



KUMPULAN H & L HIGH-TECH BERHAD

RISK MANAGEMENT POLICY

Version 1.1

Date: 24th December 2021

TABLE OF CONTENTS

POLICY STATEMENT

CORPORATE GOVERNANCE

PURPOSE OF THIS POLICY

POLICY OBJECTIVES

SCOPE OF THIS POLICY

ERM STAKEHOLDERS

RISK MANAGEMENT FRAMEWORK

CONCLUSIONS

DEFINITIONS AND ABBREVIATIONS

APPENDIXES:

A - ERM ROLES AND RESPONSIBILITIES

B - RISK APPETITE AND TOLERANCE

C - RISK UNIVERSE

D - RISK PARAMETERS

E - RISK ASSESSMENT

F - SAMPLE RISK REGISTER AND MONITORING TABLE

G - ILLUSTRATIVE PORTFOLIO VIEW OF RISKS

H - REPORTING REQUIREMENTS & STRUCTURE

POLICY STATEMENT

Kumpulan H & L High-Tech Berhad (“KHLHT” or the “Company”) recognises that commitment to risk management contributes to sound management practice and good corporate governance as it improves decision making and enhances outcomes and accountability. The Management is committed to ‘best risk management practices’ across KHLHT.

The Board of Directors (the “Board”) is accountable to the shareholders of KHLHT for the development and implementation of a risk management framework specific to the organisation’s business and the organisational context. The design of this framework reflects the principles and the process outlined in the *Enterprise-wide Risk Management (“ERM”)*, published in 2004 by the *Committee of Sponsoring Organizations of the Treadway Commission (“COSO”)* and *ISO 31000:2018 Risk Management - Guidelines*.

Risk management is underpinned by the key principle that:

“Risk management contributes to the creation of sustainable value.”

The consistent and systematic application of risk management is central to maximising shareholders value, effectively leveraging the benefit of opportunities, managing uncertainty and minimising the impact of adverse events.

Risk assessment is integrated into planning and all other activities of KHLHT. The risk information obtained is a fundamental consideration in measured risk taking and decision making.

[The remaining of this page is intentionally left blank]

CORPORATE GOVERNANCE

KHLHT is required to include in its annual report, a Statement on Risk Management and Internal Control (“SORMIC”), including how the following broad principles of corporate governance, have been applied:

- The identification and management of risk should be a continuous process linked to the achievement of KHLHT’s objectives.
- The approach to internal control should be risk based including evaluation of the likelihood and impact of risks becoming a reality.
- Risk assessment and internal controls should be embedded in on-going operational procedures.
- The Board via the ARMC should receive regular reports during the year from Senior Management on internal control and risk.
- The principal results of risk assessment, treatment and management review of its effectiveness should be reported to, and reviewed by, the Board.
- The Board acknowledges that it is their responsibility to ensure that a sound system of risk management and internal control is maintained and that it has reviewed the effectiveness of the above process.
- Where appropriate, set out details of actions taken or proposed, to deal with significant internal control issues.

[The remaining of this page is intentionally left blank]

PURPOSE OF THIS POLICY

This policy is a formal acknowledgement of the commitment of KHLHT to risk management. The aim of the policy is not to have risk eliminated completely from KHLHT activities, but rather to ensure that every effort is made by KHLHT to manage risk appropriately to maximise potential opportunities and minimise the adverse effects of risk, when it happens. The policy articulates the organisation's risk management philosophy, the processes and practices that are in place to identify, communicate and manage material risks across the organisation. The policy also ensures that responsibilities have been appropriately assigned for risk management.

The key objective for managing risk in KHLHT is to contribute to sound corporate governance by:

- enabling consistent and systematic risk identification and management strategies to be implemented at all levels of the organisation;
- enabling the identification and implementation of appropriate internal controls;
- improving decision-making processes;
- helping to achieve a balance between realising opportunities to improve shareholders value while minimising the possibility of financial loss or other adverse impacts; and
- assisting with the achievement of the organisation's strategic objectives.

SCOPE OF THE POLICY

Risk is an inherent aspect of all business activities. Sound risk management principles must become part of routine management activity across KHLHT. The Risk Management Policy establishes a mechanism for identifying, analysing, evaluating, treating, monitoring and reporting risks within the organisation.

ERM STAKEHOLDERS

The following list represents internal and external risk management stakeholders that have an interest in KHLHT's performance and the ability to manage risks.

Internal

- The Board
- Audit and Risk Management Committee
- Senior and Middle Management
- Divisional Heads
- Staff
- Internal Auditors

External

- Customers
- Principals, Distributors and Suppliers
- Agents, Third Party Service Providers and Business Partners

- Regulatory Bodies
- Insurance vendors
- External Auditors

RISK MANAGEMENT FRAMEWORK

KHLHT considers risk management to be fundamental to good management practice and a significant aspect of corporate governance. Effective management of risk will provide an essential contribution towards the achievement of KHLHT's strategic and operational objectives and goals.

Risk management forms an integral part of KHLHT's decision making and routine management and are incorporated within the strategic and operational planning processes of KHLHT.

An ongoing risk management communication strategy (depicted in the following diagram) will address how KHLHT will communicate and distribute risk management policies, procedures and key principles on an ongoing basis.



The Audit and Risk Management Committee ("ARMC") reviews the Risk Management Report ("RMR") prepared by the Senior Management. The RMR provides a regular update on risks which the Senior Management views as having potential negative impact on KHLHT's performance. Mitigating actions as well as key indicators (where relevant) measuring the extent of the risks are included as part of the RMR. The ARMC provides feedback and input on the RMR and monitors the mitigating actions taken by the Management. The ARMC reviews the SORMIC and recommends to the Board for approval.

Risk assessments are conducted on all key aspects of the Group, especially on new ventures and activities, including projects, processes, systems and commercial activities to ensure that these are aligned with KHLHT's objectives and goals. Any risks or opportunities arising from these assessments will be identified, analysed and reported to the appropriate management level. KHLHT will maintain a risk register containing strategic and operational risks of the business, including corruption, financial and compliance risks. KHLHT is committed to ensuring that all staff, particularly the Management are provided with adequate guidance on the principles of risk management and their responsibilities to implement risk management effectively.

KHLHT will regularly review and monitor the implementation and effectiveness of the risk management process, including the development of an appropriate risk management culture across KHLHT.

ERM Principles

ERM Implementation for KHLHT shall comply with the following principles: -

i) ERM creates and protects value

ERM contributes to the demonstrable achievement of objectives and improvement of performance in, for example, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance, and reputation.

ii) ERM is an integral part of all KHLHT's processes

ERM is not a stand-alone activity that is separate from the main activities and processes of the organisation. ERM is part of the responsibilities of management and an integral part of all organisational processes, including strategic planning and all project and change management processes.

iii) ERM is part of decision making

ERM helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action. The risk management framework and system are also tools in assisting the decision-making process to assess new investments, projects or initiatives.

iv) ERM explicitly addresses uncertainty

ERM explicitly takes into account of uncertainty, the nature of that uncertainty, and how it can be addressed.

v) ERM is systematic, structured and timely

A systematic timely and structured approach to ERM contributes to efficiency and to consistent, comparable and reliable results.

vi) ERM is based on the best available information

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgments. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

vii) ERM is tailored

ERM is aligned with the organisation's external and internal context and risk profile.

viii) ERM takes human and cultural factors into account

ERM recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organisation's objectives.

ix) ERM is transparent and inclusive

Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organisation, ensures that ERM remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

x) ERM is dynamic, iterative and responsive to change

ERM continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some changes, and others disappear.

xi) ERM facilitates continual improvement of the organisation

Organisations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organisation.

Risk Management Strategy

Policies, procedures, guidelines, templates and the like are being developed to assist in ensuring an awareness of what is an acceptable level of risk and that risks and opportunities are managed consistently and effectively across KHLHT.

Senior Management are required to undertake risk assessments against KHLHT's business plan, strategies and other significant activities and to maintain risk registers that reflect an appropriate risk profile.

There are seven steps to management of risks assessed in the risk registers / profile which consist of:

- i) Identifying the risks to achieving strategic and operational objectives.
- ii) Determining the owner of the risk.
- iii) Assessing the impact and likelihood of the risk before taking account of any existing controls to derive the gross risk.
- iv) Determining and identifying the existing controls in place.
- v) Determining the effectiveness of existing controls in managing the impact and likelihood of the risk.
- vi) Assessing the impact and likelihood of the risk after taking account of existing controls to derive the nett risk.

- vii) Determining additional control improvements / management actions to further manage the risk.

Risk Reporting and Investigation

All new real or potential risks identified are to be recorded and reported to KHLHT's Senior Management at the earliest opportunity. KHLHT's Senior Management should undertake an initial investigation to determine the cause and potential consequences of the risk.

Risk Management as Part of the System of Internal Control

The system of internal control incorporates risk management. This system encompasses a number of elements that together facilitates an effective and efficient operation, enabling KHLHT to respond to a variety of strategic, operational, corruption, financial and compliance risks. These elements include:

i) Strategies, Policies and Procedures

KHLHT has a series of strategies, policies and procedures that underpin the internal control processes. Key strategies and policies implemented and communicated by Senior Management to staffs, including policies and procedures covering:

- Board approved Risk Appetite and Risk Tolerance Statement <Refer to Appendix B for details>;
- Board approved Financial approval limits;
- Finance related policies;
- Operational policies;
- Information Technology (IT) policies; and
- Disaster recovery and business continuity planning.

ii) Planning and Budgeting

KHLHT planning and budgeting process is used to set objectives, agree action plans, and allocate resources. Progress towards meeting planned objectives is monitored regularly.

iii) High Level / Key Risk Registers (Significant / Key Risks only)

KHLHT's key risk register is compiled by the Senior Management and helps to facilitate the identification, assessment and on-going monitoring of risks significant to the organisation, including actions taken to mitigate these risks. The document is formally reviewed periodically but emerging risks are added as required and mitigating actions and risk indicators are monitored regularly and updated on an on-going basis. The key risk registers are discussed at regular meetings of the Senior Management and reported periodically to the Board via the ARMC.

iv) Audit and Risk Management Committee (ARMC)

The ARMC is required to report to the Board on risk management and alert the Board of any emerging issues. The committee is therefore well-placed to provide advice to the Board on the effectiveness of KHLHT's system for the management of risk.

v) Internal Audit Programme

At present, the Internal Audit function is outsourced to professional consulting firm(s). The internal audit function adopts a risk-based approach to its work with the overall objective of evaluating and improving the effectiveness of KHLHT's risk management, internal control, whistle-blowing, anti-corruption and governance processes.

vi) External Audit

In addition to the statutory audit of the financial statements, external audit also provides feedback to the ARMC on the operation of the internal controls reviewed as part of their annual audit.

vii) Third Party Reports

From time to time, the use of external consultants may be necessary in specialist areas of KHLHT's operations. The use of specialist third parties for consulting and reporting can increase the reliability and integrity of the internal control system.

RISK MANAGEMENT FRAMEWORK (Cont'd)

Yearly Review of Effectiveness

The Board via the ARMC is responsible for reviewing the effectiveness of risk management framework of KHLHT, based on information provided by the Senior Management. Its approach is outlined below:

i) For each fundamental risk identified, the Board via the ARMC will:

- review the previous year and examine KHLHT's track record on risk management and internal controls; and
- consider the internal and external risk profile of the coming year and consider if current internal control arrangements are likely to be effective.

ii) In making its decision the Board via the ARMC will consider the following aspects:

- Control environment (e.g., the Company's business strategies, culture and organisation structure).
- On-going identification and evaluation of fundamental risks.
- Information and communication (e.g., time taken for control breakdowns to be recognised or new risks to be identified).
- Monitoring and corrective action (e.g., commitment and speed of which corrective actions are implemented).

CONCLUSIONS

In today's environment of change and uncertainty, risk management is a critical success factor for achieving KHLHT's strategic and operational goals. Embedding risk management into existing processes is a key to making informed decisions and proactively planning for possible future events stemming from internal as well as external sources.

The implementation of an effective ERM process is a strategic initiative that has the full support of KHLHT's Board and Senior Management.

Risk management is everyone's responsibility. KHLHT's ERM Framework provides a proactive, systematic and integrated approach to risk management. The principles outlined in the Framework are the foundation for the risk management objectives of KHLHT ERM initiative.

DEFINITIONS AND ABBREVIATIONS

ARMC	Audit and Risk Management Committee
KHLHT	Kumpulan H & L High-Tech Berhad
ERM	Enterprise-wide Risk Management
ISO	International Organisation for Standardisation
RMR	Risk Management Report
SORMIC	Statement on Risk Management and Internal Control
The Board	The Board of Directors

APPENDIX A

ERM ROLES AND RESPONSIBILITIES

ERM ROLES AND RESPONSIBILITIES

ERM roles and responsibilities of Stakeholders	ERM Role	Key ERM Responsibilities
The Board	Risk Management Philosophy	<p>Oversight of the Group ERM Framework/ Process:</p> <ul style="list-style-type: none"> • Approve the Group ERM Framework, (incorporating policy and process), including changes or additions. <p>Monitor the ERM process and associated risks:</p> <ul style="list-style-type: none"> • Review and approve the yearly enterprise-wide risk assessment including effectiveness of management's responses/ mitigation of key risks. • Review KHLHT's enterprise-wide portfolio of risk, evaluate against risk appetite and consider impact of business strategy and organisational changes. • Approve action on new risks identified that could have a significant strategic, financial or reputational impact.
Audit and Risk Management Committee (ARMC)	Risk Management Oversight and Control	<ul style="list-style-type: none"> • Review KHLHT's ERM Framework (incorporating policy and process), including changes or additions. • Ensure that Senior Management creates and maintains an effective process to identify, evaluate and manage risk. • Provide guidance in respect of risk management and support management in the monitoring of risk across KHLHT. <p>Monitor the ERM process and associated risks</p> <ul style="list-style-type: none"> • Review and validate prioritised risks identified, risk profile and risk registers and evaluate against risk appetite. • Monitor effectiveness of management's responses/ mitigation of key risks. • Review significant events, performance surprises and incidents and understand root cause and required actions. • Review new risks that could have a significant financial, strategic, operational, compliance or reputational impact and escalate to the Board as appropriate.

ERM roles and responsibilities of Stakeholders	ERM Role	Key ERM Responsibilities
Audit and Risk Management Committee	Oversight of Independent ERM Review	<ul style="list-style-type: none"> • Approve the scope and approach of the independent evaluation of the ERM process. • Review the independent report regarding the effectiveness of the overall ERM process and monitor corrective actions. • Report evaluation findings to the Board and recommendations to improve KHLHT's ERM process.
Senior Management / Divisional Heads	<p>Risk Management Approach, Strategy and Directives</p> <p>Risk Management Implementation</p>	<p>Develop, Implement and sustain KHLHT's ERM Framework:</p> <ul style="list-style-type: none"> • Assist in establishing the appropriate tone at the Senior Management level to implement an effective ERM process. • Integrate risk management into objective and strategic goal setting processes. • Provide input into the development of the ERM framework and policy including: <ul style="list-style-type: none"> - Risk management responsibility and accountability; - Risk appetite and risk tolerance; - Risk rating parameters; etc. • Identify and prioritise risks on an on-going basis. Ensure risks are identified, managed and regularly assessed and that controls are operating effectively. • Execution of risk treatment activities consistent with risk appetite and tolerance, where applicable. • Identify and provide sufficient level of resources to ERM and ensure succession planning for continuity. Review significant events, performance surprises and incidents to understand root cause and required actions. • Identify and/or consider new risks on an ongoing basis that could have a significant financial, strategic, operational, compliance or reputational impact and escalate to the ARMC. • Consider high impact/ low likelihood risks (time bombs) and ensure appropriate internal controls are in place. Ensure ongoing monitoring/ testing thereof through assurance providers if necessary.

ERM roles and responsibilities of Stakeholders	ERM Role	Key ERM Responsibilities
		<ul style="list-style-type: none"> • Prepare the RMR that provides a regular update on risks as well as key risk indicators measuring the extent of the risks.
Internal Auditor	Independent ERM / Internal Control Review	<p>Evaluate the ERM process and internal controls:</p> <ul style="list-style-type: none"> • Evaluate the effectiveness of KHLHT's Risk Management processes and associated controls, monitor compliance with the framework and provide independent assurance to the Board/ Risk Management on the effective operation thereof. • Provide input into the control effectiveness ratings. <p>Reporting, communication, and change management:</p> <ul style="list-style-type: none"> • Report evaluation findings to the ARMC and recommendations to improve the Group ERM process. ▪ Report the results of internal audit to the Risk Management Function to enable the Senior Management to determine the control effectiveness rating.
External Auditor	Independent ERM / Internal Control Review	As required by the Listing Requirement, the External Auditor reviews the Statement on Risk Management & Internal Control for inclusion in the Annual Report.

APPENDIX B

RISK APPETITE AND RISK TOLERANCES

RISK APPETITE AND RISK TOLERANCES

Risk Appetite

Risk appetite is the amount of risk that KHLHT is *willing to accept* in pursuit of the achievement of its goals, which provides a basis to create and sustain value. Risk appetite is an important, forward-looking perspective because it:

- serves as a guide to KHLHT as to how much risk is acceptable;
- is used as a benchmark during the strategy and goal setting process; and
- sets stakeholder expectations with regards to the level of risk that KHLHT is willing to undertake.

The risk appetite will need to be re-evaluated:

- as part of the annual strategic planning cycle and goal setting processes;
- when significant changes are made to KHLHT organisation (mergers, restructuring, etc.);
- when changes are made to the overall strategy and goals of KHLHT;
- with changes in the business and economic landscape; and
- with changes in expectations and risk preferences of key stakeholders.

Risk appetite is developed at the entity level by the Senior Management and proposed to the Board, through the Audit and Risk Management Committee, for approval. Once approved, it is the responsibility of the Board and the Senior Management to communicate the entity's risk appetite to the Group staffs and key stakeholders (as deemed necessary).

The Group's risk appetite has been stated in the following table:

Risk appetite categories	Risk Appetite
Strategic	The Group will accept a moderate level of risk for current / new strategic initiative that is in alignment with the Group long-term goals.
Compliance	The Group will not tolerate non-compliance with any legal or regulatory requirement.
Financial	The Group will not tolerate non-compliance with financial reporting standards. The Group will accept a low level of risk for financial related procedures other than financial reporting standards.
Operational	The Group will accept a low level of risk for operational related procedures.

Risk Appetite (Cont'd)

Once risk appetite has been determined by the Senior Management, it is communicated to the middle management and considered during their goal setting processes.

Risk Tolerance

Risk tolerance is quantifiable measures of the risk appetite statements which state the limits of risk capacity the Board of Director of the organisation is willing to take. Setting risk tolerance limits allow the company to have a solid standard and target in managing and monitoring the risks from an overall perspective.

As part of the goal setting process, the Senior Management determines the Company's target and objectives (i.e., annual sales growth, Earnings Before Interest & Tax ("EBIT") sustained, Returns on Asset Employed, Working Capital ratio, etc.) on a yearly basis.

APPENDIX C

RISK UNIVERSE

RISK UNIVERSE

Risks identified will be grouped into similar types of risk called “risk universe”. The risk universe is aligned to KHLHT’s strategic goals, and will facilitate the coordinated management of risk across KHLHT.

The risk universe to be used to group risks is as follows:

Risk Universe	Risk Areas	
a) Strategic	<ul style="list-style-type: none"> ➤ <u>External</u> <ul style="list-style-type: none"> • Industry • Economy • Political change • Competitor • Customer preference 	<ul style="list-style-type: none"> ➤ <u>Internal</u> <ul style="list-style-type: none"> • Market Share • Reputation • Brand equity • Strategic focus • Investor confidence
b) Compliance	<ul style="list-style-type: none"> ➤ <u>Legal</u> <ul style="list-style-type: none"> • Contract Approval • Litigation Management • Intellectual Property • Whistle Blowing • Corruption ➤ <u>Code of Conduct</u> <ul style="list-style-type: none"> • Policies & Procedures 	<ul style="list-style-type: none"> ➤ <u>Regulatory</u> <ul style="list-style-type: none"> • All relevant Acts • Listing Requirements • Environmental • Corporate Governance • Financial Reporting • Licensing
c) Financial	<ul style="list-style-type: none"> ➤ <u>Treasury</u> <ul style="list-style-type: none"> • Cash Flow / Liquidity • Capital Availability • Interest Rate • Foreign Exchange ➤ <u>Finance</u> <ul style="list-style-type: none"> • Accounting • Budgeting • Taxation 	<ul style="list-style-type: none"> ➤ <u>Credit</u> <ul style="list-style-type: none"> • Credit Capacity • Credit Concentration • Credit Default

Risk Universe	Risk Areas
d) Operational	<div data-bbox="448 271 901 448"> <p>➤ <u>Sales & Marketing</u></p> <ul style="list-style-type: none"> • Product Marketing • Product Design • Sales Commission • Customer's satisfaction </div> <div data-bbox="448 555 901 1153"> <p>➤ <u>People / Human Capital</u></p> <ul style="list-style-type: none"> • Succession Planning • Recruitment • Retention • Integrity / Competencies • Leadership / Empowerment • Training • Culture • Performance Evaluation • Knowledge Capital • Employee Satisfaction / Morale / Behaviour • Incentive & Remuneration • Communication • Social: Community support & volunteerism </div> <div data-bbox="448 1200 798 1377"> <p>➤ <u>Hazards</u></p> <ul style="list-style-type: none"> • Third Party Liability • Health & Safety • Natural Hazards • Property Loss </div> <div data-bbox="927 271 1364 515"> <p>➤ <u>Supply Chain</u></p> <ul style="list-style-type: none"> • Sourcing • Supplier Contractor Concentration • Supplier Management • Inventory Management • Quality Control </div> <div data-bbox="927 555 1364 974"> <p>➤ <u>Information Technology</u></p> <ul style="list-style-type: none"> • IT Strategy / Planning • System Implementation & Integration • Maintenance • Network Administration (Security / Privacy) • Business Continuity Planning (Disaster Recovery) • Information / Records Management </div> <div data-bbox="927 1200 1340 1444"> <p>➤ <u>Facilities management and administration</u></p> <ul style="list-style-type: none"> • Business Interruption • Safeguarding & Security • Asset Management • Maintenance • Insurance </div>

APPENDIX D

RISK PARAMETERS

RISK RATING CRITERIA – LIKELIHOOD

Score	Rating	Description
5	Very High	• 81-100% chance of occurrence
		• Almost certain to occur within the next 3 months
4	High	• 61-80% chance of occurrence
		• The risk is likely to occur within the next 6 months
3	Medium	• 41-60% chance of occurrence
		• The risk could occur at least once in the next 1 year
2	Low	• 21-40% chance of occurrence
		• The risk could occur at least once in the next 1 to 3 years
1	Very Low	• Less than 20% chance of occurrence
		• Unlikely to occur in the next 3 years or more

RISK RATING CRITERIA – IMPACT

Impact Rating		Quantitative	Qualitative					
		Financial	Business Interruption	Business Strategies	Reputation	Stakeholders' Confidence	Safety, Health & Environment (SHE)	Human Resources
5	Very Significant	Financial loss of above RM800,000	Severe business disruption (>10 weeks)	Failure to meet key strategic objectives	Very significant reputation impact	Catastrophic loss of stakeholders' confidence	Continuous closure of premises	Significant morale issues and loss of productivity
4	Major	Financial loss of RM500,001 – RM800,000	Major business disruption (6 to 10 weeks)	Major impact on business strategies	Adverse Reputation damages	Major loss of stakeholders' confidence	Temporary closure / suspension of premise by regulators	Major morale issues and loss of productivity
3	Moderate	Financial loss of RM300,001 – RM500,000	Moderate business disruption (3 to 5 weeks)	Moderate impact on business strategies	Some damage to reputation	Concern from stakeholders	Continuous warnings received from regulators / authorities	Some morale issues and loss of productivity
2	Minor	Financial loss of RM100,001 – RM300,000	Some business disruption (1 to 2 weeks)	Minor impact on business strategies	Minimal reputation sensitivity	Minimal concern from stakeholders	Complaints by 3rd party and/or first warning received from Regulators / authorities	Short term staff morale issues and loss of productivity
1	Insignificant	Financial loss of RM100,000 or less	Minimal business disruption (< 1 week)	No impact on business strategies	No reputation damage	No concern from stakeholders	Minor complaints / feedback	No effect on staff morale

CONTROL EFFECTIVENES RATING CRITERIA

Control Effectiveness can be segregated as follows:

- **Effectiveness of Control to Reduce Likelihood** - This is defined by how well the controls in place decrease the likelihood of a risk occurring (i.e., Preventive controls and detective controls where avoidance is possible). When evaluating the effectiveness of controls, ratings have taken into account the degree of Compliance.
- **Effectiveness of Control to Reduce Impact** - This control is defined by how well the controls in place decrease the impact where the risk has occurred (i.e., primarily corrective controls. May include detective controls where further damage may be minimised). When evaluating the effectiveness of controls, ratings have taken into account the state of Compliance.

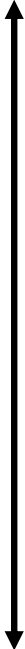
Score	Rating	Description
5	Very Good	Controls are strong and very robust. Compliance is in place. Management is fully committed and competent in managing risks.
4	Good	Controls are sufficiently robust and operating effectively. Compliance is generally in place.
3	Satisfactory	Controls and compliance are generally in place. Minimum control issues.
2	Needs Improvement	Some control weakness / non-compliances have been identified. Although there are not considered to present a serious risk exposure, improvements are required to provide reasonable assurance that objectives will be achieved.
1	Poor	Controls do not meet an acceptable standard, as many weaknesses exist. Controls do not provide reasonable assurance that objectives will be achieved. There is a high degree of non-compliances.

APPENDIX E

RISK ASSESSMENT

RISK ASSESSMENT

The impact and likelihood scores combined determine the priority of risks and what risks are reported at the entity level. This also provides an indication of the exposure of KHLHT to risks being the likelihood plus the impact rating:

		Residual Risk Scoring							Risk Level	
Likelihood	Very High (5)	6	7	8	9	10		High	QA	Very High
	High (4)	5	6	7	8	9			QB	High
	Medium (3)	4	5	6	7	8			QC	Medium
	Low (2)	3	4	5	6	7			QD	Low
	Very Low (1)	2	3	4	5	6			Low	QE
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Very Significant (5)				
		Impact								

The risk assessment process shall take into account both financial and non-financial aspects and it involves the following steps: -

1) Analyse Gross Risk Rating

The Gross Risk Rating is essentially made up as follows:

$$\text{Gross Risk Rating} = \text{Gross Possibility} + \text{Gross Impact}$$

Gross rating reflects the maximum exposure in the event of inadequacy or failure of controls i.e., “worst case scenario”. The gross rating score is intended to reflect the risk of the event occurring (e.g., the likelihood and impact of the risk) if KHLHT was to carry on the business without the benefit of any specific risk analysis, external assistance, management action or risk transfer in the form of insurance, sub-contracting, etc.

Gross Possibility is to determine the likelihood of the risk occurring. When making this determination, consideration should be given to factors such as:

- **Nature of the business environment;**
- **Culture of the organisation;**
- **History of the risk occurrence;**
- **The expectation of the risk occurring; and**
- **The perceived frequency of the risk occurring (particularly in the case of future strategies).**

Gross Impact is the evaluation of the consequences of the risk. The impact rating can be made on the basis of both quantitative and/or qualitative measure.

For each risk, Management needs to decide if a risk is a time bomb. Time bomb is defined as potential catastrophic risk which may affect the organisation. This is the watch list for potential risks, which may currently be well managed, but may create significant problems for the organisation in the future. As such, a risk may be rated as having a low score (i.e., low likelihood with significant impact), but because of its potential implications, be classified as a time bomb.

2) Analyse Existing Control Effectiveness

This step is to identify the key existing controls relating to the identified risks in the categories of preventive, detective and corrective controls.

Types of Control	Description
Preventive	Controls to prevent the risk from occurring.
Detective	<p>There are 2 aspects to detective controls:</p> <ul style="list-style-type: none">• to identify impending risks which are about to take place; thereby, enabling awareness of risks; and• to identify unfortunate events as soon as possible to prevent further deterioration. This reduces impact.
Corrective	After the risks have taken place, the control to minimize losses and to enable recovery to take place promptly.

The effectiveness of the controls is assessed in terms of their design strength and the overall effectiveness in reducing the gross risk to nett risk.

3) Analyse Nett Risk Rating

$$\text{Nett Rating} = \text{Gross Rating} - \text{Overall Control Effectiveness}$$

The rating is a combination of the gross risk rating and the control effectiveness rating. Once the Nett rating of each risk has been obtained, target rating should be considered accordingly. This is critical as KHLHT clarifies the acceptable risk exposure, and in which area it would be inefficient or not cost effective to manage.

Target rating represents the nett position that is considered acceptable or tolerable risk exposure by management on specific risk. Target setting approach enables a direct comparison between the nett status and the ideal scenarios. These may be one of the followings:

- **The risk is within acceptable parameters**
- **The risk may need improvement**
- **The risk may be over-controlled**

Using this approach will provide a solid base for determining whether further management action is required.

a) Risk Treatment

Risk treatment is the process of formulating, selecting and implementing control measures to modify the risk according to the organisation's risk appetite. It can be of the following four (4) options: -

- **Tolerate / Accept: Risk is accepted, and controls are sufficient**
- **Treat / Reduce: Risk is accepted but controls are required to minimize risk likelihood and / or impact**
- **Transfer: Risk is accepted but function is to be outsourced or transferred to other party**
- **Terminate / Avoid: Risk is unacceptable and to be terminated / avoided**

APPENDIX F

SAMPLE RISK REGISTER

SAMPLE RISK REGISTER AND MONITORING TEMPLATE

The risk register is compiled using the outputs of event identification, risk assessment and risk treatment steps in the framework. It is used to record all the risks identified by Management that could impact the attainment of KHLHT's strategic goals, the inherent risk ratings decided upon and the appropriate risk response taking into account KHLHT's risk appetite. It also provides for Management to record the management actions and controls it has in place to mitigate the identified risks and serves as an action registry for those areas where there are gaps in the controls implemented.

Risk Register

No.	Risk Category	Risk Type	Risk Factor	Risk Owner	Causes	Consequences	Gross		Gross Risk (GL + GI)	Existing Controls	Control Owner	Control Effect'		Nett		Nett Risk (NL + NI)
							Likelihood (GL)	Impact (GI)				Likelihood (LCE)	Impact (ICE)	Likelihood (NL)	Impact (NI)	

Notes	
No.	Running number of risks (i.e., 1, 2, 3, 4...)
Risk Category	<p>The risks as classified as per the business activities of KHLHT and provides a structured overview of the underlying and potential risks faced by KHLHT. We categorize our risks based on commonly used risk classifications:</p> <ul style="list-style-type: none"> Strategic risk Changes in the business environment with potentially significant effects on operations and business objectives. For examples, customer behavior, competitors, brand positioning, etc.

Notes	
	<ul style="list-style-type: none"> • Compliance risk Threats posed to a company's financial, organizational, or reputational standing resulting from violations of laws, regulations, codes of conduct, or organizational standards of practice. • Operational risk Operational risks can be defined as the risks of loss arising from improper implementation of processes, external issues (e.g., government regulations, non-performance vendors), etc. Operational risks can be better understood as a type of risk due to inefficiencies in business operations carried out by an organization. • Financial risk Financial risks with a potential impact on financial position and performance, such as, credit risk, liquidity risk, interest rate risk, etc.
Risk Type	<p>There are 2 types of risks:</p> <ul style="list-style-type: none"> • Inherent risk Risk arises nature of business model / operation which is an independent condition to KHLHT, and KHLHT has no control over it to prevent it from happening. • Controllable risk Risk arises from loss arising from events which can be managed / prevented, be it a process / condition within the organisation or any stakeholders which KHLHT has control over.
Risk Factor	Brief description of the risk identified.
Risk Owner	Refers to the designated personnel / position within the organisation accountable to manage the risk.
Causes	The root causes which potentially contribute to the happening / likelihood of the risk.
Consequences	Refers to the probable outcome / threat to the organisation. A consequence can be quantifiable / qualitative and direct / indirect.
Gross Likelihood (GL)	Refers to chance of something happening without considering the effectiveness of internal controls / in its inherent nature. It is analysed using the risk parameters (Appendix D), throughout a defined period of time.

Notes	
Gross Impact (GI)	Refers to magnitude / damage of the event without considering the effectiveness of internal controls / in its inherent nature. It is analysed using the risk parameters (Appendix D), throughout a defined period of time.
Gross Risk (GL + GI)	Refers to the combination of the likelihood of the risk happening and the impact of the consequences suffered by the organisation without considering the effectiveness of internal controls / in its inherent nature. These are the worst-case scenario. Gross Risk = Gross Likelihood + Gross Impact
Existing Controls	Refers to internal control measures currently implemented within the organisation to manage the identified risk.
Control Owner	Refers to the designated personnel / position within the organisation accountable / responsible to execute and monitor the control activities.
Likelihood Control Effectiveness (LCE)	Refers to measures that eliminate or reduce the chances of the risk happening .
Impact Control Effectiveness (ICE)	Refers to measures that reduce the magnitude / damage of the risk which has happened .
Nett Likelihood (NL)	Refers to the chance of the risk happening after considering the effectiveness of existing internal controls. Nett Likelihood = Gross Likelihood – Likelihood Control Effectiveness
Nett Impact (NI)	Refers to magnitude / damage of the event after considering the effectiveness of existing internal controls. Nett Impact = Gross Impact – Impact Control Effectiveness
Nett Risk (NL + NI)	Refers to the current condition / risk position of KHLHT after considering the effectiveness of internal controls. Nett Risk = Nett Likelihood + Nett Impact

APPENDIX G

ILLUSTRATIVE PORTFOLIO VIEW OF RISKS

ILLUSTRATIVE PORTFOLIO VIEW OF RISKS

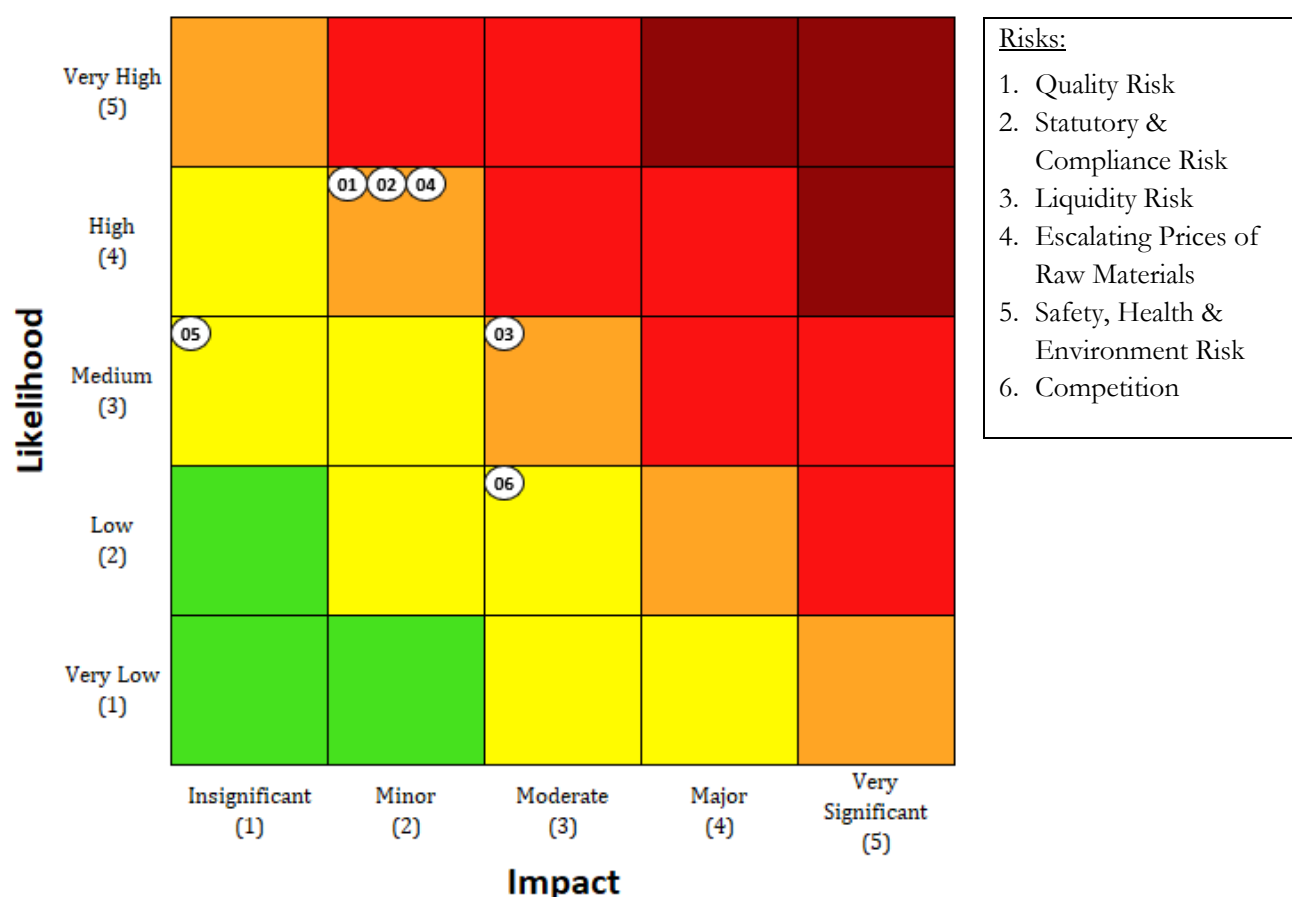
From the information in the risk register, it is possible to categorise and aggregate the risks in order to provide management with a portfolio view of risks. Possible alternatives in presenting a portfolio view include the following:

- Risk profile of risk categories at the Company level;
- Risk profile by strategic goal at the Company level;
- Risk profile of Company level;
- Risk profile of risk owners at the Company level; and
- Risk profile of top 10 risks at the Company level.

Risk profiles can be presented at a gross or a nett risk basis and can also reflect the movement of risk ratings over a period of time.

One example of how this information can be presented graphically is included below. Such a graphical representation allows management to obtain a “snapshot” view of the risks facing the Group and identify those risk categories that are outside of the Group’s risk appetite.

(Illustrative example only)



APPENDIX H

REPORTING REQUIREMENTS & STRUCTURE

REPORTING REQUIREMENTS

Type of Risk Management Information	Reporting Responsibility	Timing	Format of Report	Forum of Discussion & Evaluation
The Board				
<p>Key risk management issues & related actions arising from the Audit and Risk Management Committee reviews including:</p> <ul style="list-style-type: none"> • Reports on the ongoing operation of the risk management process and reviews on the effectiveness thereof. • Prioritized updated risk register and monitoring report for key risks. • Updated enterprise risk profile and broad strategies for risk responses. 	Audit and Risk Management Committee	Yearly	Risk Management Report	Board Meeting
Audit and Risk Management Committee				
<p>Prioritized updated risk register and monitoring report for key risks.</p> <p>Updated enterprise risk profile and broad strategies for risk responses.</p> <p>Performance surprises/ significant incidents, the cause and corrective action.</p> <p>Summary of significant issues raised in reports from assurance providers (regulatory bodies, internal audit), the cause of non-compliances and corrective action.</p>	Senior Management	Yearly	Risk Management Report	Audit and Risk Management Committee

Senior Management				
Updated key risk register (Company/ Department and enterprise).	Divisional Heads and Risk Owners	Yearly	Risk Register	Informal discussion
Performance surprises/ significant incidents, the cause and corrective action.	Divisional Heads and Risk Owners	Immediate	Risk Register	Informal discussion
Identification of new risks that could have a significant financial, strategic, operational or reputational impact.	Divisional Heads and Risk Owners	Immediate	Ad-hoc report on significant risk arising	Informal discussion

REPORTING STRUCTURE

