RISK MANAGEMENT POLICY

Contents

1. Introduction

Risk is an inherent aspect of the dynamic business environment. Risk is the probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action.

2. Purpose of the Policy

All activities undertaken by SeQuent Scientific Limited ('**SSL'**) carry an element of risk. The exposure to these risks is managed through the practice of Risk Management. In managing risk, it is the Company's practice to take advantage of potential opportunities while managing potential adverse effects. Managing risk is the responsibility of everyone in the Company.

This policy outlines the Company's risk management process and sets out the responsibilities of the Board, the Risk Management Committee, the Managing Director, Senior Management and others within the Company in relation to risk management.

This policy applies to all employees of Company and its Subsidiaries.

The Policy is formulated in compliance with Regulation 17(9)(b) read with Regulation 21 of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("the LODR Regulations") and Section 134 of the Companies Act, 2013 ("the Act"), which requires the Company to lay down procedures about risk assessment and risk minimization.

The terms used in this Policy will have the meaning ascribed to it under the Companies Act, 2013 or the Listing Regulations, as may be amended from time to time.

3. Understanding Risk Management

Risks have been described in terms of combination of the consequences of an event occurring and its likelihood of occurring.

Risk is the chance of something happening that will have an impact on objectives of the Company. Risk management can be described as the culture, processes and structures that are directed towards realising potential opportunities whilst managing an adverse effect.

SSL's risk management system is designed to identify the risks it faces and has measures in place to keep those risks to an acceptable minimum. The existence of risk presents both threats and opportunities to SSL.

The Company's risk management program comprises of a series of processes, structures and guidelines which assist the Company to identify, assess, monitor and manage its business risk, including any material changes to its risk profile.

4. Responsibility

4.1 Board

The Board of Directors of SSL, through the Risk Management Committee, has responsibility to review and report that:

(i) the Committee reviews the SSL's risk management framework to satisfy itself that it continues to be sound, and that SSL is operating with due regard to the risk appetite set by the Board, and effectively identifies all areas of potential risk;

(ii) adequate policies and processes have been designed and implemented to manage identified risks;

(iii) a regular program of audits is undertaken to test the adequacy of and compliance with prescribed policies; and

(iv) proper remedial action is undertaken to redress areas of weakness.

4.2 Risk Management Committee

The Risk Management Committee, has responsibility under its Charter:

(i) To formulate a detailed risk management policy which shall include:

(a) 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 Committee.
(b) Measures for risk mitigation including systems and processes for internal control of identified risks.
(c) Business continuity plan.

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

(iii) To monitor and oversee implementation of the risk management policy, including evaluating the inadequacy of risk management systems;

(iv) To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;

(v) To keep the Board of Directors informed about the nature and content of its discussions, recommendations and actions to be taken;

(vi) To review the appointment, removal and terms and conditions of the Chief Risk Officer (If any);

(vii) 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;

(viii) To co-ordinate 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 of Directors

4.3 Chief Financial Officer and Chief Risk Officer

The Chief Financial Officer and Chief Risk Officer of SSL has responsibility under this policy for:

(i) Monitoring compliance with this policy;
(ii) Reporting to the Board on compliance with this policy;
(iii) Developing, implementing and monitoring systems, management of policies and procedures relevant to the business, including facilitating review by the executive on a regular basis; and
(iv) Maintaining the risk register.

4.4 General Responsibilities

The Company's Senior Management is responsible for designing and implementing risk management and internal control systems which identify material risks for the Company and aim to provide the Company with warnings of risks before they escalate. Senior Management must implement the action plans developed to address material business risks across the Company and individual business units.

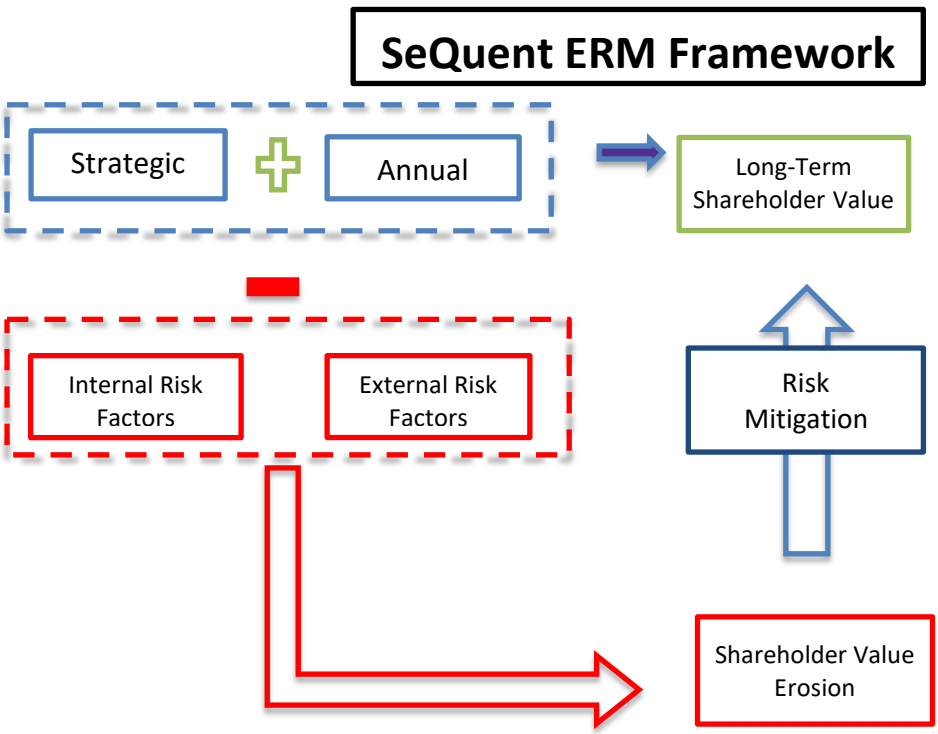
Senior Management should regularly monitor and evaluate the effectiveness of the action plans and the performance of employees in implementing the action plans, as appropriate. In addition, Senior Management should promote and monitor the culture of risk management within the Company and compliance with the internal risk control systems and processes by employees. Senior Management should report regularly to the Risk Management Committee regarding the status and effectiveness of the risk management program.

4.5 Employees

All employees are responsible for implementing, managing and monitoring action plans with respect to material business risks, as appropriate.

5. Risk Management Procedure

5.1 Summary of Procedure



5.2 Risk Management Process

The risk management system is dynamic and is designed to adapt to SSL's developments and any changes in the risk profile over time. Compliance measures are used as a tool to address identified risks.

The risk management system is based on a structured and systemic process which takes into account SSL's internal and external risks.

The main elements of the risk management process are as follows:

Step 1: Establish Context

- Business Objectives in Long-Term & Annual Plan with Road Map to achieve the same
- ESG Objectives
- Assumption

Step 2: Identify Risks

- List of Risks

The Risk Management Committee has identified the following types of material risks:

i) Structural Risk
ii) Operational Risk
iii) Regulatory & Compliance Risk
iv) EHS Risk
v) Credit Risk
vi) Liquidity Risk
vii) Market Risk

viii) Foreign Currency Risk

ix) Interest Rate Risk

x) Information Technology & Cyber Security Risk

xi) Reputational Risk

xii) Competition Risk

xiii) Fiduciary Risk

xiv) Fraud Risk

xv) IPR Risk

Step 3: Assess Risks

- Impact in value terms
- Likelihood
- Classification (High, Medium and Low)

Step 4: Evaluate & Mitigate

- Prioritize
- Mitigation Plan
- KPIs with Timelines
- Responsibilities & Internal monitoring

Step 5: Monitor, Review & Report

- Monitoring at Committee Level
- Continue with guidance on Way Forward

5.3 Risk Management Methodology

The methodology adopted by SSL for managing and treating its risks can be defined as follows:

1. Document a risk management framework (i.e. the context)
2. Identify the general activities involved in running the business (ie risk categories)
3. Identify the risks involved in undertaking the specific business activity by asking the questions:
   a) What could happen?
   b) How and why, it could happen?
4. Rate the likelihood of the business activity not being properly performed. Likelihood is assessed to the assumption that there are no existing risk management and compliance processes in place. It is assessed as either **Almost Certain**, **Likely**, **Possible**, **Unlikely** and **Rare**.
5. Rate the consequence of not properly performing the business activity - damage can be quantified in terms of financial loss to investors and/or SSL itself. It is assessed as **Catastrophic**, **Major**, **Severe**, **Serious and Minor**.
6. Assign the inherent risk rating based on a combination of the risk rating. Low and medium risks may be considered acceptable and therefore minimal further work on these risks may be required. The rating may be assessed as **Critical, High**, **Significant**, **Medium** and **Low**.
7. Decide whether a control (e.g. policy, procedure, checklist, reporting mechanism or account reconciliation) is necessary given the level of risk, based on likelihood and consequences and if so, identify control.
8. Assess whether the existing controls are adequate and allocate the responsibility of monitoring the control to treat the risk. This will integrate risk management and compliance to daily activities and facilitate appropriate control of operational risk.

9. Raise awareness about managing risks across the organisation through communicating the policy and responsibilities.
10. Routinely monitor and review ongoing risks so can risk can be effectively managed.

6. Limitation and Amendment

The Board of Directors may in their discretion and on recommendation of the Audit Committee, make any changes/modifications and/or amendments to this Policy from time to time.

In the event of any conflict between the provisions of this Policy and of the Act or LODR Regulations or any other statutory enactments, rules, the provisions of such Act or LODR Regulations or statutory enactments, rules shall prevail over and automatically be applicable to this Policy.