformation

- 4.1 To understand and manage diversity in all forms
- 4.2 To be the top rated company in terms of BBEEE credentials

Lead & Grow

- 5.1 To grow the EOH business in manner that enhances long term sustainability, as well as stakeholder wealth
- 5.2 To ensure sustainable and corresponding bottom-line growth in the process of growing EOH as an entity

Fig 05: EOH Risk Objectives

The EOH ERM risk model is based on ERM best practice and focuses on strategic risk categories and sub-categories. The EOH ERM risk analysis framework supports the organisational decision making responsibilities and control ownership.

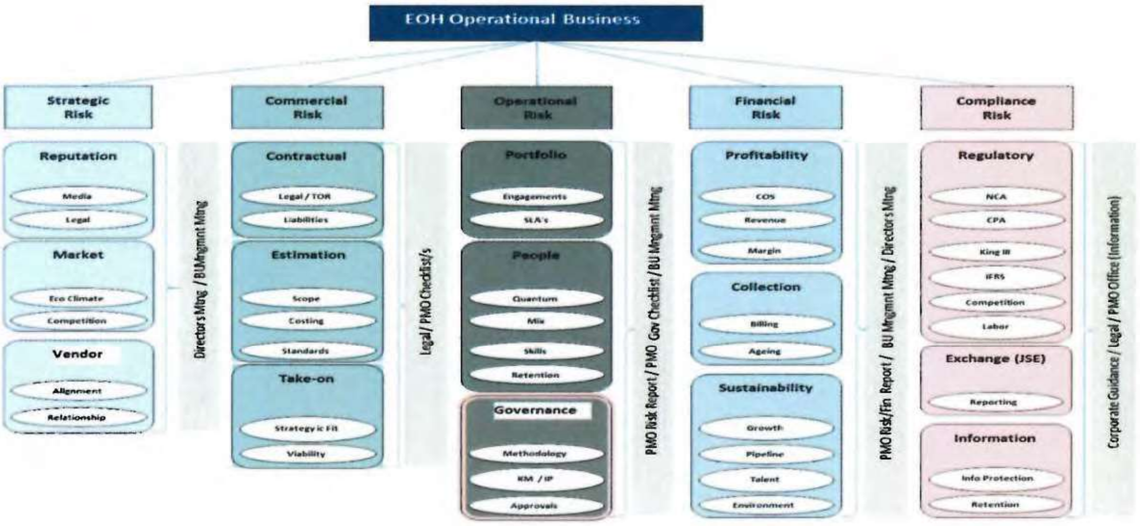
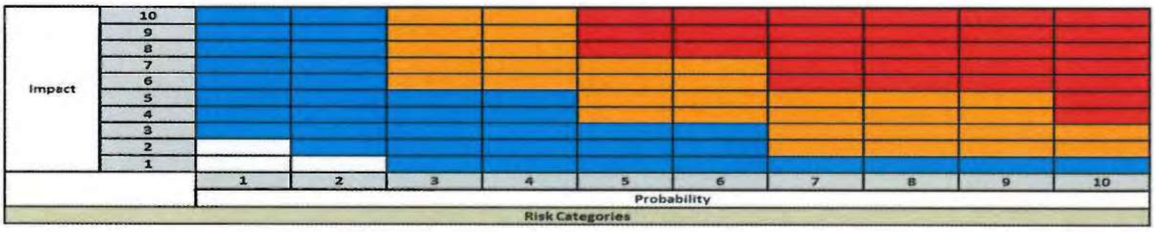


Fig 06: EOH Risk Categories

The EOH Risk Assessment Matrix is based on a Risk factor calculation using a scoring model for Probability (Likelihood) and Impact (Severity), from low to high, where low is 1 and high is 10.



Risk Factor = Probability X Impact

Risk Factor	Factor	Probability translated to Impact
Almost Certain - Very High	Calculated	A disaster with the potential to severely impact the business and is fundamental to the achievement of objectives. Likely monetary value in excess of R20 million.
Highly Likely - High	Calculated	Critical event which can be endured but which may have a prolonged negative impact and extensive consequences. Monetary impact R15 to R20 million.
Possible - Medium	Calculated	Major event which can be managed but requires additional resources and management effort. Monetary impact R10 to R15 million.
Unlikely - Low	Calculated	Event, which can be managed under normal operating conditions. Consequences can be readily absorbed under normal operating conditions. Monetary impact between R5 to R10 million.

Fig 07: EOH Risk Assessment Matrix

9. EOH ERM Structures

The EOH ERM structure implemented is based on a multi-layered ERM responsibility and communication level within EOH.

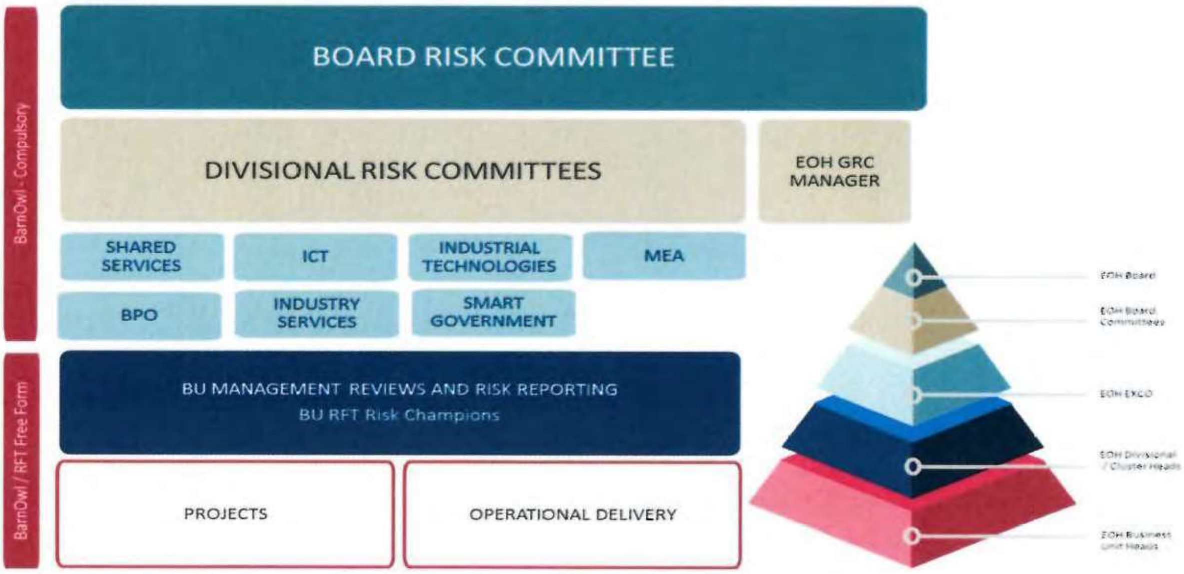


Fig 08: EOH ERM Structure

The ERM structure supports the Divisional (incl. Cluster and BU) operational obligation to form their own risk structures to identify and evaluate risks as well as to implement measures to mitigate risks.

The Divisional ERM Risk Committees will be responsible for evaluating the risks within the Division and consolidating the evaluated risks into the Divisional Risk report for incorporation and / or escalation to the EOH Executive Committee and /or the EOH Risk Committee for further mitigation action and response.

The following information must be captured in a Risk Register (BarnOwl preferred choice):

- Risk Date (registered / aware of since)
- Risk Objective
- Risk Description
- Risk Category
- Risk Impact Score
- Risk Probability Score
- Risk Mitigation Strategy (Treat, Tolerate, Terminate)
- Risk Mitigation Owner
- Risk Mitigation Plan (High – level)
- Risk Mitigation Target Date

10. EOH ERM Roles and Responsibility Matrix and Mandates

The EOH ERM responsibility matrix (fig 5), using the RACI approach, will be applied.

Description	Board Risk Committee	EOH Risk Committee	EOH Executive Committee	EOH Divisional	EOH BU's	EOH Risk Office
ERM Structure and Program incl. Policy and Standards	I	A	R	I	I	C / I
Annual ERM Plan	I	I	A	I	I	R
ERM System Administration	I	I	A	C	C	R
ERM System Capturing Group Registers	I	I	A	C	C	R
ERM System Capturing Divisional (incl. Cluster and BU) Registers	I	I	A	R	R	C / I
ERM Group Reporting	I	A	R	C	C	R
ERM Divisional Reporting	I	I	A	R	R	C / I
Responsible, Accountable, Consulted and Informed						

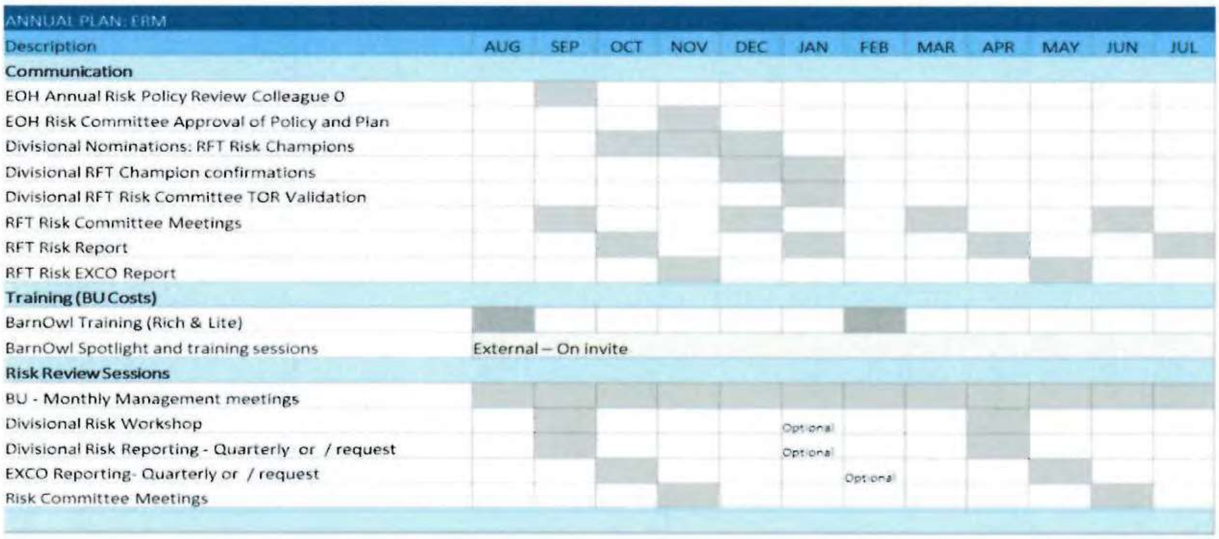
Fig 09: EOH ERM Responsibility Matrix

11. EOH ERM Controls and Reporting

The EOH Committee Structure and the EOH ERM Annual Plan refers to the reporting requirements and frequency of such meetings and / or reports. The summarised EOH ERM Plan will be endorsed by the EOH EXCO and published annually.

12. EOH ERM Annual Plan

The EOH ERM Annual Plan includes the following activities:



ANNUAL PLAN: ERM

Description	AUG	SEP	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL
Communication												
EOH Annual Risk Policy Review Colleague O		▨										
EOH Risk Committee Approval of Policy and Plan				▨								
Divisional Nominations: RFT Risk Champions			▨	▨	▨							
Divisional RFT Champion confirmations					▨	▨						
Divisional RFT Risk Committee TOR Validation						▨						
RFT Risk Committee Meetings		▨			▨			▨			▨	
RFT Risk Report			▨			▨			▨			▨
RFT Risk EXCO Report				▨						▨		
Training (BU Costs)												
BarnOwl Training (Rich & Lite)	▨						▨					
BarnOwl Spotlight and training sessions	External – On invite											
Risk Review Sessions												
BU - Monthly Management meetings	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Divisional Risk Workshop		▨				Optional			▨			
Divisional Risk Reporting - Quarterly or / request		▨				Optional			▨			
EXCO Reporting- Quarterly or / request			▨				Optional			▨		
Risk Committee Meetings				▨							▨	

13. EOH ERM System Support and Change Management

System Administration and Change Management is the responsibility of EOH GRC Manager supported by the EOH Divisional RFT Directors and EOH IMS. All change requests will be logged through the EOH Helpdesk (help365@eoh.co.za) and assigned for support.

Any BarnOwl license holder / user must be a full time employee of EOH and registered on the EOH domain.

The EOH BarnOwl system security is based on Active Directory login and full transactional history. The system back-up is part of the EOH Corporate Back-Up schedule.

14. Implementation Guideline Approval

This Implementation Guideline is approved on signature date and effective immediately from signature date.

EOH Chief Risk Officer

2016.06.22

Date