Global Health Limited

RISK MANAGEMENT (ERM) POLICY

Type: Governance Document / BOD / CS	Version: 001
Effective Date: 10th September 2021	Last Review: NA
Classification : Non-Confidential / Web	Review Schedule: Annual

PURPOSE

This document sets out the organisation's Risk Management Policy to be read together with Company`s Internal Risk Management Policy and includes:

The *objectives* of our Risk Management arrangements;

***Definitions* of relevant terms;**

***Risk management principles*;**

Relative *responsibilities*;

The Organisation's *'Risk Tolerance'*;

The *Risk Framework* and how it will work; and

How Risk Management contributes to providing an *Assurance*.

The Board of Directors (the "Board") of **Global Health Limited** has approved this Risk Management Policy after due consultations with the Senior Management Team of the Company and has made the policy consistent with the requirements of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, as amended (the "Listing Regulations"). This policy will come into force with effect from [ ].

Risk Management in the organisation provides a framework to identify, assess and manage potential risks and opportunities. It provides a way for managers to make informed management decisions.

Businesses operate in a dynamic environment. Changes in government policies, legislation, information technology, customer preferences, competitors' initiatives, financial markets, etc. all contribute to this ever changing environment, a situation demanding a mechanism to proactively assess risks and design controls to mitigate those risks. Effective Risk Management ensures sustenance of the organisation and everyone associated with the Organisation. To ensure a widespread understanding, Board members and all operational /

business unit managers should be familiar with, and all staff aware of, the principles set out in this document.

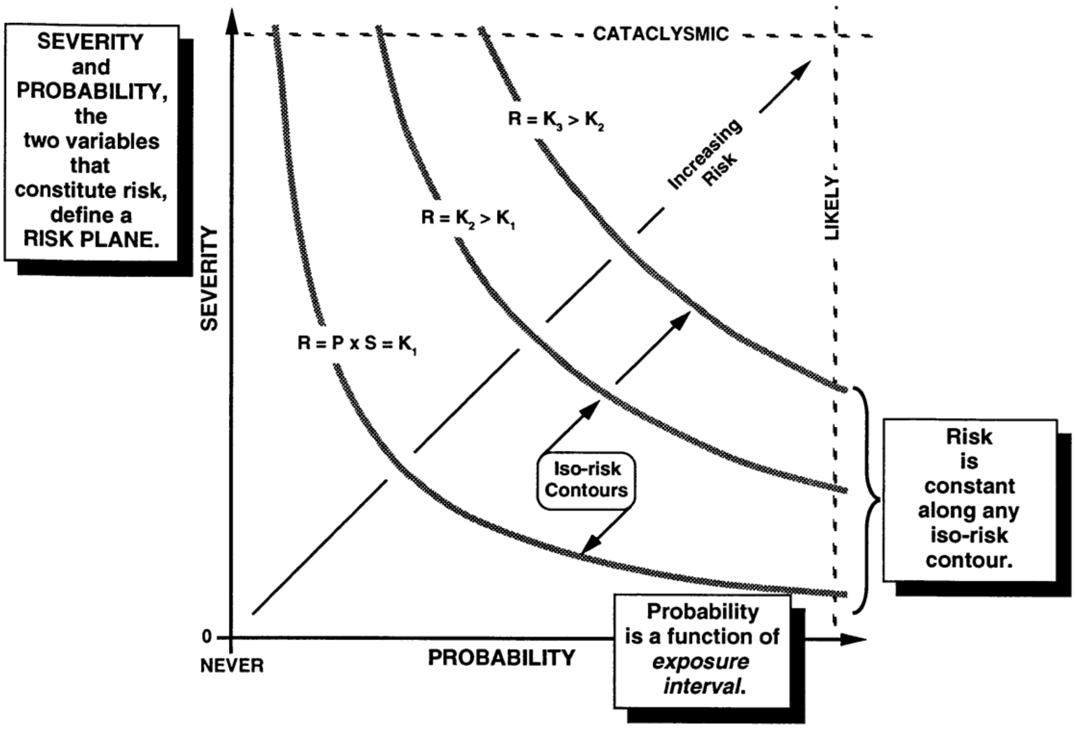
Risk Management Objectives

The objective of this organisation's Risk Management arrangements is to help managers make informed choices which:

- Improve business performance by informing and improving decision making and planning;

- Promote a more innovative, less risk averse culture in which the taking of calculated risks in pursuit of opportunities to benefit the organisation is encouraged;

- Provide a sound basis for integrated risk management and internal control as components of good corporate governance.


SEVERITY and PROBABILITY, the two variables that constitute risk, define a RISK PLANE.
SEVERITY
CATACLYSMIC
LIKELY
R = K3 > K2
R = K2 > K1
R = P x S = K1
Increasing Risk
Iso-risk Contours
Risk is constant along any iso-risk contour.
0
NEVER
PROBABILITY
Probability is a function of exposure interval.

The improvements and benefits, which effective Risk Management should provide are:

- An increased likelihood of achieving the organisation's aims, objectives and priorities;

- Prioritising the allocation of resources;

- Giving an early warning of potential problems; and

- Providing everyone with the skills to be confident risk takers.

Effective risk assessment can be achieved by considering:

- Risk management ownership and accountability
- Risks related to strategic, economic, financial, market, legal and regulatory, human resources, political, environmental, IT and systems, operations
- Defined and communicated risk tolerance profile
- Root cause analysis and risk brainstorming sessions
- Quantitative and/or qualitative risk measurement
- Risk assessment methodology
- Risk action plan
- Timely reassessment

Definitions

The organisation's Risk Management Policy is framed around a common understanding of what *Risks - Corporate Risk (Strategic and Residual Risk), Operational Risk (specific Business and Functional risks including Economic, Market, Financial, Human resources, Legal and Compliance, etc. Risks)* AND *Risk Management are*. These are set out in **Appendix - A**.

Risk Management Principles

The principles contained in this policy and strategy will be applied at both corporate and operational levels within the organisation.

The organisation's **Risk Management Policy and Strategy** will be applied to all operational aspects of the Organisation and will consider external strategic risks arising from or related to various statutory and regulatory non-compliance risks, as well as wholly internal risks.

Other Corporates and outside agencies are devising and implementing Risk Management Strategies. Our organisation may impinge on their risk profile.

Our positive approach to risk management means that we will not only look at the risk of things going wrong, but also the impact of not taking opportunities or not capitalising on corporate strengths.

General Principles

a. All risk management activity will be aligned to corporate aims, objectives and organisational priorities, and aims to protect and enhance the reputation and standing of the organisation.

b. Risk analysis will form part of organisational strategic planning, business planning and investment/project appraisal procedures.

c. Risk management will be founded on a risk-based approach to internal control, which is embedded in day-to-day operations of the organisation.

d. Our risk management approach will inform and direct our work to gain an assurance on the reliability of organisational systems and will form the key means by which the Board gains its direct assurance (Management Evaluation of Internal Controls Document).

e. Managers and staff at all levels will have a responsibility to identify, evaluate and manage or report risks, and will be equipped to do so.

f. We will foster a culture, which provides for spreading best practice, lessons learnt and expertise acquired from our risk management activities across the organisation for the benefit of the entire organisation.

Principles for Managing Specific Risks

Risk Management in the organisation should be proactive and reasoned. Corporate and operational risks should be identified, objectively assessed and where this is the appropriate response, actively managed.

The aim is to anticipate, and where possible, avoid risks rather than dealing with their consequences. However, for some key areas where the likelihood of a risk occurring is relatively small, but the impact on the organisation is high, we may cover that risk by developing Contingency Plans, eg. Disaster Recovery/Business Continuity Plans. This will allow us to contain the negative effect of unlikely events, which might occur.

In determining an appropriate response, the cost of control / risk management, and the impact of risks occurring will be balanced with the benefits of reducing risk. This means that we will not necessarily set up and monitor controls to counter risks where the cost and effort are disproportionate to the impact or expected benefits.

We also recognise that some risks can be managed by transferring them to a third party, for example by contracting out, hedging or by insurance.

Responsibilities

All personnel have a responsibility for maintaining strong internal controls and managing risk in order to achieve personal, team and corporate objectives. Collectively, staff in business units needs the appropriate knowledge, skills, information and authority to establish, operate and monitor the system of internal control. This requires an understanding of the organisation, its objectives, the risks it faces and the people we deal with. Everyone should be aware of the risks they are empowered to take, which should be avoided and which should be reported upwards the organisation reporting levels.

The responsibilities of the Directors on the Board, Chief Executive and the Senior Management Personnel; Operational/Business Unit Managers; the Audit Committee; and Specialist Central Functions are set out in **Appendix B.**

Risk Tolerance

The Directors, Chief Executive and the Board encourage the taking of controlled risks, the grasping of new opportunities and the use of innovative approaches to further the interests of the organisation and achieve its objectives provided the resultant exposures are within *the organisation's risk tolerance range.*

The organisation's Risk Tolerance can be defined by reference to the following components.

Acceptable risks

All personnel should be willing and able to take calculated risks to achieve their own and the organisation's objectives and to benefit the organisation. The associated risks of proposed actions and decisions should be properly identified, evaluated and managed to ensure that exposures are acceptable.

Within the organisation, particular care is needed in taking any action, which could:

- Impact the reputation of the organisation;
- Impact performance;
- Undermine the independent and objective review of activities;
- Result in censure/fine by regulatory bodies; or
- Result in financial loss.

Any threat or opportunity which has a sizeable potential impact on any of the above should be examined, its exposures defined and it should be discussed with the appropriate line manager. Where there is significant potential impact and high likelihood of occurrence it should be referred to the Director's Board as a corporate risk.

Prohibited Risk Areas

Organisational policies and guidance manuals define where there are mandatory processes and procedures (both regulatory and internal). Full compliance with these standards is required and confirmation of compliance will be sought in the annual Certificates of Assurance process. Non-compliance with prescribed procedures constitutes an unacceptable risk.

Some risks are acceptable provided the prescribed organisational process is followed, e.g. approved Budgets (Capex and Revex), Organisation structuring (manning) and Designated responsibilities / authorities (Job responsibilities / Limits Of Authority) are adhered to.

A Risk Framework Document specifying the principles governing the relationship between Corporate, Divisional and the Area Offices business wise should be established and the Area managers may take risk management decisions on the basis of their delegated financial authority and devolved responsibilities set out in such Framework Document.

Risk Framework

The Company will maintain a current '***Corporate Risk Profile***' and an '***Operational Risk Profile***' as basis for implementing and monitoring the risk management activities. This framework will include detail of the ***Impact and Likelihood*** of each of the risk identified, indicate ***Ownership / Responsibility*** and specify an ***Action Plan*** for treatment. This will be reviewed and updated regularly. Progress of the risk management programme will be reviewed by the Board, periodically.

The corporate and operational risk will be assessed along the profile matrix of business, finance, functional, IT risks. Please refer **Appendix C.**

To help to meet their responsibilities to identify, evaluate and manage operational risks, Divisional Heads and Business Unit Managers are asked by the Board to maintain:

- A Divisional Risk profile which details the priority (impact and likelihood) and ownership within the Division;
- A Risk Management Action Plan;
- Evidence, e.g. Minutes of regular review and monitoring of the profile and action plan.

Assurance

The use of this risk management approach should help in identifying aspects for detailed review within the Area (for example using Control & Risk Self-Assessment) and inform and support the Divisions and Corporate, vide periodic (say half yearly or annual) Certificate of Assurance.

The Corporate Risk Profile document will inform the Head of Internal Audit and the designated Officer for Compliance of Corporate governance of the work necessary to provide the annual assurance to the Board. For the corporate risks identified by the Board, the internal audit and the management will evaluate the effectiveness of the existing controls and risk management responses. The assurance will include an assessment of the reliability and effectiveness of the organisation's overall Risk Management arrangements.

Appendix A

DEFINITIONS

RISK MANAGEMENT is the culture, processes and structure that are directed towards the effective management of potential opportunities and threats to the organisation and its contribution to the stakeholders and public at large.

RISK is an event that could

- Have an impact by not taking opportunities or not capitalising on corporate strengths,
- Prevent, hinder or fail to further the achievement of objectives,
- Cause financial disadvantage, i.e. additional costs or loss of money or assets; or
- Result in damage to or loss of an opportunity to enhance the organisation's reputation.

CORPORATE RISK is a risk requiring reference to and monitoring by the Director's Board, i.e. those risks assessed as having a high impact on the business of the organisation re: strategic decisions setting business directions, funding and investments such as in new project, capex, information technology and systems; corporate policies such as HR policy, Delegated Limits of authority, organisation structure, IT and security policies; business continuity plan and disaster recovery procedures, etc. and Residual operational risks

OPERATIONAL RISK is any risk requiring resolution in operations of the organisation, i.e. risks associated with the management of business and functional risks by individual divisions / units and categorised as having high, medium or low impact on the business.

The key elements in the operational risk management process include:

- Appropriate policies and procedures;
- Efforts to identify and measure operational risk;
- Effective monitoring and reporting;
- A sound system of internal controls; and
- Appropriate testing and verification of the operational risk framework.

Appendix B

CORPORATE RISK MANAGEMENT RESPONSIBILITIES

The Risk Management Committee: is a committee constituted by the Board in accordance with the Companies Act, 2013 and the Listing Regulations**.** The committee will co-ordinate with all departmental heads in identifying the risks, its mitigations and reporting to Board and its **scope would *inter-alia* be as under:**

a. To formulate a detailed risk management policy which shall include:

    (i) A framework for identification of internal and external risks specifically faced by the Company, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the risk management committee;

    (ii) Measures for risk mitigation including systems and processes for internal control of identified risks; and

    (iii) Business continuity plan.

b. To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;

c. To monitor and oversee implementation of the risk management policy of the Company, including evaluating the adequacy of risk management systems;

d. To periodically review the risk management policy of the Company, at least once in two years, including by considering the changing industry dynamics and evolving complexity;

e. To keep the Board informed about the nature and content of its discussions, recommendations and actions to be taken;

f. To set out risk assessment and minimization procedures and the procedures to inform the Board of the same;

g. To review the status of the compliance and undertake regulatory reviews and business practice reviews;

h. To review and recommend the Company's potential risk involved in any new business plans and processes;

i. To review the appointment, removal and terms of remuneration of the chief risk officer, if any; and

j. To perform such other activities as may be delegated by the Board and/or prescribed under any law to be attended to by the Risk Management Committee.

The Risk Management Committee shall coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the Board.

The Risk Management Committee shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.

The Division/Functional Heads of the Senior Management will assume ownership for managing specific business, technological and other operational risks in their area and co-ordinate with Risk Management Committee on same.

Operational/Business Unit Managers (Business Managers /Plant Heads) – are responsible for ensuring compliance with the prescribed procedures set out in organisational policies. They have a responsibility to identify, evaluate and manage operational risks and bring to the attention of the Risk Management Committee. Business unit managers are ideally placed to pick up on those early warning indicators, which might identify where problems are developing and this is an important responsibility.

Operational managers should ensure that everyone in their unit understands their risk management responsibilities and must make clear the extent to which staff is empowered to take risks.

Corporate Functions – Internal Audit (and Control Assurance), Corporate Finance and Taxation, Corporate HR, Secretarial, Legal, IT, and Other Corporate functions will assist operational managers by providing advice and support in relation to their area of specialisation.