POWER ROOT BERHAD

Registration No.: 200601013517 (733268-U)

GROUP RISK MANAGEMENT FRAMEWORK

CONTENTS		PAGE

ABBREVIATIONS

AC	**The Audit Committee**
BOARD/ BOD	**The Board of Directors**
BURSA	**Bursa Malaysia Securities Berhad**
CEO	**Chief Executive Officer**
CA 2016	**The Company Act 2016 and amendments**
COSO ERM 2017	**Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management - Integrating with Strategy and Performance**
The Company	**Power Root Berhad**
The Group/ PRB Group	**Power Root Berhad and its Subsidiaries**
HOD	**Head of Departments/ Division**
IAD	**Internal Audit Department**
IRB	**Inland Revenue Board**
ISO	**International Organization for Standardization**
KRR	**Key Risk Registers**
KRP	**Key Risk Profile**
KSRO	**Co-Key Sustainability & Risk Officer**
MACC	**Malaysian Anti-Corruption Commission**
MFRS	**Malaysian Financial Reporting Standards**
PIC	**Person In-Charge**
SC	**Securities Commission**
SRMC	**Sustainability & Risk Management Committee**

Section 1

Risk Management Policy

INTRODUCTION

Power Root Berhad (hereinafter referred to as "the Company") and its subsidiaries (collectively referred to as "the Group" or "PRB Group") shall be guided by the policies and guidelines set out in this framework.

The Board's risk oversight role covers the following key areas, amongst others:

- Reviewing proposed strategy and risk appetite;
- Alignment of strategy and business objectives with the Group's mission, vision, and core values;
- Significant business decisions including mergers, acquisitions, divestments, capital expenditure allocations, funding, and dividend-related decisions;
- Responding to significant fluctuations in the Group's performance; and
- Communications with investors and stakeholder relations.

Enterprise Risk Management ("**ERM**") is defined as:

"The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value."

(Source: COSO ERM 2017)

The BOD takes into account risk considerations in its strategic planning process to achieve the corporate objectives as well as integrate enterprise risk management into the business processes throughout the Group as depicted in Table 1 below: -

Table 1 Risk & Strategy – extracted from COSO ERM 2017

The Group has established an ERM framework along the principles promulgated in the COSO ERM 2017. The Framework consists of the five interrelated components of enterprise risk management. Table 2 below illustrates these components and their relationship with the Group's mission, vision, and core values. The three ribbons in the diagram of Strategy and Objective-Setting, Performance, and Review and Revision represent the common processes that flow through the Group. The other two ribbons,

Governance and Culture, and Information, Communication, and Reporting, represent supporting aspects of enterprise risk management.

Table 2 ERM framework – COSO ERM 2017

1. Governance and Culture: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviours, and overall understanding about risk held by personnel within the entity.

2. Strategy and Objective-Setting: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

3. Performance: Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses (e.g. Acceptance, Avoidance, Pursuit, Mitigation & Sharing) and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.

4. Review and Revision: By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.

5. Information, Communication, and Reporting: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

The above five components are supported by a set of principles as per Table 3 below:

Table 3 - 5 components of ERM framework - COSO ERM 2017

In line with the ERM framework, the Group adopts a structured approach to the enterprise risk management for critical business management process, and is championed by the Company's BOD and include the involvement of all level of employees, as well as internal and external stakeholders. The structured approach serves to manage key risks within the Group's risk appetite and provide reasonable assurance to its achievement of the Group's strategic objectives, operational objectives, reporting objectives and compliance objectives.

- Strategic objectives – to provide reasonable assurance that Group's' mission, vision, core values, strategies and business objectives can be achieved. This is achieved via aligning and integrating corporate culture, capabilities, and practices of the Group with strategy setting and performance;
- Operational objectives – to provide reasonable assurance of the effective and efficient use of the Group's resources, including setting, measurement and assessment of operational and financial performance goals, and safeguard of assets;
- Reporting objectives- to provide reasonable assurance that the internal and external financial and non-financial reporting information is accurate and complete, timely, comprehensive for management decision making and in accordance with the rules and regulations promulgated by regulators, authorities, standards setting bodies and the Group's policies and procedures; and
- Compliance objectives – to provide reasonable assurance to the compliance with applicable laws and regulations.

1. PRINCIPLES

The Group's attitude to risk shall be based on the following key principles:

(a) **Philosophy**

The Group will take on a level of risk that is in line with its risk appetite. As profits result from successful risk-taking, the aim is to manage the key business risks appropriately rather than eliminate them at whatever cost. With a well-established risk management framework and effective risk management processes, the Group will be able to manage key business risks in the pursuit of its corporate objectives.

(b) **Culture**

The CEO champions the cause for effective risk management throughout the Group in order to achieve its risk management objectives. Risk management is not the sole responsibility of the CEO but rather the collective action by all the employees within the Group playing their part in ensuring the proper functioning of the risk management processes.

The BOD accepts that risk taking is part and parcel of managing and running the businesses it pursues and acknowledges that effective risk management is essential for the continuing success of the Group in achieving its corporate ambitions. Risks which may have a significant impact are promptly identified for timely action to minimise its impacts on the Group.

(c) **Education**

The CEO is committed to promoting a high level of risk awareness amongst all the employees in the management of the Group's business operations.

(d) **Risk Ownership**

The Board affirms its overall and ultimate responsibility for maintaining a sound risk management system in order for the Group to achieve its strategic objectives, operational objectives, reporting objectives and compliance objectives.

The Board delegates the duty of risk management to the SRMC. It is the duty of the SRMC to ensure that a sound risk management system is implemented across all level in the Group, to ensure all key business risks are promptly identified and managed.

The duty for managing risk at operational level lies with the relevant risk owners who are also responsible for carrying out an on-going process of identifying and assessment of risks, evaluating the adequacy and integrity of the controls and as well as formulating and implementing action plan(s) for mitigating the risks identified in line with the risk appetite of the Group.

(e) **Assurance**

The Board will seek to obtain independent assurance of the soundness of the risk management process through reporting on the review and assessment, findings and actions taken by the risk owners, Executive Directors, Internal Audit Function and the external auditors to confirm that the risk management and internal control system is operating effectively and in compliance with the Group's policies and all relevant regulatory requirements.

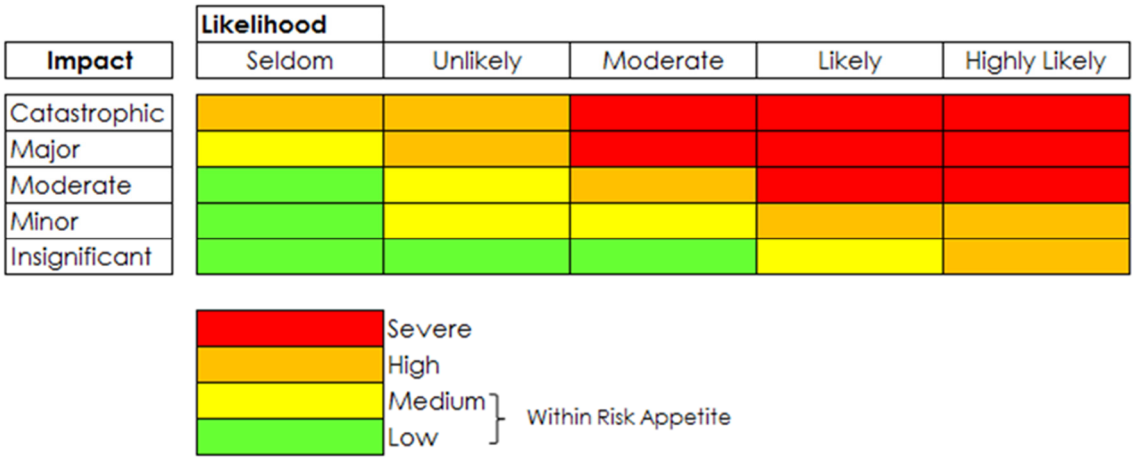
(f) **Recognised International Risk Management Framework**

The principles, practices and process of this Risk Management Policy established by the Board are, in material aspects, guided by the ISO 31000:2018 – Risk management - Guidelines.

2. RISK APPETITE

Risk appetite is the amount/ level of risks, on broad level, the Group is willing to accept in pursuit of its corporate objectives and must not be more than the risk capacity of the Group.

It is acknowledged that there is a certain level of risk to be undertaken in business and the Board determines the level of risk acceptance of "Medium" and "Low" level as within the risk appetite, as follows:



The Group's risk appetite will be reviewed annually or more often as circumstances dictate to reflect the changes in the Group's internal and external business context. Business

context is defined as "the trends, events, relationships and other factors that may influence, clarify, or change the Group's current and future strategy and business objectives".

3. KEY FEATURES

The key features of the Group's Risk Management Policy are as follows:

(a) An adequate and effective risk management governance structure and process that provide for continuous risk monitoring and management by risk owners and SRMC;

(b) A risk management process that is embedded into the day-to-day operations and decision makings (strategic and operations) at all level of the Group;

(c) Monitoring of the key business risks by governance body of the Group to ensure its adequacy and effectiveness; and

(d) Assurance processes in place in relation to management of key risks of the Group.

The key responsibilities of the Board, AC, SRMC, Key Risk Officer and risk owners are documented in the **Risk Management Reporting Structure** set out in Section 2.

4. ONGOING IDENTIFICATION AND EVALUATION OF RISKS

The Group shall ensure that there is an ongoing process for identification, evaluation and management of risks. This process primarily involves:

(a) identifying the mission, vision, core values, strategies and business objectives of the Group to ensure that the risk management activities are carried out in the pursuit of mission, vision, core values, strategies and business objectives established;

(b) identifying the events/conditions that, should they occur, would lead to the objectives not being achieved;

(c) assessing the probability that the risk events could occur and the significance of their impact on achieving the mission, vision, core values, strategies and business objectives;

(d) identifying controls that are/ can be put in place that prevent or detect the occurrence of the risk or mitigate the impact;

(e) assessing the probability of occurrence and impact of the risk having considered the existence and effectiveness of the internal controls identified;

(f) identifying options available to manage the risk identified and to evaluate such options and to determine appropriate responses to such risk and resulting management actions, in the event that the controls are non-existence or are not adequate and/or effective;

(g) establishing effective information and communication system at all level of organisation to facilitate effective risk management action and activities and to provide continuous training to embed risk management awareness in day-to day operations; and

(h) monitoring of adequacy and effectiveness of risk management continuously, through internal review and verification and verification from independent party(ies).

The SRMC uses the Risk Register as per **Appendix A** for the above-mentioned processes and performs updates on a yearly basis or as and when there are any changes in internal and/or external business context requiring such updates. The SRMC updates the Risk Register with the assistance and feedback from the risk owners and also through the results of the internal audit work.

The Key Risk Report and KRP are compiled and reviewed by SRMC based on updated KRR and submitted to the CEO for his review and approval.

Subsequent to the review and approval of the CEO, the Key Risk Report and KRP shall be presented to the AC for their review and approval. The AC is to subsequently report results of such review and approval and recommendations to the Board for their final review and decision.

5. STRATEGIES AND BUSINESS OBJECTIVES SETTING

To align corporate strategies and business objectives (including undertaking of new project, merger & acquisition and corporate exercise) with the mission, vision, core values and risk appetite, it is important that the corporate strategies and business objectives setting be subjected to the following process which primarily involves:

(i) identifying the mission, vision, core values, strategies and business objectives of the Group to ensure that the strategies and business objectives envisaged (including all options) are properly aligned;

(ii) identifying the potential material events/conditions (i.e. the strengths, weakness, risks and opportunities) that, should they occur, would adversely affect the achievement of the proposed strategies and business objectives;

(iii) assessing the probability that the material events/ conditions could occur and the significance of their impact on the achievement of the proposed strategies and business objectives;

(iv) identifying controls that are in existence that prevent or detect the occurrence of the material events/conditions and its impact;

(v) assessing the possibility and impact of the material events/conditions identified having considered the existence and effectiveness of the internal controls in existence or action plans implemented to mitigate the risks; and

(vi) identifying options available to manage the material events/conditions identified and to evaluate such options and to determine appropriate response(s) to such material events/conditions and feasible action plan in the context of the Group, in the event that the controls are non-existence or are not adequate and/or ineffective or inadequate or no action plan implemented.

The SRMC uses the Strength, Weakness, Opportunity and Threat ("SWOT") Analysis for all options of the Group's corporate strategies and business objectives as per **Appendix B** for any proposed strategies/business objectives, new projects, mergers and acquisitions and corporate exercises. The duly completed SWOT Analyses, together with the feasibility study of all options shall be tabled to the Board for review and decision making.

During the implementation and integration for merger & acquisition exercises, continuous SWOT Analysis and monitoring of internal and external events, progress of the implementation of management action plans to mitigate the weaknesses and risks and to optimise the strengths and opportunities identified, is carried out and where necessary appropriate modifications or additional action plans instituted to align the implementation and integration to meeting the mission, vision, core values, strategies and business objectives of the Group. The SRMC shall report to the Board on the progress of the implementation and integration for merger & acquisition exercise during the scheduled meetings until it is implemented and integrated completely into the Group.

Upon the new strategies and business objectives being implemented and integrated completely into the Group, the relevant Risk Registers of the new strategies and

business objectives are to be compiled by SRMC and subjected to the process of Ongoing Identification and evaluation of Risks above.

6. DEFINITIONS

Risks

Risk is defined as the possibility of an adverse event taking place which will result in the organisation not being able to achieve its business objectives. There are two categories of risks - **inherent** risk and **controllable** risks, both of which when combined together makes up the enterprise-wide risks. Risk is measured in terms of possibility and impact.

Inherent risks are risks that exist in a specific corporate or business environment. These risks are generally outside the control of management. Examples of such risks are trade war, disruptive business model, volatility of markets, actions of competitors, fast changing technological advances affecting products and business processes, ad hoc changes in government policies, political disruptions, pandemics, natural disasters, etc.

Controllable risks are those that may result in material losses due to failure of the internal control system. Management can directly influence these risks. Examples of such risks are compliance with regulatory requirements, doubtful trade debts, foreign currency fluctuations, etc.

Opportunity refers to those actions or potential actions that creates, improves or alters positively goals or approaches for creating, preserving and realising value.

Controls

Controls are policies, standards, procedures, physical changes put in place to minimise adverse risks. Controls can be classified into three main categories as follows:

(a) **Preventive Controls** are controls that helps prevent the risks from occurring by reducing the possibility. Examples of such risks are segregation of duties, established policies and procedures, etc.

(b) **Detective Controls** are controls which:

(i) Identify impending risks that are about to take place thereby allowing action to be taken in reducing the possibility of the risk occurring.

(ii) Identify unfortunate events as soon as possible after its occurrence to prevent further deterioration. This reduces impact.

(c) **Corrective Controls** are controls that minimise the impact of the losses to enable prompt recovery when an unfortunate event occurs. Examples of corrective controls are business continuity plan, trained personnel for succession, periodical backup of data in the computer, etc.

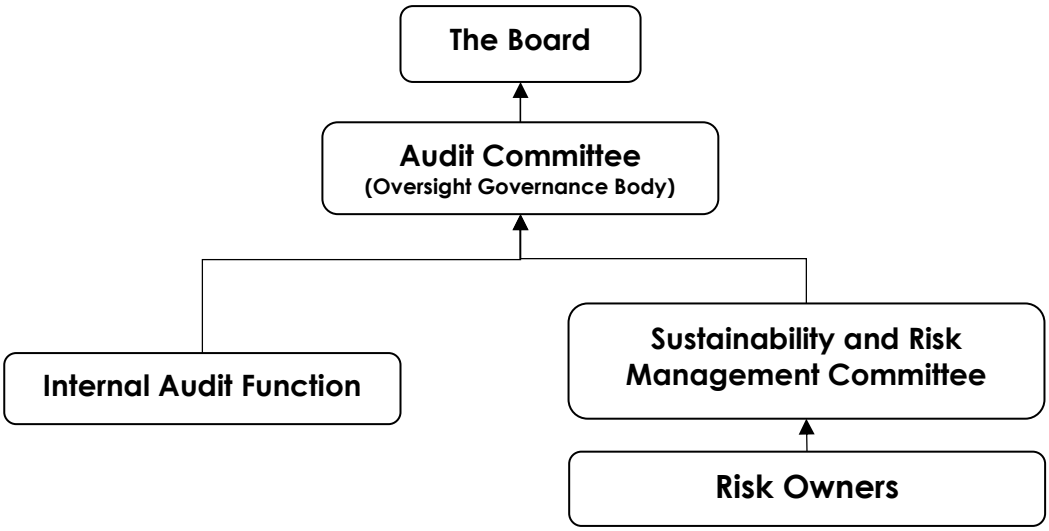
7. REVIEW

The Risk Management Framework shall be reviewed by the AC and the Board at least once every 3 (three) years or as and when the need arises to keep it current and relevant at all times and in line with prevailing listing requirements and guidelines.

Section 2

Risk Management Reporting Structure

1. OUTLINE OF RISK REPORTING STRUCTURE



The roles and responsibilities of each function in the proposed risk management reporting structure is as follows:

Function		**Roles/Responsibilities**
Board of Directors ("the Board")	:	Primarily responsible for the risk management on group wide basis. This would involve: (a) determining and approving the Group Risk Management Framework as well as the Group's risk appetite; (b) periodic review of the Key Risk Report and Key Risk Profiles of the Group (at least on an annual basis) and determine the acceptability of the residual risks of the Group and proposed management action plan(s) (if applicable); (c) to ensure the adequacy and effectiveness of the Group's governance, risk management and control structure and processes to manage the key business risks to a level acceptable to the Board or to exploit opportunities or emerging opportunities for value creation; (d) To ensure proposed corporate strategies and business objectives (including undertaking of new projects, mergers & acquisitions and corporate exercises) are aligned with the mission, vision, core

values, strategies and business objectives of the Group, including within the risk appetite of the Group; and

(e) To monitor the progress of the implementation and integration of the proposed strategies and business objectives, alignment of the action plans undertaken or to make decisions on the continuation of the implementation (with or without changes) and integration.

Audit Committee ("AC") : Delegated with the oversight roles in relation to risk management:

(a) To assess, formulate, review and approve the Group Risk Management Framework (including policies and processes) and risk appetite and recommend to the Board for adoption;

(b) To ensure implementation and compliance with approved Group Risk Management Framework (including policies and processes) and to ensure that key risks identified are addressed appropriately and on timely basis;

(c) To review the Group's risk exposures and to review the status of management action in mitigating significant risks identified;

(d) To review and assess the adequacy and effectiveness of the Group Risk Management Framework (including policies and processes), risk appetite and internal control system and to recommend such changes as may be deemed necessary to the Board;

(e) To review and assess the risks associated with all significant proposed strategic transactions of the Group and report the same to the Board for its deliberation of the transaction; and

(f) To review the adequacy and effectiveness of the Group's system of internal controls established by the Management to manage key business risks through internal audit reports from Internal Audit Function.

Sustainability and Risk Management : The SRMC is delegated the task of implementing the approved Group Risk Management Framework and

Committee ("SRMC")	continuous risk monitoring. The duties of the SRMC are as follows:

(a) Implement the Group Risk Management Framework approved by the AC and the Board;

(b) Implement the risk management process which includes the identification of key risks and devising appropriate action plan(s) in cases where existing controls are ineffective, inadequate or non-existence and communicate methodology to the risk owners;

(c) Ensure that risk strategies adopted are aligned with the Group's organisational strategies. (e.g. vision/mission/core values, corporate strategies/ business objectives, etc.), Group Risk Management Framework (including policies and processes), risk tolerance and risk appetite;

(d) Continuous review and update(s) of the Key Risk Registers (including changes (increase or decrease) in identified risk events/ levels and incorporation new or emerging risks or integration of business risks from implementation and integration of new strategies and business objectives into new key risk registers for monitoring) and compilation of Key Risk Profile and Key Risk Report of the Group due to changes in internal and external business context, business processes, business strategies or external environment and determination of management action plan, if required;

(e) Update the Board, through the AC, on changes to the Key Risk Profile on periodical basis (at least on annual basis) or when appropriate (due to significant change to the internal and external business context) and the course of action to be taken by management in managing the changes; and

(f) To performs SWOT Analysis for all options of the proposed strategies and business objectives as per **Appendix B** and to monitor and report to the Board on the progress of the implementation and integration for merger & acquisition during the scheduled meetings until it is implemented and integrated completely into the Group.

Risk Owners : The responsibilities of risk owners would be:

(a) Manage the risks of the business processes under his / her control;

(b) Continuously identify risks and evaluate existing controls. If controls deemed ineffective, inadequate or non-existent, to establish and implement controls to reduce the likelihood and/or impact.

(c) To report to the SRMC of the emergence of new business risks or change in the existing business risks through the use of prescribed form in **Appendix A** on a timely manner and assist the SRMC.

(d) To assist with the development of the management action plans and implement these action plans;

(e) Assist the SRMC with the yearly update of the changes in the Key Risks Register, management action plans and the status of these plans; and

(f) Ensure that staffs working under the him/her understand the risk exposure of the relevant process under his / her duty and the importance of the related controls; and

(g) Ensuring adequacy of training for staff on risk and opportunity management.

Co-Key Sustainability & Risk Officer ("KSRO") : The responsibilities of Co-Key Sustainability and Risk Officer are:

(a) Acting as central contact and coordinator for all risk management and sustainability matters within the Group;

(b) Assisting the Board and AC in the implementation of the approved Risk Management Framework;

(c) Facilitating and coordinating all risk management processes and activities (for example, continuous monitoring of risks and risk events identified, identification and incorporation of new or emerging risks and risk events into Risk Register, update (including analysis and evaluation) of risks and risk events, project leader in dealing with new or changes

in material risks and risk events, progress of mitigation plans implementation, risk reporting and continuous improvement in risk management process) in the Group;

(d) Documenting all risk management activities and meetings in the Group; and

(e) Ensuring proper communication of all risk matters, through the use of the prescribed form in **Appendix A** or meetings or other electronic platforms, between the SRMC and the respective risk owners;

(f) Reporting to and regularly updating the AC and Board on risk matters (including any changes in risk matters, matters discussed at the regular SRMC meeting, etc)

Internal Audit Function : The Internal audit function is responsible for:

(a) Reviewing the Group's governance, risk management and internal control structures, processes and procedures to determine their adequacy and effectiveness in relation to the Group's key risks and to reporting the same to the AC;

(b) Reviewing whether all relevant key risks have been identified and managed adequately for the business activities under review and to reporting the same to the AC; and

(c) Verifying and ensuring compliance with the internal controls established, company policies, rules and regulations and relevant laws and statutory rules and regulations.

The internal audit function's findings may be used by the SRMC to facilitate the review of the Key Risk Registers.

Independence of Internal Audit Function:

To provide for the independence of the internal audit function, the internal audit function shall not perform the following:

- Perform work or act on behalf of Management. The Management acknowledges and agrees that the Management has the ultimate

responsibility for all management decisions and shall ensure it acts to preserve the independence of the IA function at all times;

- Determine which, if any, recommendations for improving internal control should be implemented;

- Perform on-going internal control monitoring activities or other control activities that may affect the execution of transactions or any activity to ensure that transactions are properly executed and/or accounted for or perform routine operating activities in connection with the Group's operations; and

- Acts in any capacity as or equivalent to a member of the Management.

2. PROPOSED TERMS OF REFERENCE FOR SUSTAINABILITY AND RISK MANAGEMENT COMMITTEE

2.1 Introduction

Risks are inherent in every business and the increasing complexity and volatility of today's business and external environment, coupled with additional and more stringent compliance legislations means that the ability to effectively manage risk has become ever more important. The Board is mindful that, as the Group concentrates its business attention on its existing businesses, it may be exposed to inherent risks in relation to the industry and business environment it operates in and serves. Whilst the Board still retain ultimate responsibility for risk management and for determining the appropriate level of risk appetite, the SRMC and AC are respectively entrusted by the Board with the duty to implement the approved Group Risk Management Framework (including policies and processes) approved by the Board and oversight of risk management practices on a group wide basis respectively. In essence, the SRMC is responsible for the execution and management of the Group Risk Management Framework (including policies and processes) while the AC takes on a supervisory role in respect of the Group's Group Risk Management Framework (including policies and processes).

2.2 Terms of Reference

The terms of reference of the SRMC are as follows:

- To ensure that the Group Risk Management Framework (including policies and processes) is embedded into business processes and functions effectively throughout the Group and is within the risk appetite established by the Board.

- To identify the potential risks and to formulate mitigation action plan(s) to manage the risks identified within the risk appetite of the Group.

- To ensure that the KRR and the KRF of the Group compiled therefrom remains relevant taking into consideration any changes in internal business processes, business strategies or external environment.

- To provide awareness and training/ education on risk management to all level of the Group.

- To report the risk management activities, as well as Key Risk Report and KRP and the Risk Dashboard of the Group compiled therefrom, to the AC on periodical basis (at least annually) or on a timely manner (if there are substantial changes in internal and business processes, business strategies or external environment) for their independent review.

- To ensure adequate resources are available in order to carry out its functions and responsibilities.

- At the direction of the AC, to perform assessment for all options of any significant proposed strategies and business objectives and to report the results of the assessment to the AC for their review and recommendation to the Board.

2.3 Powers and Authorities

As the committee that has been entrusted by the Board with the task of executing and managing the risk management policy, the SRMC is vested with the following authority:

- Have the adequate resources which it needs to perform its duties;

- Have full access to any information which it requires in the course of performing its duties, subject to restrictions and limitation on access to highly confidential information;

- Have direct communication channels with the CEO, the AC and the Board, as the case may be, to obtain direction, advice, and feedback in performing its duties; and

- To obtain the services of the external professional (if required) at the expense of the Group in carrying out its duties

2.4 Composition

- The members of the SRMC shall include a mix of persons with risk and business management knowledge and experience.

- SRMC members are nominated employees from the various divisions in the Group, preferably Executive Directors and Head of Departments. The SRMC should also include the KSRO as a member.

- The number of members of the SRMC shall not be less than 5 and more than 15.

Secretary of the SRMC

- The Secretary of the SRMC shall be appointed from among the members of the SRMC or such other person as the SRMC shall decide from time to time.

- The Secretary of the SRMC is to assist the SRMC in performing work pertaining to calling of meeting, preparation of notices and agendas, delivery of supporting documents for the meeting and keeping of minutes of meetings.

2.5 Minutes

- The SRMC meeting proceedings shall be minuted by the Secretary and circulated prior to the next meeting along with notice and meeting papers at least 7 (seven) working days before the meeting.

- A copy of minutes of meeting has to be circulated to the AC and the Board to keep them adequately informed of the SRMC's activities.

2.6 Meetings

- The SRMC shall meet at least once (1) in each financial year or more frequently if necessary. The quorum for a meeting shall be more than 50% of the existing members (including Chairman and KSRO) of the SRMC.

- The Chairman of the SRMC may call for a meeting as and when required with reasonable notice (preferably 7 days' notice with agenda of matters to be discussed). An emergency SRMC meeting to discuss urgent/ critical matters may be called with short notice if at least 50% of the members agree to the short notice.

- The SRMC may invite any non-member and external professionals whom the SRMC thinks fit and proper to attend its meeting to assist in its deliberations and resolutions of matters raised.

2.6 Confidentiality

The members of SRMC shall ensure that all matters and information presented and discussed in the meeting (including but not limited to, matters relating to the affairs of the Group) are kept strictly confidential.

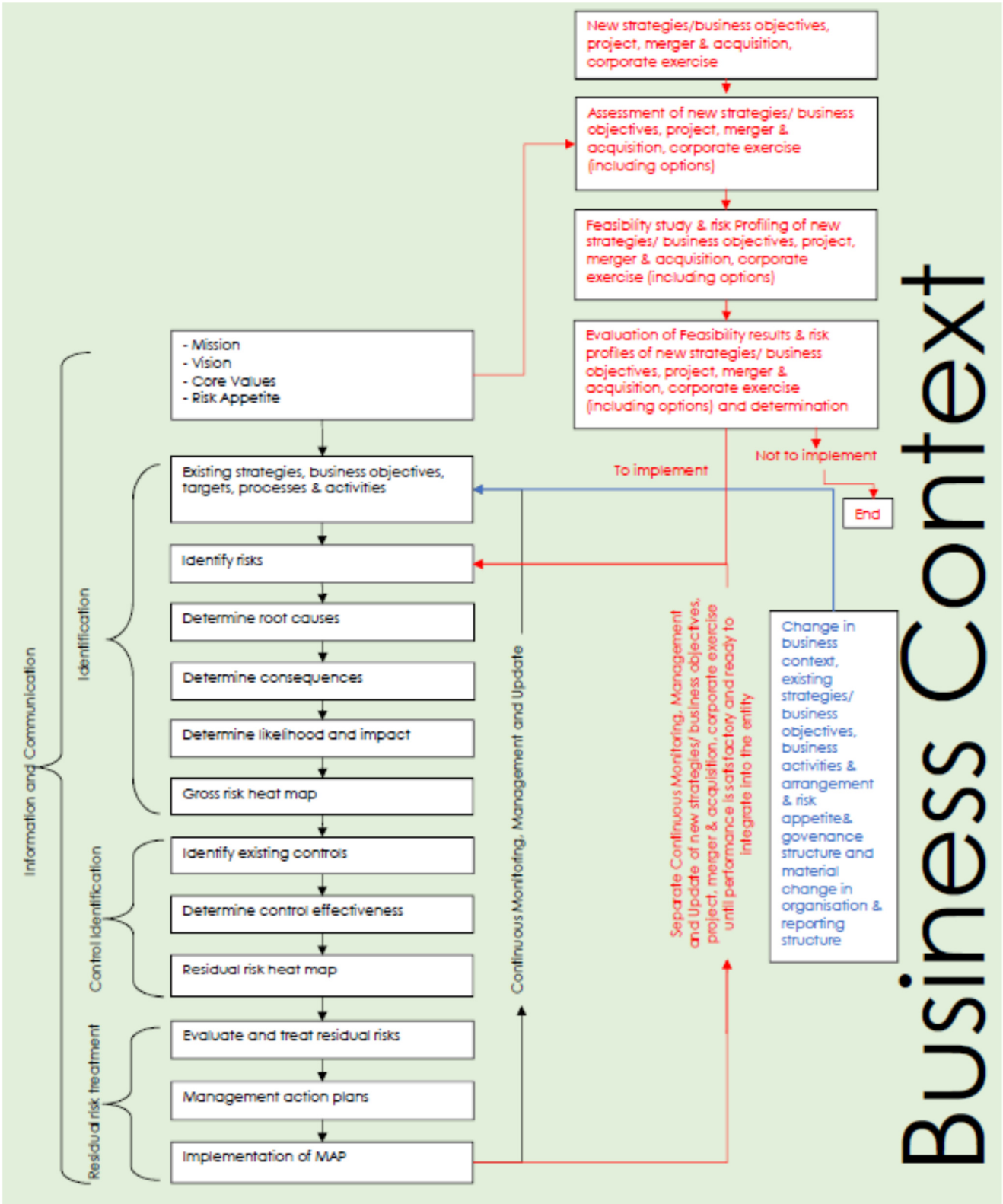
2.7 Membership of SRMC

Designation		**Member**
Chairman	:	Executive Director
Co-Key Sustainability & Risk Officer	:	Corporate Finance Manager & Head of Internal Audit
Members	:	Risk Owners (to be nominated by the Chairman of the SRMC)

Section 3

Risk Assessment, Communication and Monitoring Process

1.1 Risk Identification Process



The Board, along with the CEO, shall be responsible for the establishment of the vision, mission and strategic plans (including specific goals and business objectives for the Group). The strategic plans will be used to understand and identify the risks that the Group faces and opportunities available.

In order to assess the Group's risks comprehensively, the Group shall utilise its risk and control parameters approved by the Board, and the KRR (refer to **Appendix A)** as the common risk language and risk communication tool within the Group respectively. The approved risk and control parameters as well as KRR will be used to ensure that all departments/ divisions within the Group are using the same terminology and methodology when referring to risk management.

In using the KRR as a risk communication tool, current and emerging risks that could impact or influence the achievement of the Group's business objectives and strategies can be properly identified and documented.

In identifying risks, the following sources of risks will be used as a guide to ensure that all key risks have been identified.

- **External** - External factors such as industry competition, take-over bids, globalisation, mergers, economic conditions, environment;
- **Regulatory** - Rules, regulations and guidelines by statutory and government bodies with penalties for non-compliance
- **Legal** - Legal arrangements, contracts, agreements and obligations and legal actions by third parties
- **Corporate Governance** - Corporate framework for managing the organisation, e.g. organisational structure, corporate culture, values and delegation of authorities.
- **Financial** - Financial considerations, e.g. profitability, cash flow and cost management and asset/liability management.
- **Customer** - Internal and external customers, including agents, distributors, etc.
- **Product and Services** - Product or services sold by organisation, including marketing and promotions.
- **Suppliers** - External parties who supply goods and services to the organisation, e.g. vendors and contractors, including outsourcing providers.
- **Human Capital** - Human resources of organisation, permanent and temporary, e.g. staff development and growth, open channel of communication, succession planning.

- **Technology and innovation** - Risks arising from the use of technology and innovation in operation and product/service dependency on technology and innovation (Including cybersecurity and disruptive technologies)
- **Physical** - Risks arising from hazards to assets and people
- **Fraud** - Risks arising from any act characterised by deceit, concealment or violation of trust
- **Bribery & Corruption -** Risks arising from the bribery & corruption incident within the entity
- **Sustainability** – Risks and opportunities identified through formal sustainability assessment process. The Heads of Department to include sustainability issues, together with its results of assessment, current standing and responses, in the Risk Management Process for risk management and consideration.

The identification of risk is the joint responsibility of the risk owners and SRMC. The SRMC should have sufficient details such as the following:

(i) The potential causes that could result in the risk event occurring;

(ii) The likelihood of the risk event arising and the risk materialising and impacting the Group; and

(iii) The potential consequences when such risk materialises.

1.2 Risk Assessment Process

(a) The risk identified shall be rated based on the following criteria: Possibility of risk occurring; and

(b) Impact to the Group should the risk occur – financially, reputation wise, effects on safety, health and environment, risk consequence and opportunities

Best judgement should be used in rating the risk based on the tables below assuming that the Group carry on its business activities with implementation of controls to manage or mitigate the risk.

With all the relevant controls for a particular risk have been identified, the risk shall be rated **at Residual level**, taking into consideration the adequacy and effectiveness of the controls put in place, in terms of possibility of the risk occurring

and its impact if and when it occurs after taking into consideration existing controls using the rating tables as follows.

The possibility rating used for is as follows:

ID	Description	User Description
5	Highly Likely	• Very likely to happen & the event may occur more than once on a monthly basis • Speculative with no mitigation procedure • > 75% chance of probability within next 12-24 months
4	Likely	• Highly likely to happen & the event may occur more than once on a quarterly basis • Analytically demonstrated possible mitigate procedure • 50-75% chance of probability within next 12-24 months
3	Moderate	• Known to happen & the event might occur at some time, i.e. once per quarterly basis • Partially demonstrated or mitigated by existing procedure • 25-50% chance of probability within next 12-24 months
2	Unlikely	• Very low likelihood of happening & the event could occur at some time, i.e. once in a year • Demonstrated or well mitigated by existing procedure • 0-25% chance of probability within next 12-24 months
1	Seldom	• The event may occur only in exceptional circumstances, e.g. once in every 3 years • Not known to happen, proven or completely mitigated by existing procedure • Minimal chance of probability within next 12-24 months.

1.2.1. Impact rating (Financial Aspect)

ID	Consequences				
	1	2	3	4	5
Factors	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Revenue (Based on latest available audited financial statements)	• < RM 100,000 decrease in revenue	• RM 100,000 to 2.0% decrease in revenue	• 2.0% to 10.0% decrease in revenue	• 10% to 30% decrease in revenue	• > 30% decrease in revenue
Gross Profit (Based on latest available audited financial statements)	• < RM 100,000 decrease in gross profit	• RM 100,000 to 2.0% decrease in gross profit	• 2.0% to 10% decrease in gross profit	• 10% to 30% decrease in gross profit	• > 30% decrease in gross profit

1.2 Risk Assessment Process (Cont'd)

1.2.1. Impact rating (Financial Aspect)

	Consequences				
ID	**1**	**2**	**3**	**4**	**5**
Factors	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Profit/(Loss) before taxation for the year (Based on latest available audited financial statements)	• < RM 50,000 decrease in profit	• RM 50,000 to 2.0% decrease in profit	• 2.0% to 10% decrease in profit	• 10% to 30% decrease in profit	• > 30% decrease in profit
Cash flow impact	• Insignificant impact • Reduce cash flow from operating activities by < RM 50,0000	• Cash flow impact absorbed under normal operating conditions • Reduce cash flow from operating activities by RM 50,000 < X < Rm 1.0 million • Gearing ratio increased by < 10%	• Cash flow is affected negatively and working capital requirements rely on external funding • Reduce cash flow from operating activities by RM 1.0 million < X < Rm 5.0 million • Gearing ratio increased by 10% to 30%	• Cash flow is adversely affected and rely heavily on external funding for working capital • Resulting in negative cash flow from operating activities • Gearing ratio increased by 30% to 100%	• Imminent cash flow problems resulting in inability to meet liabilities / obligations • Gearing ratio increased by > 75%
Financial institution/Debt Financing	• No clawback by financial institution.	• 10% drawn down financial facilities or debt equity are being clawback and no difficulty in obtaining additional funding to meet the call-back.	• 10% to 30% drawn down financial facilities or debt equity are being clawback and facing some difficulties which can be overcome within 3 months	• 30% to 80% drawn down financial facilities or debt equity are being clawback and facing difficulties which take more than 3 months to overcome.	• More than 80% of financial facilities or debt equity are being drawn back and being blacklisted for future borrowings from any financial institution. Winding up proceeding is being instituted against the company.

1.2. Risk Assessment Process (Cont'd)

1.2.2. Impact rating (Non-Financial Aspect)

ID	Consequences				
	1	2	3	4	5
Factors	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
• **Regulatory Compliance: Department of Environment and Department of Occupational Safety and Health** • **Product & Service Quality**	• Minimal impact • No customer complaint or no impact • No pollution • No penalty imposed by regulators or governing authorities	• Moderate impact • Noticeable effect, minor customer complaint • Verbal feedback by regulators / governing authorities	• Moderate impact • Customer complaint resulting in claim • Customer rework • Non-compliance which may result in penalty / compound • Alternative available	• Moderate impact • Customer complaint (major) that may incur business loss • Violation of environmental requirements • Penalty	• Major impact • Catastrophic, recall, fatality, legal action, costly compensation • Violation of environmental & OSHA compliance that may cause operation stoppage
Anti-Bribery and Corruption	[redacted]	• Verbal feedback and comment on non-compliance and no penalty imposed by regulators or governing authorities	• Complaint on minor non-compliance reported to or instance of minor non-compliance discovered by ABC Compliance Unit and promptly resolved and corrective action implemented. No penalty imposed by regulators or governing authorities.	• Written warning on non-compliance and/or penalty imposed by regulators or governing authorities	• Violation of Anti-Bribery and Corruption resulting in prosecution by regulators or governing authorities or legal action taken against the company by stakeholders.
Image / reputation	• Minimal / no impact on image / reputation	• There is potential impact on image / reputation with minor complaints	• Image / reputation will be affected in the short term with complaints to minister / local members and stakeholders	• Serious with potential for permanent diminution in image / reputation with adverse publicity	• Sustained, serious loss in image / reputation in longer term with extensive negative nationwide media coverage

1.2. Risk Assessment Process (Cont'd)

1.2.2. Impact rating (Non-Financial Aspect) (Cont'd)

ID	Consequences				
	1	2	3	4	5
Factors	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Other Regulatory Compliance, e.g. SC, BURSA, the Companies Act, MFRS, IRB, anti-money laundry etc.	• Verbal complaints/ warning	• No fine but warning – no disruption to operations / services	• Fined and minor disruption to operations / services	• Disruption to operations / services over a period of time (1 weeks < X ≤ 2 weeks)	• Significant disruption to operations / services over an extended period of time
Operational and Environmental Performance – ISO Certification	• No negative trend • May lead to environmental concern • No efficiency loss	• Indicators with negative trend < those with positive trend • Slight aesthetic effect • Slight process inefficiency	• Indicators with negative trend = those with positive trend • on-site pollution • Able to be contained immediately • Process inefficiency resulting in significant resource loss / wastages	• Indicators with negative trend > those with positive trend • Alternatives available • Pollution occurred • Injuries	• Consistently all indicators negative trend • No alternatives available • Widespread pollution occurred • Injuries that lead to fatality
Management's response and action	• Impact can be readily absorbed through normal activity	• An adverse event which can be absorbed with some management response and action	• A serious event which requires additional management response and action	• A critical event which requires extraordinary management effort, response and action	• Disaster with potential to lead to collapse of the business
Business disruption	• < 1 day	• 1 day < X ≤ 7 days	• 7 days < X ≤ 14 days	• 14 days < X ≤ 30 days	• > 30 days
Key Customers (defined as top 10 customers)	• No loss of key customer	• Loss of 1 key customer	• Loss of 2 key customers	• Loss of 3 key customers	• Loss more than 3 key customers

1.2. Risk Assessment Process (Cont'd)

1.2.2. Impact rating (Non-Financial Aspect) (Cont'd)

ID	Consequences				
	1	2	3	4	5
Factors	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Employees	• < 5% employee turnover rate • Involving non key position.	• 5% to 10% employee turnover rate. • Involving 1 key position resignation.	• 10% to 20% employee turnover rate. • Involving not more than 2 key position resignations.	• 20% to 50% employee turnover rate. • Involving not more than 3 key position resignations. • Employee strike may occur.	• High employee turnover rate. More than 50%. • Involving more than 3 key position resignations. • Employee strike for more than 3 days.
Key Suppliers (defined as top 10 suppliers)	• No loss of key supplier	• Loss of 1 key supplier • The alternative source of material supply cannot be identified in order to fulfil customer orders from 1 day to 3 days	• Loss of 2 key suppliers • The alternative source of material supply cannot be identified in order to fulfil customer orders from 3 days to 7 days	• Loss of 3 key suppliers • The alternative source of material supply cannot be identified in order to fulfil customer orders from 7 days to 21 days	• Loss more than 3 key suppliers • The alternative source of material supply cannot be identified in order to fulfil customer orders for more than 21 days
Operational Improvement - ISO	• Insignificant • The impact on objectives of QMS is very low. • Opportunity occurring would represent a minor revision to planned outcome	• Minor • The impact on objectives of QMS is low • Opportunity occurring may improve slightly the desired quality of the outcome	• Moderate • The impact on objectives of QMS is moderate • Opportunity occurring would improve the desired quality of the outcome but not improve the overall purpose	• Significant • The impact on objectives of QMS is high • Opportunity occurring would significantly improve the original desired quality of the outcomes	• Very significant • The impact on objectives of QMS is very high • Opportunity occurring improve the quality of desired outcomes to an extent that it exceeded the planned result

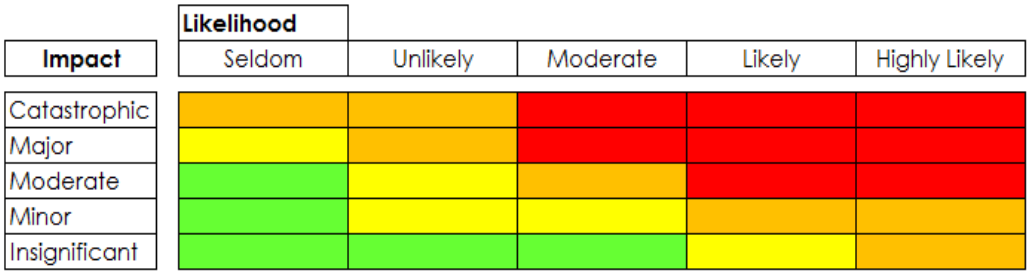
1.2. Risk Assessment Process (Cont'd)

1.2.2. Impact rating (Non-Financial Aspect) (Cont'd)

Best Practices	• No perceived value for improvement	• Pursuing the opportunity will slightly improve good governance	• Pursuing the opportunity will considerably improve good governance and will improve customer satisfaction	• Pursuing the opportunity will highly improve good governance and bring new business opportunities for the company and value added to customer	• Pursuing the opportunity will improve good governance essential for sustainability and enable company to become market player in industry.

1.2. Risk Assessment Process (Cont'd)

Consequently, the all-rated risks will be mapped in the Gross Risk Heat Map as illustrated below.



1.3 Control Activities Identification Process

As part of the risk identification process, existing controls in place should be identified together with its control owner (person responsible to monitor the controls to ensure its effectiveness and compliance).

Controls are the policies, standards, procedures and physical changes to minimise adverse risks or to maximise opportunity(ies). The controls relating to the identified risks can be categorised as follows:

Preventive : Controls to prevent the risk from occurring.

Detective : There are two aspects to detective controls: -

- To identify impending risks which are about to take place thereby enabling awareness of risks.
- To identify adverse events as soon as possible to prevent further deterioration. This reduces impact.

Corrective : After the risk event(s) have taken place, the control(s) in place to minimise losses and to enable recovery to take place promptly.

Once all the relevant controls for a particular risk have been identified, the risk shall be rated **at Residual level**, take into consideration of the adequacy and effectiveness of the controls put in place, in terms of possibility of the risk occurring and its impact when it occurs after taking into consideration existing controls using the same rating tables in Section 1.11.2 above.

The adequacy and effectiveness of the controls can be assessed in accordance with the following criteria:

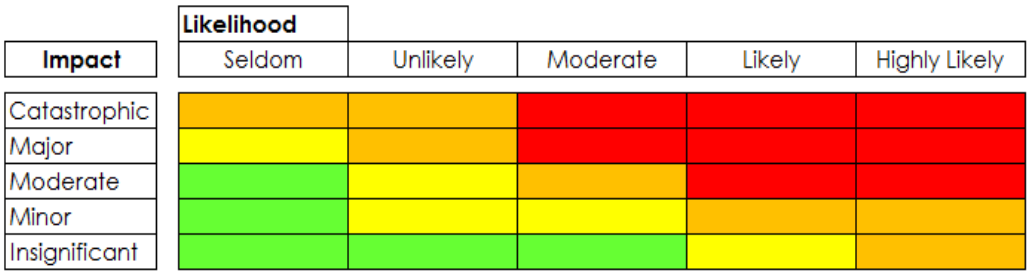
(i) Reduce the possibility of risk occurring; and

(ii) Reduce the impact on the Group after the risk has occurred.

Rating Category	Criteria
4	***High – Adequate & Effective*** • Controls are operating adequately & effectively and in accordance with management's control objectives for the area under review. • Controls are operating at its optimum level, functioning as intended and limited opportunity for further improvement exists in the form of long term action plan. • Presence of all controls and no control weaknesses were noted • No incidence of non-compliance/control lapses. • Good compliance culture and control environment.
3	***Moderate - Improvement opportunity available for Adequacy & Effectiveness*** • Few risks/controls require further improvement in order for the overall control mechanism to operate effectively. • Presence of all key controls / No key controls weaknesses were noted. • Absence of very limited less significant controls due to cost/benefit trade-off/Less significant control weaknesses are noted in a number of control components with compensating controls exist. • Opportunity for further improvement exists in the form of long term action plan. • No incidences of non-compliance/control lapses of critical control point or few incidences of non-compliance/control lapses of non-critical control point. • Satisfactory compliance culture and control environment
2	***Low - Unsatisfactorily Controlled - Significant improvement opportunity*** • Controls are not operating satisfactorily and effectively in accordance to its control objectives • Absence of very limited key controls/Key controls weaknesses are noted in a number of control components. • Less significant control weaknesses exist over the entire control environment. • Certain compensating controls exist where control weaknesses were noted. • Few incidences of non-compliance/control lapses of critical control point or frequent occurrence of non-compliance/control lapses of non-critical control point requiring short term Senior Management's attention. • Unsatisfactory compliance culture and control environment
1	***Very Low - Poorly Controlled*** • An effective control structure and mechanism had not been established • Significant weaknesses in controls have been noted across the control environment including a lack of both basic and compensating controls. • High to very high frequency of non-compliance/control lapses requiring immediate Senior Management's attention. • Weak compliance culture and control environment

It is important that only existing controls are being considered during the determination of control effectiveness. Proposed controls or controls which are currently not in place (e.g. in process of implementation) should not be considered in arriving at the residual level rating, as such proposed controls are management action plans which the management of the Group will need to put in place in a future date to manage or mitigate the risk.

Consequently, the rated risk will be mapped in the residual Risk Heat Map as illustrated below:



1.4 Risk Treatment Process

The Residual Risk Heat Map will enable the risk owners and the SRMC to identify and evaluate whether the residual risks are acceptable in the context of the departments or divisions' as well as the Group's objectives. The objective is not to eliminate all residual risks regardless but rather to ensure that the residual risk is reduced to an acceptable level in a cost effective and efficient manner.

It also allows the risk owners and the SRMC to make conscious and visible risk management decisions. The options available to the management in addressing the residual risks which is at an unacceptable level after a risk assessment is completed are as follows:

(i) **Avoid the risk** by ceasing to undertake the process or business activity altogether. Normally, this route is chosen when the risk could have a catastrophic impact on the business and where the costs of continuing with mitigating measures significantly outweigh the potential benefits; or

(ii) **Reduce the risk** by taking steps to minimise its impact and / or possibility of occurrence. This can be achieved by taking specific cost-effective actions aimed at reducing the possibility of the risk occurring in the first place or reducing the impact that the risk might have on the business should it actually occur; or

(iii) **Accept the risk** without any further action. Management may choose not to act and to consciously accept the risk as the risk is regarded insignificant to moderate risk in relation to the Group's risk appetite. However, management may want to consider the following factors before deciding to tolerate the risk:

(a) The adequacy and effectiveness of the existing controls;

(b) The possibility and consequences of the risk occurring; and

(c) The cost of additional controls to be put in place; or

(iv) **Share the risk** by passing on all or part of the risk to another party by:

(a) Transferring the entire business process / activity to another party such as outsourcing and sub-contracting;

(b) Sharing the business process / activity with another party such as joint venture;

(c) Sharing of risk through insurance; and

(d) Retaining the business process and transferring the legal or financial risks such as insurance.

(v) Pursue the risk or opportunity refers to action taken that accepts increased risk or optimise opportunity to achieve improved performance, e.g. extend credit term to above average credit rating customers during conducive economic environment.

However, if the management decision is to accept the unacceptable residual risk level, specific management action plans need to be formulated for implementation, documented and monitored for its implementation to ensure that the identified unacceptable risk is addressed.

2. CONTINUOUS MONITORING, MANAGEMENT AND UPDATE

2.1 Monitoring

- **Risk Owners**

  Risks and the effectiveness of control measures implemented to mitigate the risks need to be monitored on an ongoing basis to ensure changing circumstances do not alter the residual risk of the specific risk under his/her responsibilities. Therefore, for each risk under his/her duties, the risk owners are responsible to ensure compliance to the existing system of internal controls and take appropriate actions, where necessary, to manage the risks under their care.

  In addition, it is important for the risk owners to compile the KRR for new or emerging risks that are material by using the prescribed form per **Appendix A** and to submit such completed form to the SRMC in a timely manner for their

review for its adequacy and effectiveness of the mitigation plans formulated and implemented. It is important for the risk owners to implement additional mitigation plan(s) proposed by the SRMC to address and inadequacy(ies).

- **Internal Audit Function**

  The Internal Audit Function will review the adequacy and effectiveness, and relevance of the Group's risk management process and system of internal controls and report its findings to the AC respectively. The internal audit report will also be discussed with the management to agree on management action plans in respect of weaknesses in compliance with the internal controls as well as improvements to internal control procedures.

- **SRMC**

  Review is an integral part of the risk management policy and process. The SRMC will conduct ongoing review to ensure that the management action plan(s) remains relevant and are implemented in a timely manner. Factors which may affect the possibility and consequences of an outcome may change as may the factors which affect the suitability or cost of the various mitigation options. It is therefore necessary for the SRMC to update the KRR to reflect the current state of affairs of the Group as well as internal and external business context. The Internal Audit reports can also be used as a source of information by the SRMC to review the KRR. The SRMC shall compile the Key Risk Report and KRP of the Group based on the updated KRR and to table these reports to the AC for review.

  It is important that the SRMC lead in the assessment of new strategies and business objectives setting ((including undertaking of new projects, mergers & acquisitions and corporate exercises) for risk identification and assessment so that all key risks in relation to the proposals are considered and assessed prior to any decision making. It is important for the SRMC to monitor the progress of implementation and integration of the new strategies and business objectives on timely basis for alignment and to report to the AC and Board for their decision making.

- **AC**

  The AC will direct the internal audit activities and review the internal audits findings. Areas where risk is inadequately addressed, internal controls can be

improved or where there is lack of compliance shall be communicated to the Management for formulation and implementation of action plan(s).

The AC shall review and monitor the implementation of Group's Risk Management Framework (including policies and processes) as approved to ensure that they are adequate, effective and efficient in managing the Group's risks. A copy of the internal audit reports shall be presented by the Head of Internal Audit to the AC for their review and to assess and ensure material business risks are appropriately addressed.

- **The Board**

  The Board will review the KRR and KRP compiled by the SRMC after it has been reviewed by the AC and recommended for Board approval. The Board is ultimately responsible for the Group's risk management policy and process and shall approve the appropriate risk management policy.

  The Board shall take the lead in the assessment of the new strategies and business objectives setting (including undertaking of new projects, mergers & acquisitions and corporate exercises) to ensure that it is aligned with the mission, vision, core values and risk appetite of the Group. Upon receipt of the assessment results from the SRMC, the Board shall review the assessment results together with the feasibility study of all options and to make decision accordingly. The same process applies to the monitoring of the progress of the implementation and integration of new strategies and business objectives whereby upon receipt the updates from SRMC, the Board shall review and decide accordingly in line with the mission, vision, core values and risk appetite of the Group.

2.2 Communication

Communication is an important consideration at every step of the risk assessment process that involves both internal and external stakeholders, such as employees and customers respectively. The factors to consider in addressing communication issues relating to both the risk and process to manage the risk are:

- Communication should involve a 2-way dialogue with stakeholders with efforts focused on consultation rather than a one-way flow of information from decision maker to other stakeholders;

- Internal communication should be centrally organised by the KSRO with input directly from the risk owners at the point of identification, through prescribed form as per **Appendix A** or meetings or other electronic platforms;

- Annual reporting by the SRMC to the AC and subsequently to the Board in connection with updates and changes to the Group's KRP; and

- Periodic reporting by the AC to the Board to inform them on the state of the internal controls.

2.3 Continuous Improvement

The following are methods in which risk management capabilities can be continuously improved:

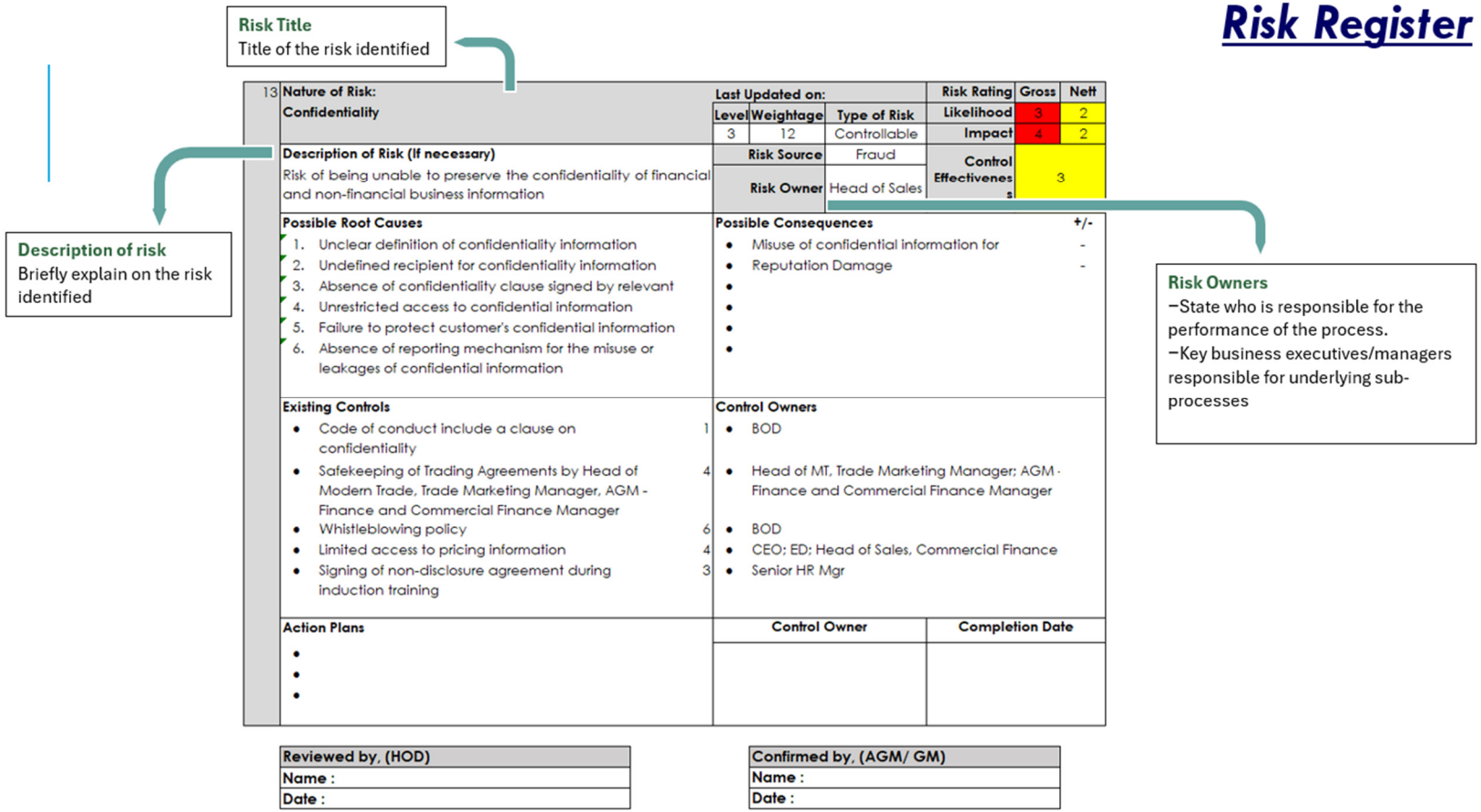
- **Benchmarking performance** to identify best practices. However, factors such as expected returns against cost incurred or return on investment, criticality of areas of improvement and availability of data need to be considered prior to performing a benchmarking exercise.

- **Interactive communication and knowledge sharing**, where this entails 360 degrees and cross functional communication. Risk Owners from different departments or companies within the Group, should be encouraged to communicate freely on sharing ideas about risk management strategies, risk management process improvements, potential risk events, etc.

- The Group Risk Management Framework should be included as part of the employee training program. Workshop session may be conducted by Risk Owners to create and emphasise awareness of risk management among employees of the Group and should emphasise the following areas:

  - Group's risk management policies.
  - Group's risk management framework and its supporting rationale.
  - Effective use of risk measurement methodologies of the Group.
  - Participation in communication channels to enable flow of risk information within the Group.
  - the Group's commitment to continuous improvement and what it means to the individual employee.

Appendix A – Risk Register



13	Nature of Risk: Confidentiality	Last Updated on: Level	Weightage	Type of Risk	Risk Rating	Gross	Nett
					Likelihood	3	2
		3	12	Controllable	Impact	4	2
	Description of Risk (If necessary): Risk of being unable to preserve the confidentiality of financial and non-financial business information	Risk Source		Fraud	Control Effectiveness	3	
		Risk Owner		Head of Sales			

Possible Root Causes	Possible Consequences	+/-
1. Unclear definition of confidentiality information	• Misuse of confidential information for	-
2. Undefined recipient for confidentiality information	• Reputation Damage	-
3. Absence of confidentiality clause signed by relevant	•	
4. Unrestricted access to confidential information	•	
5. Failure to protect customer's confidential information	•	
6. Absence of reporting mechanism for the misuse or leakages of confidential information	•	

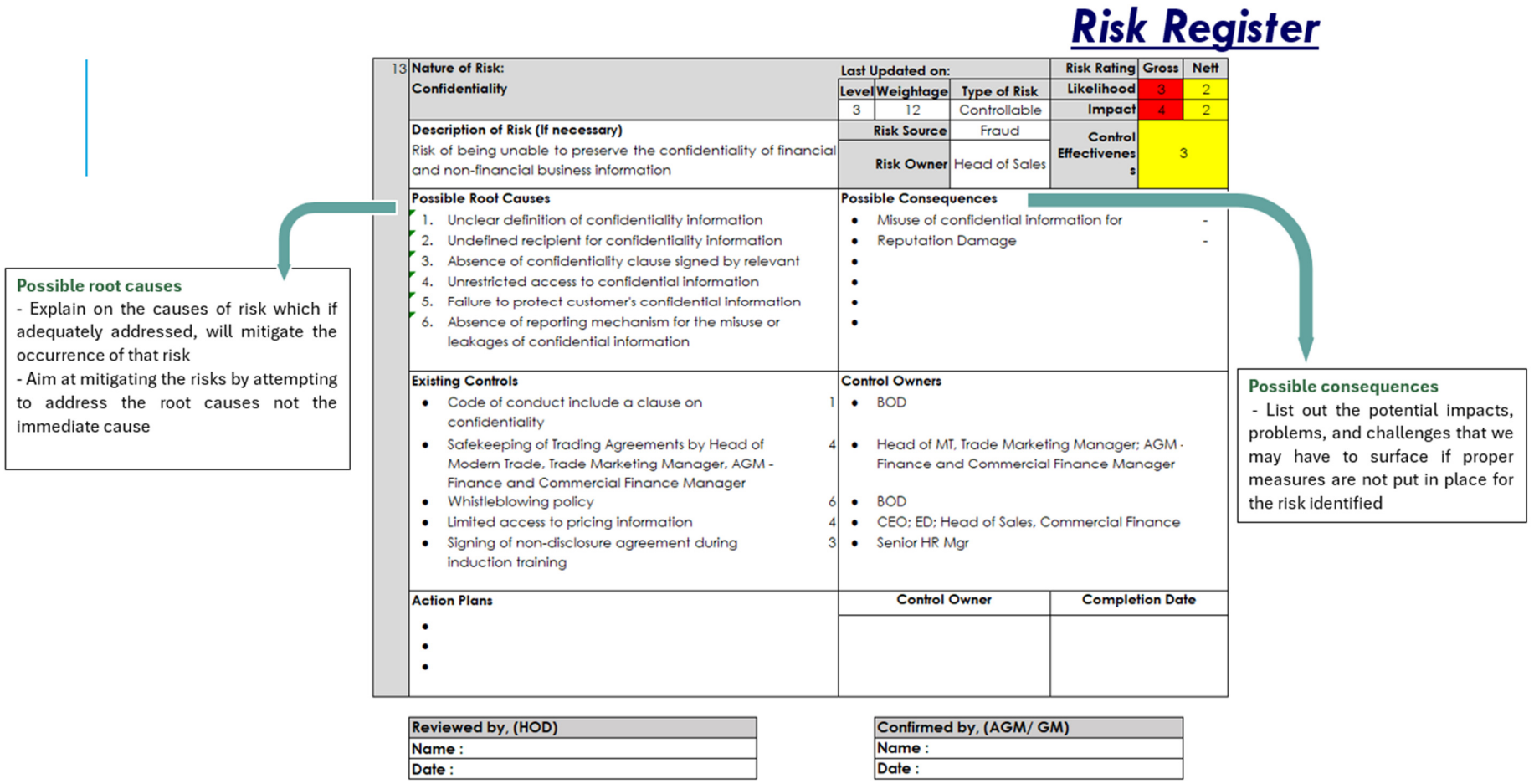
Existing Controls		Control Owners
• Code of conduct include a clause on confidentiality	1	• BOD
• Safekeeping of Trading Agreements by Head of Modern Trade, Trade Marketing Manager, AGM - Finance and Commercial Finance Manager	4	• Head of MT, Trade Marketing Manager; AGM - Finance and Commercial Finance Manager
• Whistleblowing policy	6	• BOD
• Limited access to pricing information	4	• CEO; ED; Head of Sales, Commercial Finance
• Signing of non-disclosure agreement during induction training	3	• Senior HR Mgr

Action Plans	Control Owner	Completion Date
•		
•		
•		

Reviewed by, (HOD)
Name :
Date :

Confirmed by, (AGM/ GM)
Name :
Date :

Appendix A – Risk Register (cont'd)



Risk Register

13	Nature of Risk: Confidentiality	Last Updated on: Level	Weightage	Type of Risk	Risk Rating	Gross	Nett
		3	12	Controllable	Likelihood	3	2
					Impact	4	2
	Description of Risk (If necessary): Risk of being unable to preserve the confidentiality of financial and non-financial business information	Risk Source		Fraud	Control Effectiveness	3	
		Risk Owner		Head of Sales			

Possible Root Causes	Possible Consequences
1. Unclear definition of confidentiality information	• Misuse of confidential information for -
2. Undefined recipient for confidentiality information	• Reputation Damage -
3. Absence of confidentiality clause signed by relevant	•
4. Unrestricted access to confidential information	•
5. Failure to protect customer's confidential information	•
6. Absence of reporting mechanism for the misuse or leakages of confidential information	•

Existing Controls		Control Owners
• Code of conduct include a clause on confidentiality	1	• BOD
• Safekeeping of Trading Agreements by Head of Modern Trade, Trade Marketing Manager, AGM - Finance and Commercial Finance Manager	4	• Head of MT, Trade Marketing Manager; AGM - Finance and Commercial Finance Manager
• Whistleblowing policy	6	• BOD
• Limited access to pricing information	4	• CEO; ED; Head of Sales, Commercial Finance
• Signing of non-disclosure agreement during induction training	3	• Senior HR Mgr

Action Plans	Control Owner	Completion Date
•		
•		
•		

Reviewed by, (HOD)
Name :
Date :

Confirmed by, (AGM/ GM)
Name :
Date :

Possible root causes
- Explain on the causes of risk which if adequately addressed, will mitigate the occurrence of that risk
- Aim at mitigating the risks by attempting to address the root causes not the immediate cause

Possible consequences
- List out the potential impacts, problems, and challenges that we may have to surface if proper measures are not put in place for the risk identified

Appendix A – Risk Register (cont'd)

Risk Register

13	**Nature of Risk:** **Confidentiality**	**Last Updated on:**			**Risk Rating**	**Gross**	**Nett**
		Level	**Weightage**	**Type of Risk**	**Likelihood**	3	2
		3	12	Controllable	**Impact**	4	2
	Description of Risk (If necessary) Risk of being unable to preserve the confidentiality of financial and non-financial business information	**Risk Source**		Fraud	**Control Effectiveness**	3	
		Risk Owner		Head of Sales			
	Possible Root Causes 1. Unclear definition of confidentiality information 2. Undefined recipient for confidentiality information 3. Absence of confidentiality clause signed by relevant 4. Unrestricted access to confidential information 5. Failure to protect customer's confidential information 6. Absence of reporting mechanism for the misuse or leakages of confidential information	**Possible Consequences**					**+/-**
		• Misuse of confidential information for					-
		• Reputation Damage					-
	Existing Controls			**Control Owners**			
	• Code of conduct include a clause on confidentiality	1		• BOD			
	• Safekeeping of Trading Agreements by Head of Modern Trade, Trade Marketing Manager, AGM - Finance and Commercial Finance Manager	4		• Head of MT, Trade Marketing Manager; AGM - Finance and Commercial Finance Manager			
	• Whistleblowing policy	6		• BOD			
	• Limited access to pricing information	4		• CEO; ED; Head of Sales, Commercial Finance			
	• Signing of non-disclosure agreement during induction training	3		• Senior HR Mgr			
	Action Plans			**Control Owner**		**Completion Date**	
	•						
	•						
	•						

Existing Control
- List down on the internal control(s) that are currently in place/ implemented to manage the risks identified
- Specify the **control owner** for each internal control in place/implemented

Reviewed by, (HOD)
Name :
Date :

Confirmed by, (AGM/ GM)
Name :
Date :

Appendix A – Risk Register (cont'd)

Risk Register

13	Nature of Risk: Confidentiality	Last Updated on: Level	Weightage	Type of Risk	Risk Rating	Gross	Nett
					Likelihood	3	2
		3	12	Controllable	Impact	4	2
	Description of Risk (If necessary) Risk of being unable to preserve the confidentiality of financial and non-financial business information	Risk Source		Fraud	Control Effectiveness	3	
		Risk Owner		Head of Sales			

Possible Root Causes	Possible Consequences	+/-
1. Unclear definition of confidentiality information	• Misuse of confidential information for	-
2. Undefined recipient for confidentiality information	• Reputation Damage	-
3. Absence of confidentiality clause signed by relevant	•	
4. Unrestricted access to confidential information	•	
5. Failure to protect customer's confidential information	•	
6. Absence of reporting mechanism for the misuse or leakages of confidential information	•	

Existing Controls		Control Owners
• Code of conduct include a clause on confidentiality	1	• BOD
• Safekeeping of Trading Agreements by Head of Modern Trade, Trade Marketing Manager, AGM - Finance and Commercial Finance Manager	4	• Head of MT, Trade Marketing Manager; AGM - Finance and Commercial Finance Manager
• Whistleblowing policy	6	• BOD
• Limited access to pricing information	4	• CEO; ED; Head Sales, Commercial ance
• Signing of non-disclosure agreement during induction training	3	• Senior HR Mgr

Action Plans	Control Owner	Completion Date
•		
•		
•		

Action Plan
- Based on the possible root cause and consequences of the risk identified, define the action plan(s) that can be implemented in order to mitigate the risk
- **Control owner and estimated completion date** to be updated for the action plan

Reviewed by, (HOD)
Name :
Date :

Confirmed by, (AGM/ GM)
Name :
Date :

Appendix A – Risk Register (cont'd)

Risk Register

13	Nature of Risk: Confidentiality	Last Updated on: Level	Weightage	Type of Risk	Risk Rating	Gross	Nett
		3	12	Controllable	Likelihood	3	2
					Impact	4	2
	Description of Risk (If necessary) Risk of being unable to preserve the confidentiality of financial and non-financial business information	Risk Source		Fraud	Control Effectiveness	3	
		Risk Owner		Head of Sales			
	Possible Root Causes 1. Unclear definition of confidentiality information 2. Undefined recipient for confidentiality information 3. Absence of confidentiality clause signed by relevant 4. Unrestricted access to confidential information 5. Failure to protect customer's confidential information 6. Absence of reporting mechanism for the misuse or leakages of confidential information	**Possible Consequences** • Misuse of confidential information for • Reputation Damage					
	Existing Controls			**Control Owners**			
	• Code of conduct include a clause on confidentiality	1		• BOD			
	• Safekeeping of Trading Agreements by Head of Modern Trade, Trade Marketing Manager, AGM - Finance and Commercial Finance Manager	4		• Head of MT, Trade Marketing Manager; AGM - Finance and Commercial Finance Manager			
	• Whistleblowing policy	6		• BOD			
	• Limited access to pricing information	4		• CEO; ED; Head of Sales, Commercial Finance			
	• Signing of non-disclosure agreement during induction training	3		• Senior HR Mgr			
	Action Plans			**Control Owner**		**Completion Date**	
	•						
	•						
	•						

Control effectiveness
- Based on the **rating category and criteria of control effectiveness stated in slide no. 6,**
- assess on the adequacy and effectiveness of Internal control(s) identified/implemented to manage the risks identified

Reviewed by, (HOD)
Name :
Date :

Confirmed by, (AGM/ GM)
Name :
Date :

Appendix B – SWOT Analysis