



A Member of **kps** Group

**CENTURY BOND BHD.**

**Reg. No. : 199101018358 (228669-V)**

**ENTERPRISE RISK MANAGEMENT  
POLICY  
VERSION 2/2022**

TO BE APPROVED BY CBB BOARD on :-

22 Sept 2022



A Member of **kps.** Group

<b>Document Reference Number</b>	<b>RMD/Policy/Risk/ERM/V2</b>
Date	
Title	ENTERPRISE RISK MANAGEMENT POLICY
Author	Associate Director, Risk Management
Owning Department	Risk Management Department
Version	2
Approval Date	22 Sept 2022
Review Date	Version 1 : 11 November 2020
Approving Body	CBB Board of Directors

## TABLE OF CONTENTS

### **CONTENTS**

### **PAGE**

### **POLICY**

1.	Purpose statement	3
2.	Introduction	4
3.	Objectives of the Policy	6
4.	ERM Policy Statement	6
5.	Guiding Principle	7
6.	ERM Framework	9
7.	ERM Reporting & Monitoring Structure	22
8.	Exceptions	25
9.	Appendices	26

## 1.0 PURPOSE STATEMENT

In achieving its vision and mission, CBB is facing with numerous uncertainties and risks - both internally and externally driven. The emergence of e-commerce, globalisation, connected economy, technological innovation, industry consolidation and other factors are causing the business environment to become complex and unique. This increasingly unique business landscape has created a range of equally complex and interrelated risks. Ineffective assumption management of these uncertainties could result in wrong decision made, strategic missteps, operating losses, asset failures and litigation, all of which could have significant impact on shareholder value and return on equities. The Board of Directors ("the Board") of KPS are closely examining the effectiveness of risk management activities group wide, with the aim of providing a consistent and practical approach to risk management.

Bearing this in mind, KPS continuously seeks to strengthen its enterprise risk management practices - the adoption of this Enterprise Risk Management ("ERM") Policy and Framework throughout all subsidiaries is key initiative in this direction. The ERM Policy and Framework aims to assist CBB by providing a structured process for risk management and promoting a risk-based decision-making environment. This ERM Policy and Framework also provide the starting point in the enterprise risk management practices as to ensure that risk management becomes the mindset of everyone in CBB and the application of standard or practices are consistent across the whole of CBB. The ERM Policy and Framework consists of the following key elements (further elaborated in the proceeding sections of this document):

- 1.1 An ERM Policy which sets out CBB's definition of risk, enterprise risk management and key principles that all divisions, departments, subsidiaries and associate must adhere to;
- 1.2 An ERM Framework which sets out the foundations and arrangements that CBB will adopt in consistent with the ISO31000:2018, Risk Management Guidelines in embedding risk management processes throughout CBB at all levels.
- 1.3 An ERM Reporting and Monitoring Structure which facilitates the process of communicating risk related information and ensuring effective oversight of risks and risk management activities throughout the organisation; and
- 1.4 Structured ERM processes that are consistent with the ISO31000:2018 - Risk Management Guidelines tailored to suit CBB risk appetite.

Most importantly, risk management is an integral component of CBB and subsidiaries where all employees must be responsible and take ownership managing risks in performing daily activities. The ERM Policy and Framework is prepared to ensure that risk management becomes a primary concern in all decision making process throughout the organisation.

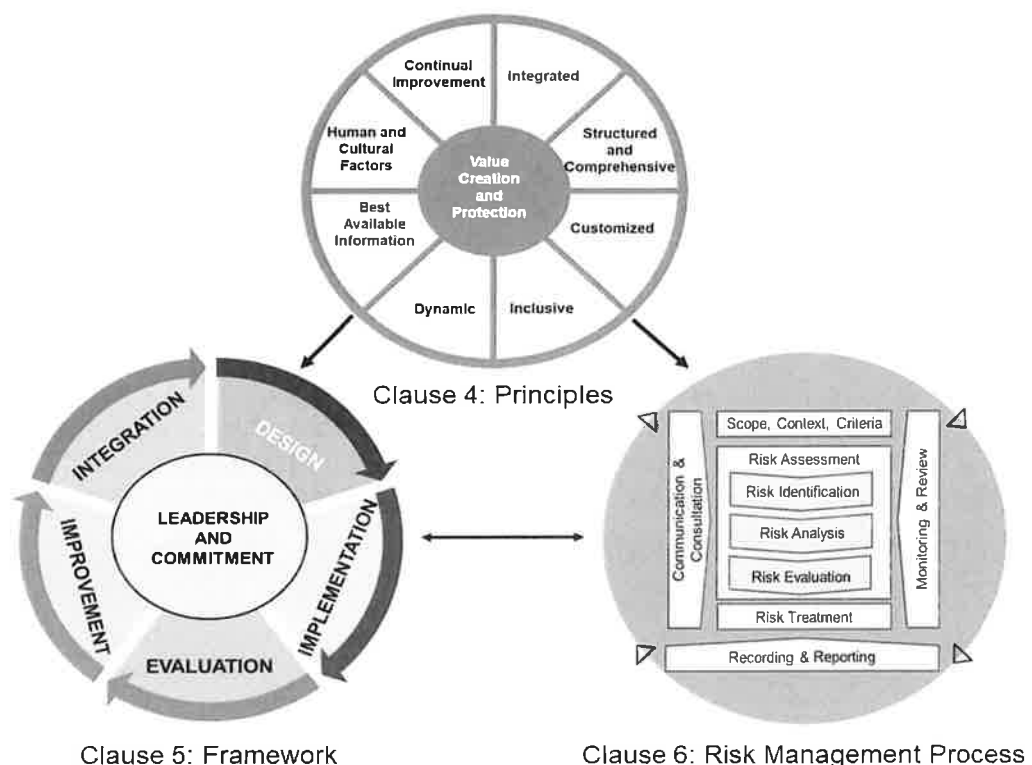
## 2.0 INTRODUCTION

### 2.1 Purpose

The purpose of this Policy is to adopt and implement ERM Policy and Framework within CBB and subsidiaries. It prescribes a comprehensive risk management approach, guidelines and methodology used in identifying and assessing risks, which will serve as tools in making decision.

The following diagram are key elements of CBB's ERM Policy and Framework adopted from ISO31000:2018 Risk Management Guideline:

**Diagram 1: ISO31000:2018 Risk Management Principles, Framework and Process**



### 2.2 Scope

This Policy applies to CBB collectively for implementing the ERM policy.

### 2.3 Responsibility

The Risk Management Department ("RMD") is responsible for the development and maintenance of this document including any reviews, changes, amendments, additions or deletions of any clauses.

### 2.4 Approving Authority

The Board of Directors of CBB ("CBB Board") is the approving authority of this Policy document.

## **2.5 Date of Implementation of the Policy**

The policy will be implemented immediately once approval is obtained from CBB Board.

## **2.6 Review frequency**

The policy will be reviewed every three (3) years at the latest, at a minimum to ensure that it remains consistent with the overall objectives of the Company.

## **2.7 Reference**

This Policy document is to be read in conjunction with all the other relevant policies and internal procedural documents which include, but not limited to the following documents:

- 2.7.1 KPS Board Charter.
- 2.7.2 Terms of Reference of the KPS Board Governance and Risk Committee.
- 2.7.3 Enterprise Risk Management Standard Operating Procedures.
- 2.7.4 Risk Management – Principles and Guidelines ISO 31000:2018.
- 2.7.5 Malaysian Code on Corporate Governance (MCCG) 2021 – Principle B II – Risk Management and Internal Control Framework.
- 2.7.6 CBB Procurement Policy.
- 2.7.7 MCCG Practices:
  - 2.7.7.1 Practice 10.1;
  - 2.7.7.2 Practice 10.2; and
  - 2.7.7.3 Practice 10.3 (Step-up).

## **2.8 Definition**

The key terms and acronyms appeared in this document shall be defined as **Appendix I.**

### **3.0 OBJECTIVES OF THE POLICY**

The main objectives of this Policy are to:

- 3.1** Keep the Board of CBB informed and advised of all aspects of ERM and significant key risk areas and emerging risk as the need arises;
- 3.2** Continuously enhance the risk awareness and understanding amongst CBB's Senior Management and staff;
- 3.3** Provide guidance for effective implementation of ERM in CBB and subsidiaries ; and
- 3.4** Embedded into the day-to-day decision making process.

### **4.0 ERM POLICY STATEMENT**

Risk management shall be integrated into CBB's management philosophy. CBB Board and Management of CBB shall take ownership in implementing the risk management policy which is aligned with the CBB and KPS corporate objectives.

This Risk Management Policy ("the Policy") shall be adopted and communicated appropriately to all levels within CBB. This Risk Management Policy addresses the following:

#### **4.1 To embed risk management processes into all policies and procedures.**

Better business decision can be made with in-depth risk consideration. All critical processes such as budgeting, forecasting, , procurement must consider risk information.

#### **4.2 To identify, assess and analyze both risks and opportunities.**

To ensure all key assumptions are investigated and checked subsequently linking it with mitigation plans. All assumptions made need to be tested with simulation to show effective answer for decision made. While simulation are tested, any opportunities found are to be optimized in maximizing shareholders' wealth.

#### **4.3 To embrace greater transparency culture**

Risk management helps to improve planning process, budgeting, operation strategy, compliance and decision-making quality hence supports greater transparency culture which is expected from regulators, auditors and other stakeholders. Arising for greater transparency culture, a better cost saving could be achieved.

#### **4.4 To ensure that risk assessment is being performed and embedded in the system.**

All key approvals, significant decision via system must include a risk assessment and that risk assessment should be part of the system.

**4.5 To adapt an effective and formalised risk management framework in CBB and subsidiaries**

Establish, implement and maintain adequate risk management policies and procedures which identify the risks related to CBB's activities, processes and systems.

**5.0 GUIDING PRINCIPLES**

CBB should adopt the following principles for an effective ERM practice:

**5.1 ERM creates and protect value**

ERM should contribute to the demonstrable achievement and improvement of performance through its implementation. ERM should enhance CBB's competitiveness and increases customer satisfaction with the aim of improving the return on equities of CBB and maximising returns to shareholders.

**5.2 ERM is an integral part of CBB decision making processes**

ERM should not be treated as a stand-alone activity and kept separated from CBB's main activities and processes. ERM should form part of the decision making processes which comprise of strategic, operational, financial and compliance activities.

**5.3 ERM explicitly addresses uncertainty**

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

**5.4 ERM is systematic, structured and timely**

A systematic, structured and timely approach to ERM contributes to the efficiency and consistency of information gathering process as well as enhancing the comparability and reliability of results reported.

**5.5 ERM is based on the best available information**

The inputs to the process of managing risk are based on information sources available such as historical data, past experiences, latest market information, stakeholders' feedback, observation, forecasts and expert judgement. The Board and its Senior Management should be informed on the limitations of any data modeling used or the possibility of views divergence among experts.

**5.6 ERM takes human and cultural factors into account**

ERM must recognise the capabilities, perceptions and intentions of external parties and internal staff that can facilitate or hinder achievement of CBB's objectives.



CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

5.7 ERM is transparent and inclusive

ERM should engage the stakeholders and decision makers timely (e.g. the Board and Senior Management) to ensure ERM remains relevant and up-to-date. This is to ensure appropriate representative and views from stakeholders are taken into account during determining risk criteria and risk action planning process.

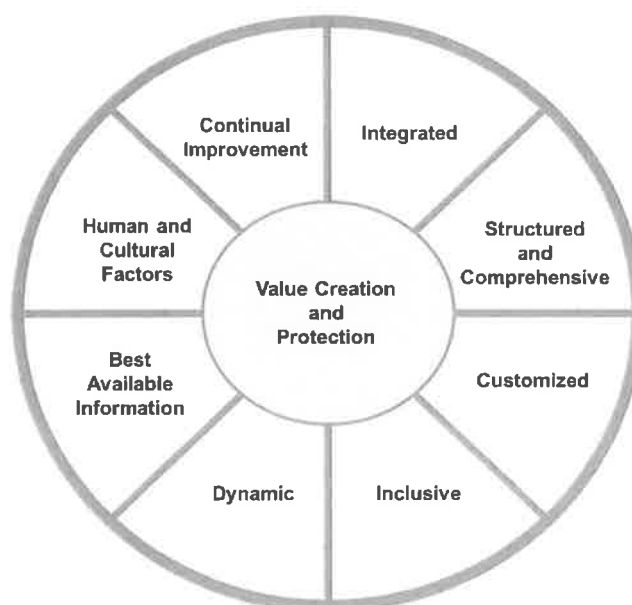
5.8 ERM is dynamic, interactive and responsive to change

The ERM process should be sensitive and possess the ability to respond to changes from internal or external factors or events.

## 6.0 ERM FRAMEWORK

This section sets out the foundations and arrangements that CBB will adopt consistent with the ISO31000:2018 - Risk Management Guidelines in embedding the risk management process. The framework assists in managing risks effectively through the application of the risk management process at varying levels and within specific contexts of CBB. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organisational levels. CBB adopts the ISO31000: 2018 ERM Framework under clause 4,5 and 6 as shown in diagram at section 2.1.

### 6.1 Key Principles (Clause 4)



CBB ERM policy will be supported by adherence to the following key principles.

No	Principle	Application
1	Integrated	Risk management is an integral part of CBB decision making process.
2	Structured and comprehensive	A structured and comprehensive approach to risk management contributes to consistent and comparable results.
3	Customized	The risk management framework and process are customized and proportionate to the CBB's external and internal context related to its objectives.
4	Inclusive	Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.
5	Dynamic	Risks can emerge, change or disappear as CBB's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

No	Principle	Application
6	Best available information	The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.
7	Human and cultural factors	Human behavior and culture significantly influence all aspects of risk management at each level and stage.
8	Continual improvement	Risk management is continually improved through learning and experience.

6.2 ERM Framework Component (Clause 5)



Adopted from ISO31000:2018, Diagram above illustrates the components of the framework for managing risk. It includes the essential steps in the implementation and ongoing support of the risk management process.

No	Principle	Application
1	Leadership and Commitment	<p>CBB Senior Management is accountable for managing risk while the Board is accountable for overseeing risk management. Board are required to:</p> <ul style="list-style-type: none"> <li>a) ensure that risks are adequately considered when setting the any agreed objectives;</li> <li>b) understand the risks faced by the CBB in pursuit of its objectives;</li> <li>c) ensure that systems to manage such risks are implemented and operating effectively;</li> <li>d) ensure that such risks are appropriate in the context of CBB's objectives; and</li> <li>e) ensure that information about such risks and their management is properly communicated.</li> </ul> <p>CBB is committed in ensuring that all applicable statutory and regulatory requirements are determined, understood and consistently met and that all risks and opportunity that can affect conformity and ability to meet its business objectives are determined and addressed.</p>
2	Integration	<p>CBB ERM Framework is focused on assisting the company in achieving its vision, mission and objectives in a dynamic and iterative approach whilst driving shareholders' and</p>

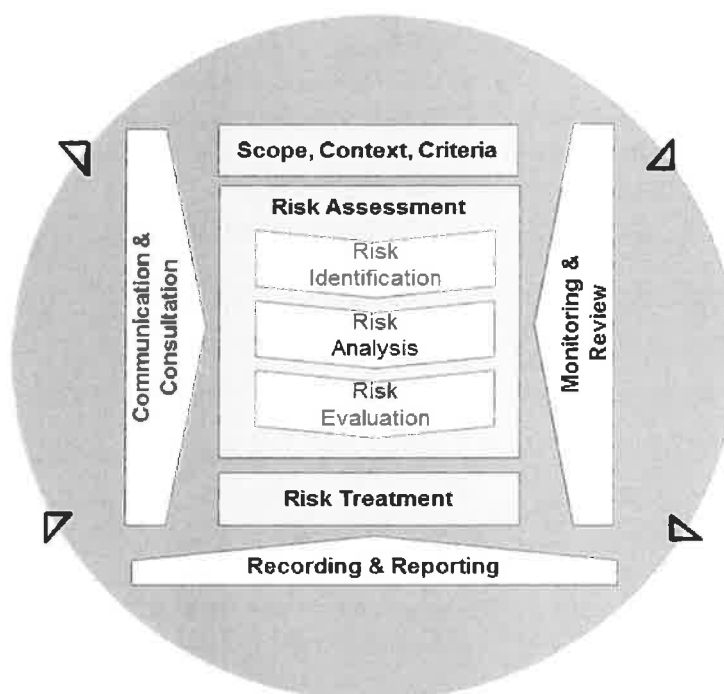
CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

No	Principle	Application
		stakeholders' value in a risk awareness and consciousness environment.
3	Design	<p>Embedding risk management involves an environment that can demonstrate a change in mindset and culture to be more risk aware at all levels. This risk aware culture is to be institutionalised into daily operational and business activities for effective risk management at the organisational and operational levels. All elements in this framework need to be dissolved in all standard operating procedures (SOPs).</p> <p>The framework involves three key steps:</p> <ul style="list-style-type: none"> <li>a) Setting the corporate strategy on an annual basis, aligning risk management to business objectives;</li> <li>b) Adopting a formal and standardised process methodology for risk management across investee companies; and</li> <li>c) Maintaining a structure that assigns ownership and responsibility for monitoring and updating risk management.</li> </ul>
4	Implementation	<p>Risk management shall be a part of the CBB's objectives, governance, leadership and commitment, strategy and operations. The risk management is not an objective by itself. It is a step that lead to something important.</p> <p>CBB shall adopt the ISO31000:2018 Risk Management process as its structured process for the identification, analyzing, evaluating, treating, monitoring and reporting of enterprise principle risks faced by CBB - covering Strategic Risks, Financial Risks, Operational Risks and Compliance Risks throughout its business.</p> <p>Risk management provides reasonable assurance to stakeholders that the objectives are achievable within its tolerable risk appetite.</p>
5	Evaluation	CBB shall periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviour; and determine whether it remains suitable to support achieving strategic objectives of CBB. Gradually, risk management should be part of performance management system of each employee.
6	Improvement	<ul style="list-style-type: none"> <li>a) Adapting</li> </ul> <p>The framework shall be monitored and reviewed on a regular basis to ensure its relevancy to changes in the external and internal context and to address the issues surrounding the external and internal changes.</p> <ul style="list-style-type: none"> <li>b) Continually improving</li> </ul>

CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

No	Principle	Application
		CBB shall continually improve the suitability, adequacy and effectiveness of the risk management framework and the way the risk management process is integrated. As relevant gaps or improvement opportunities are identified, plans and tasks shall be developed and assign them to those accountable for implementation. Once implemented, these improvements should contribute to the enhancement of risk management.

6.3 Risk Management Process (Clause 6)



No	Principle	Application
1	Communication and Consultation	<p>Successful risk management process is dependent on effective communication and consultation with interested parties or stakeholders, both internal and external. It is important to communicate and consult with interested parties at each step in the risk management process as stipulated in diagram above. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and interested parties understand the basis on which decisions are made, and the reasons why particular actions are required.</p> <p>The interested parties consultation process shall be continuous and, as such, shall be included as an integral part of the risk management process</p>
2	Establishing Scope	<p>It is important that before any risk management process is undertaken, the scope of the risk management activities must be clearly defined.</p> <p>As the risk management process may be applied at different levels (e.g. strategic, operational, budget, investment and other activities), it is important to be clear about the scope under consideration, the relevant objectives to be considered and their alignment with CBB objectives, mission and vision.</p> <p>When planning the approach, considerations include:</p> <ul style="list-style-type: none"> <li>a) objectives and decisions that need to be made;</li> </ul>

CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

No	Principle	Application
		<ul style="list-style-type: none"> <li>b) outcomes expected from the steps to be taken in the process;</li> <li>c) time, location, specific inclusions and exclusions;</li> <li>d) appropriate risk assessment tools and techniques;</li> <li>e) resources required, responsibilities and records to be kept; and</li> <li>f) relationships with other main processes, sub-processes and activities.</li> </ul>
3	Establishing the Context	<p>After the scope has been defined, next is to determine the internal and external issues that are relevant to its purpose and its strategic direction and that affects the ability to achieve the objectives. This can be done by performing the S.W.O.T Analysis. All information about these external and internal issues must be monitored and reviewed. These issues can include positive or negative factors or conditions.</p> <p>In order to consistently provide services that meet our interested parties expectations and applicable legal, other requirements and compliance obligation (LORCO), the following must be determined:</p> <ul style="list-style-type: none"> <li>a) the interested parties that are relevant within the context of the risk assessment; and</li> <li>b) the relevant requirements of these interested parties.</li> </ul> <p><i>(Risk Management Department will rely on compliance report produced by KPS Legal and Compliance Department.)</i></p> <p>All information about these interested parties must be monitored and reviewed. Establishing the context is defining the external and internal parameters to be taken into account when managing risk and setting the scope and risk criteria for the risk management policy. This is needed in order to:</p> <ul style="list-style-type: none"> <li>a) Clarify overall organisational objectives;</li> <li>b) Identify the environment in which objectives are pursued;</li> <li>c) Specify the main scope and objectives for risk management, boundary conditions and the outcomes required;</li> <li>d) Identify a set of criteria against which the risks will be measured; and</li> <li>e) Define a set of key elements for structuring the risk identification and assessment process.</li> </ul>
4	External and Internal Context	<p>The external and internal context is the environment in which CBB seeks to define and achieve its objectives.</p> <p>The context of the risk management process should be established from the understanding of the external and internal environment in which CBB operates and should</p>



No	Principle	Application
		<p>reflect the specific environment of the activity to which the risk management process is to be applied. Understanding the context is important because:</p> <ul style="list-style-type: none"> <li>a) risk management takes place in the context of the objectives and activities of CBB;</li> <li>b) organisational factors can be a source of risk; and</li> <li>c) the purpose and scope of the risk management process may be interrelated with the objectives of CBB as a whole.</li> </ul> <p>CBB should establish the external and internal context of the risk management process by considering the factors.</p> <p>(i) <u>Establishing the External Context</u> Examining the external context may include, but is not limited to: -</p> <ul style="list-style-type: none"> <li>a. The social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local;</li> <li>b. Key drivers and trends affecting the objectives of CBB;</li> <li>c. External stakeholders' relationships, perceptions, values, needs and expectations;</li> <li>d. Contractual relationships and commitments;</li> <li>e. All third parties and third parties and</li> <li>f. The complexity of networks and dependencies.</li> </ul> <p>"STEEPLE Analysis" forms part of external analysis to give an overview of the different macro environmental factors that has to be taken into consideration.</p> <p>STEEPLE is concerned with the following key factors that could indicate how the business environment is being influenced:</p> <ul style="list-style-type: none"> <li>a. <u>Social</u> Health/welfare, living conditions, poverty levels, job security.</li> <li>b. <u>Technology</u> Automation, industrial revolution 4.0 (disruptive technologies), industry focus on technological advancement, new discoveries, technology transfer, technological obsolescence, energy consumption and costs, industrial revolution 4, internet, communications, IT expenditure and investment in IT infrastructure.</li> <li>c. <u>Economy</u> Global economy, monetary policy, government spending, unemployment rate, taxation law, foreign</li> </ul>

CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

No	Principle	Application
		<p>exchange indices and rates, inflation rates, stages of the business cycle, cost of capital and financing.</p> <p>d. <u>Environment</u> Sustainability agenda, global warming, climate change, carbon emissions, recycling, environmental regulation/protection, renewable energy.</p> <p>e. <u>Political</u> General election result, tax policies, government culture, political stability.</p> <p>f. <u>Legal</u> Statutory and regulatory conditions, Corporate governance, Compliance, International trade regulations, Competition regulation.</p> <p>g. <u>Ethics</u> Business ethics, consent, confidentiality, Official Secrets Act, Security access, terms of business/trade, trust, reputation.</p>
5	Establishing the Internal Context	<p>The internal context is the internal environment in which CBB seeks to achieve its objectives. The risk management process should be aligned with the CBB culture, processes, structure and strategy.</p> <p>It is important to establish the internal context because:</p> <ul style="list-style-type: none"> <li>- Risk management takes place in the context of goals and objectives; and</li> <li>- Objective and criteria or a particular situation, process or activity shall be considered in the light of objectives as a whole.</li> </ul> <p>Evaluating the internal context may include, but is not limited to:</p> <ul style="list-style-type: none"> <li>a. Governance, organisational structure, roles and accountabilities;</li> <li>b. Policies, objectives, and the strategies that are in place to achieve above-mentioned objectives;</li> <li>c. Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);</li> <li>d. The relationships with and perceptions and values of internal stakeholders;</li> <li>e. CBB culture;</li> <li>f. Information systems, information flows and decision-making processes (both formal and informal);</li> <li>g. Standards, guidelines and models adopted by CBB; and</li> <li>h. Form and extent of contractual relationships.</li> </ul>

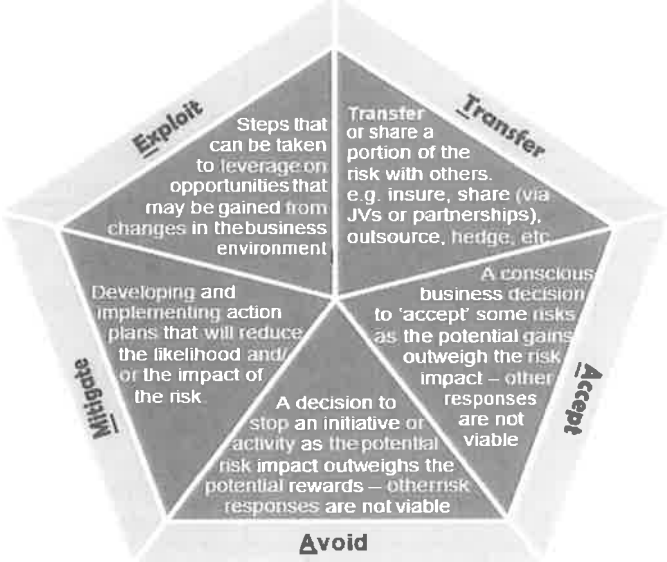
CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

No	Principle	Application
6	Risk Assessment	<p>Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. The three (3) steps to be performed in the completion of Risk Assessment can be summarized as below:-</p> <ol style="list-style-type: none"> <li>Risk Identification (Process No. 7)</li> <li>Risk Analysis (Process No. 8)</li> <li>Risk Evaluation (Process No.9)</li> </ol>
7	Risk Identification	<p>Risk identification involves identifying all possible events which may affect the achievement of CBB's business objectives. The aim of this step is to generate a comprehensive list of risk-based scenarios on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It may also involve the following:-</p> <ol style="list-style-type: none"> <li>Risk identification may starts with identifying all assumptions made in the decision making process;</li> <li>Laying out all assumptions that may have been ignored from the whole calculations;</li> <li>Finding out the adequacy of the assumptions by way of checklist, questionnaires, interview, analytical procedure and substantive testing on the relevance of assumptions made;</li> <li>Using risk information to propose for few ranges based on the assumptions made;</li> </ol> <p>CBB shall identify sources of risk, areas of impacts, events (including changes in underlying circumstances) and their causes and their potential consequences. The aim is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity.</p> <p>It is important to ensure that risks are accurately defined and articulated, i.e. risks which are not pursuing opportunities should be identified. Unidentified risks can pose a major threat as it will not be included in further analysis. Once a risk is identified, the CBB should identify any existing mitigations such as design features, people, processes and systems.</p> <p>Potential opportunities identified during the risk identification stage should be discussed during CBB strategic planning sessions or of relevant subsidiaries.</p> <p>Risk identification should be an on-going process and begins with having a clear understanding of the objectives, be it of CBB as a whole, departments, investment decisions or</p>

No	Principle	Application
		subsidiaries' revenues target. (Objectives must exist before management can identify events potentially affecting their achievement).
8	Risk Analysis	<p>Risk analysis is about developing an understanding of the risk. It provides an input to risk evaluation on whether risks need to be treated and on the most appropriate treatment strategies and methods. Some critical steps may involve:-</p> <ol style="list-style-type: none"> <li>Run few simulation and perform few analysis on the simulation together with the process owner;</li> <li>Provide information to the stakeholder based on reduced amount of uncertainty;</li> <li>Update value of range identified based on reduced amount of uncertainty; and</li> <li>Update range based on key assumption check and to re-perform the simulation based on the updated assumption.</li> </ol> <p>Risk analysis involves consideration of root causes and sources of risk, their positive and negative consequences, and the likelihood that those.</p>
9	Risk Evaluation	<p>In this process, the strength of internal control are being determined, evaluated and categorized into 3 categories:-</p> <ol style="list-style-type: none"> <li>1. Satisfactory: Controls are well managed, operated properly, and meet compliance requirements.</li> <li>2. Some weaknesses: Some control weaknesses/ inefficiencies have been identified. Although they do not present serious risk exposures but improvements in the controls are required.</li> <li>3. Weak: Unsatisfactory controls and do not meet acceptable standards, as many control weaknesses/ inefficiencies have been identified.</li> </ol> <p>The purpose of risk evaluation is to assist in making decisions, based on the outcome of risk analysis, about which risks need treatment and the priority for treatment implementation.</p> <p>It involves comparing estimated levels of risk with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.</p> <p>Risk evaluation uses the understanding of risk obtained during risk analysis to make decisions about future actions. Decisions may include:</p> <ol style="list-style-type: none"> <li>a) Whether a risk requires treatment;</li> <li>b) Whether an activity should be undertaken to mitigate risk; and</li> <li>c) Priorities for treatment.</li> </ol>

CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

No	Principle	Application
		<p>A common approach to decide on the appropriate decisions may be to divide risks into three bands:</p> <ul style="list-style-type: none"> <li>i. An upper band where the level of risk is regarded as intolerable whatever benefits the activity may bring, and risk treatment is essential whatever its cost ;</li> <li>ii. A middle band (or 'grey' area) where costs and benefits, are taken into account and opportunities balanced against potential consequences; and</li> <li>iii. A lower band where the level of risk is regarded as negligible, or so small that no risk treatment measures are needed.</li> </ul> <p>Following is an interpretation of CBB's Risk Appetite Parameter Appendix III</p>
10	Risk Treatment	<p>The objective of risk treatment or risk response is to reduce risks which are beyond CBB's risk appetite and to achieve a target risk ranking which is acceptable to CBB. Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.</p> <p>Risk treatment plans or risk mitigation plans are actions to be taken to prevent, detect or manage the risks to an acceptable level (YELLOW or GREEN zone). The design of risk treatment plans should be based on a comprehensive understanding of the risks concerned. It is particularly important to identify the root causes of the risks so that these are treated and not just the symptoms.</p> <p>Once identified risks are assessed, appropriate treatment (including Quick-wins) need to be developed for all EXTREME, TIME-BOMB and HIGH RISK as they are defined as a risk that is beyond CBB's risk appetite. Quick-wins and responses may be implemented for Moderate and Low Risks as per RGWC, MD/GCEO and Board's discretion.</p>
11	Risk Treatment Plans	<p>Once the risk treatment options are selected, they should be assembled into risk treatment plans. The purpose of risk treatment plans is to document how the chosen treatment options will be implemented. The risk treatment options can include the following:</p>

No	Principle	Application
		 <p><b>Exploit</b>: Steps that can be taken to leverage on opportunities that may be gained from changes in the business environment</p> <p><b>Transfer</b>: Transfer or share a portion of the risk with others. e.g. insure, share (via JVs or partnerships), outsource, hedge, etc.</p> <p><b>Accept</b>: A conscious business decision to 'accept' some risks as the potential gains outweigh the risk impact – other responses are not viable</p> <p><b>Avoid</b>: A decision to stop an initiative or activity as the potential risk impact outweighs the potential rewards – other risk responses are not viable</p> <p><b>Mitigate</b>: Developing and implementing action plans that will reduce the likelihood and/or the impact of the risk</p> <p>In some cases, one risk treatment option may not mitigate the risk to an acceptable level. In such cases, a combination of options may be appropriate.</p> <p>There are instances where management may decide to accept an Extreme or High Risk without developing any response plans – this should take into account the degree of controls over the risk, the cost and reputational impact and the opportunities presented by accepting risk. In such cases, the risks should still be reported on a regular basis to ensure that there is constant monitoring of these risks.</p> <p>Once the risk response option(s) has been determined by the risk owners and agreed upon by Risk and Governance Working Committee, implementation plans have to be developed and updated in the risk report with responsibility and timelines to completion clearly established. Please refer to Section 6.4 for Third Party Risk Management Strategy.</p>
12	Monitor and Review	<p>ERM monitoring is an ongoing process that assesses the presence, relevance and operationalization of components within CBB's ERM Framework over time.</p> <p>CBB's monitoring and review processes should encompass all aspects of the risk management process for the purposes of:-</p> <ul style="list-style-type: none"> <li>a) ensuring that controls are effective and efficient in both design and operation;</li> <li>b) obtaining further information to improve risk assessment;</li> <li>c) analysing and learning lessons from events (including near-misses, accident data, loss tender reports), direction changes, trends, successes and failures;</li> </ul>

No	Principle	Application
		<p>d) detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and</p> <p>e) identifying emerging risks.</p> <p>ERM monitoring techniques include:</p> <ul style="list-style-type: none"> <li>- Desktop reviews of ERM reports (on a quarterly basis) (Subsidiary Risk Report and CBB's Corporate Risk Report and Key Risk Indicators)</li> <li>- Periodic audits / reviews by the IAD and reported directly to the Board Audit Committee.</li> <li>- External Assurance Review for annual report purpose.</li> </ul>

#### 6.4 Third Party Risk Management ("TPRM")

One of the options in risk mitigation strategy is by way of "transferring risk". Transferring risk or share the risk with third party or parties e.g. through a contractual arrangement and risk financing. However, this method may not necessarily eliminate the residual risk owned by CBB. Hence, there should be a clear strategy in handling risk related to third party.

##### 6.4.1 There are six (6) main activities under TPRM:-

- i. Third Party Risk Assessment
- ii. Third Party Due Diligence and Selection of Third Parties
- iii. Third Party Contract Provisions and Considerations
- iv. Third Party Incentive / Compensation Review
- v. Third Party Oversight and Monitoring of Third Parties
- vi. Third Party's Business Continuity and Contingency Plans

##### 6.4.1.1 Third Party Risk Assessment

No	Principle	Application
1	Analysing the Implication of Outsourcing a particular activity.	Risk assessment of a business activity and the implications of performing the activity in-house or having the activity performed by a third party, are fundamental to the decision of whether or not to outsource.
2	Determining the Decision to outsource	CBB should determine whether outsourcing an activity is consistent with the strategic direction and overall business strategy of CBB. A decision needs to be made on why to outsource - what is the problem or objective - and what is expected from the sourcing arrangement.
3	Analysing Cost and Benefit of Outsourcing	After that determination is made, CBB should analyze the benefits and risks of outsourcing the proposed activity as well as the third party risk, and determine cost implications for establishing the outsourcing arrangement.
4	Area of Consideration	Consideration should also be given to the availability of qualified and experienced third parties to perform the service on an ongoing basis. CBB should also consider capability to provide appropriate ongoing oversight and

No	Principle	Application
		governance of the relationship with the third parties.
5	Update Risk Assessment	The risk assessment should be updated at appropriate intervals. CBB should revise its risk mitigation and control plans, if appropriate, based on the results of the updated risk assessment.

#### 6.4.1.2. Third Party Due Diligence and Selection of Third Parties

No	Principle	Application
1	Business background, reputation and strategy	<p>CBB should review a prospective third party's status in the industry and corporate history and qualifications; review its background, reputation and its principals; and ensure that the third party has an appropriate background check program for its employees.</p> <p>The third party's experience in providing the proposed service should be evaluated in order to assess its qualifications and competencies to perform the service. The third party's business model, including its business strategy and mission, service philosophy, sustainability initiatives, and organisational policies should be evaluated. CBB should also consider the resiliency and adaptability of the third party's business model as factors in assessing the future viability of the provider to perform services. CBB should check the third party's references to ascertain its performance record and verify any required licenses and certifications. CBB should also verify whether there are any pending legal or regulatory compliance issues (for example, litigation, regulatory actions, or complaints) that are associated with the prospective third party and its principals.</p>
2	Financial performance and condition;	<p>CBB should review the third party's financial condition and of its closely-related affiliates.</p> <p>The financial review may include:</p> <ul style="list-style-type: none"> <li>• Most recent financial statements and annual report with regard to outstanding commitments,</li> <li>• capital strength, liquidity and operating results;</li> <li>• The third party's sustainability, including factors such as the length of time that the TP has been in business and its growth of market share for a given service;</li> <li>• Its commitment (both in terms of financial and staff resources) to provide the contracted</li> <li>• services to CBB for the duration of the contract;</li> <li>• The adequacy of the third party's insurance coverage;</li> <li>• The adequacy of its review of the financial condition of any subcontractors;</li> <li>• Other current issues the third party may be facing that could affect future financial and/or operational performance.</li> </ul>



CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

No	Principle	Application
3	Operations and internal controls.	<p>CBB are responsible for ensuring that services provided by third party comply with applicable laws and regulations and are consistent with safe-and-sound business practices. Depending on the characteristics of the outsourced activity, some or all of the following may need to be reviewed on the adequacy of standards, policies and procedures:</p> <ul style="list-style-type: none"> <li>• Quality management systems and controls;</li> <li>• Facilities management (such as access requirements or sharing of facilities);</li> <li>• Training, including compliance training for staff;</li> <li>• Security of systems and privacy protection of the organisation's confidential information;</li> <li>• Maintenance and retention of records;</li> <li>• Systems development, maintenance and contingency planning;</li> <li>• Service support and delivery;</li> <li>• Employee background checks;</li> <li>• Adherence to applicable laws, regulations and supervisory guidance.</li> </ul>

6.4.1.3. Third Party Contract Provisions and Consideration

No	Principle	Application
1	Intent and expectation	A successful third-party relationship is having a mutual understanding of intents and expectations.
2	Scope	<p>In any contract &amp; purchase orders, CBB should clearly define the rights and responsibilities of each party, including:</p> <ul style="list-style-type: none"> <li>• Support, maintenance and customer service;</li> <li>• Duration and timeframes;</li> <li>• Compliance with applicable laws, regulations and regulatory guidance;</li> <li>• Training and awareness of CBB's employees;</li> <li>• The ability to subcontract services;</li> <li>• The distribution of any required statements of disclosures to the CBB's customers;</li> <li>• Insurance coverage requirements;</li> <li>• Terms governing the use of the CBB's property, equipment and staff.</li> </ul>
3	Cost and pricing structure	<p>Contracts should describe the pricing structure, variable charges, and any fees to be paid for non-recurring items and special requests. Agreements should also address which party is responsible for the payment of any legal, audit, and examination fees related to the activity being performed by the third party.</p> <p>Where applicable, agreements should address the party responsible for the expense, purchasing, and maintenance of any equipment, hardware, software or any other item</p>

CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

No	Principle	Application
		related to the activity being performed by the third party. In addition, CBB should ensure that any incentives (for example, in the form of variable charges, such as fees and/or commissions) provided in contracts, do not provide potential incentives to take imprudent risks or drive inappropriate behaviour.
4	Right to audit	Agreements may provide for the right of CBB or its representatives to audit the third party's quality systems, processes or products/services and/or to have access to audit reports. Agreements should define the types of audit that CBB will conduct and the frequency of the audit to be conducted. The audit conducted should be based on the risk profile or result of due diligence finding. (risk-based auditing).
5	Establishment and monitoring of performance standards / service level agreements	Agreements should define measurable (SMART) obligations and performance standards, structured in a comprehensive service model aligned with business needs. A dynamic set of risk-based controls and metrics (KPI/KRI) should be clearly linked to the service objective which CBB targeted to monitor.
6	Confidentiality and security of information	Consistent with applicable laws, regulations, and supervisory guidance, third parties should ensure the security and confidentiality of both the organisation's confidential information and especially customers' information. CBB is responsible to ensure third parties take appropriate control measures designed to meet the objectives of relevant security guidelines. These measures should be mapped directly to the information security processes of CBB, as well as to be included or referenced in agreements between CBB and third party(ies). These obligations also require specific controls to safeguard any cybersecurity threat. Information made available to the third party should be limited to what is needed to provide for the outsource services. Third parties may reveal confidential supervisory information only to the extent authorized under applicable laws and regulations.
7	Ownership and license	Agreements should define the ability and circumstances under which third parties may use CBB property inclusive of data, hardware, software and intellectual property. Agreements should address the ownership and control of any information generated by third parties. If CBB purchase software from third parties, escrow agreements may be needed to ensure the accessibility of the source code and programs under certain conditions.
8	Indemnification	Agreements should provide for third party indemnification for any claims against CBB resulting from the third party's negligence.
9	Default and termination	Agreements should define events of a contractual default, list of acceptable remedies, and provide opportunities for

CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

No	Principle	Application
		curing default. Agreements should also define termination rights, including change in control, merger or acquisition, increase in fees, failure to meet performance standards, failure to fulfill the contractual obligations, failure to provide required notices, and failure to prevent violations of law, bankruptcy, closure, or insolvency. Contracts should include termination and notification requirements that provide CBB with sufficient time to transfer services to another third party. Agreements should also address a third party's preservation and timely return of data, records, and other resources.
10	Dispute Resolution	Agreements should include a dispute resolution process to expedite problem resolution and address the continuation of the arrangement between the parties during the dispute resolution period.
11	Limits on liability	Third parties may want to limit their liability. CBB should determine whether the proposed limitations are reasonable when a third party fails to perform in accordance to the agreed service level.
12	Insurance	Third parties should have adequate insurance and provide outsourcing CBB with proof of insurance. Further, third parties should notify CBB when there is a material change in their insurance coverage.
13	Customer / employee complaints	Agreements should specify CBB responsibilities and third parties related to responding to complaints. If third parties are responsible for complaint resolution, agreements should provide for summary reports to the outsourcing CBB that track the status and resolution of complaints.
14	Business resumption and contingency plan of third party	Agreements should address the continuation of services provided by third parties in the event of operational failures. Agreements should address third party responsibility for backing up information and maintaining disaster recovery and contingency plans. Agreements may include a third party's responsibility for testing of plans and providing testing results to CBB.
15	Subcontracting	If agreements allow for subcontracting, the same contractual provisions should apply to the subcontractor. Contract provisions should clearly state that the third party has overall accountability for all scope of work provided. Agreements should define the services that may be subcontracted, the third party's due diligence process for engaging and monitoring subcontractors, and the notification and approval requirements regarding changes to the third party's subcontractors. Special attention should be paid to any foreign subcontractors, as information security and data privacy standards may be different in other jurisdictions. Additionally, agreements should include the third party's process for assessing the subcontractor's financial condition to fulfill contractual obligations.

#### 6.4.1.4. Third Party Claims, Compensation, and Incentive

CBB should also ensure that an effective process is in place to review and approve any incentive compensation that may be embedded in third party contracts, including a review of whether existing governance and controls are adequate in light of risks arising from incentive compensation arrangements.

If the third party represents CBB by selling products or services on its behalf, management should consider whether the incentives provided might encourage the third party to take imprudent risks, which is not aligned with overall objective.

Inappropriately structured incentives may result in reputational damage, increased litigation, or other risks to CBB. An example of an inappropriate incentive would be one where variable fees or commissions encourage the third party to push products with higher profit margins without due consideration of whether such products are suitable or required for the customer.

#### 6.4.1.5. Oversight and Monitoring of Third Parties

CBB should establish controls and performance metrics to determine third party performance meet the expectation.

Further, more frequent and stringent monitoring is necessary for “significant value” third parties that refers to performance, financial, compliance, or control concerns. For lower value risk third parties, the level of monitoring can be lessened.

No	Principle	Application
1	Financial condition	CBB should have established controls to monitor the financial condition of third parties to evaluate their ongoing viability. In performing these assessments, organizations should review the most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity and operating results. If a third party relies significantly on subcontractors to provide services to CBB, then the third party's controls and due diligence regarding the subcontractors should also be reviewed.
2	Internal controls	For significant third party relationships, CBB should assess the adequacy of the quality control environment. Assessments should include reviewing available audits or reports and on-site inspections. Performance devaluations or security incidents at the third party may also necessitate the organization to elevate its monitoring of the third party. (e.g. more in-depth / frequent reporting or inspections)
3	Escalation of oversight activities	CBB should ensure that risk management processes include triggers to escalate oversight and monitoring when third parties are failing to meet performance, compliance, control, or viability expectations.

CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

6.4.1.6. Third Party's Business Continuity and Contingency Plans

No	Principle	Application
1	Existence of Business Continuity Documentation	Ensure that a disaster recovery and business continuity plan exist with regards to the contracted products and services.
2	Adequacy and effectiveness of Business Continuity Documentation	CBB shall assess the adequacy and effectiveness of a service provider's disaster recovery and business continuity plan and its alignment to CBB BCP Documentation.
3	Clear Segregation of Duties and TOR	CBB shall document the roles and responsibilities for maintaining and testing the third party's business continuity and contingency plans;
4	Testing of BCP	Test the service provider's business continuity and contingency plans on a periodic basis to ensure adequacy and effectiveness of the plan
5	Alternative Third Party.	Maintain an exit strategy, including a pool of comparable third parties, in the event that a contracted service provider is unable to perform in accordance to the service level agreement.

## 7.0 ERM REPORTING AND MONITORING STRUCTURE

An effective risk reporting structure enables structured communication to support and embed the ERM strategy into the management and operations of CBB. An effective reporting structure also ensures accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management performance.

A defined reporting and monitoring structure to facilitate the process of communicating risk related information throughout the organisation is detailed in this section. Briefly, CBB Board and KPS Board Governance and Risk Committee ("BGRC") have the ultimate responsibility for risk management oversight with executive responsibility delegated to the Managing Director & Group Chief Executive Officer ("MD/GCEO"), RGWC and all staff. KPS Head of Risk Management Department is responsible for coordinating all risk management related activities throughout CBB and reports directly to KPS' MD/GCEO and Deputy Chief Executive Officer - Finance and Corporate Services. The ERM reporting structure of KPS Group and CBB is shown in the **Appendix II**.

In executing the above, the management shall ensure that adequate resources are available to those accountable or responsible for managing risk.

### 7.1. Overview of ERM Reporting and Monitoring Structure.

KPS' Board, BGRC, MD/GCEO, Risk and Governance Working Committee ("RGWC"), CBB Board and all staff play a critical role in ensuring that risks management activities are effectively and properly implemented throughout CBB and KPS Group.

## CENTURY BOND BHD

### ENTERPRISE RISK MANAGEMENT (ERM) POLICY

The ERM Reporting and Monitoring Structure sets out a guideline to ensure responsibility for risk management is clearly understood throughout CBB and facilitates oversight of risk management throughout the organisation.

#### 7.2. Oversight of Key Risk Areas

The ERM Reporting and Monitoring Structure covers the following areas:

##### 7.2.1 Management of CBB's enterprise risks

This involves monitoring and oversight of CBB's corporate / enterprise risks and may include risks that are pervasive across various subsidiaries.

In ensuring effective risk governance, reporting and monitoring of risks within each key risk area are divided into three levels, as follows :

##### 7.2.1.1 Oversight of ERM Activities

Oversight of ERM activities involves ensuring that effective risk management has been performed within the respective key risk area.

CBB Board has ultimate oversight of all risk management activities within CBB. Nonetheless, oversight for risk management within CBB's two key risk areas is structured as follows:

- Oversight of risk management within CBB

CBB Board provides oversight roles and responsibility during the CBB's quarterly meeting.

- Oversight of CBB's enterprise risks

The BGRC and Risk and Governance Working Committee ("RGWC") and CBB Board provide oversight of CBB's enterprise / corporate risks and overall risk management related activities throughout the company.

They are responsible for setting CBB ERM strategy whilst ensuring that an appropriate culture to promote risk awareness throughout CBB is being cultivated. Oversight of CBB's enterprise risks also involves managing risks stemming from all subsidiaries that may impact KPS as a whole.

#### 7.3. Independent Assurance

KPS' IAD is responsible for providing independent assurance that ERM related activities are effectively performed within subsidiaries and throughout CBB.

#### 7.4. Key Risk Indicators ("KRI")

Residual Risk Rating refers to the risk remaining after considering the effectiveness of all mitigations. It is the targeted position in the future state.

The residual rating will provide management with:

- A view on whether the remaining risk is within tolerance level; and
- It will act as an indication of whether the correct mitigations have been selected and whether further mitigations are required.

#### 7.4.1. Develop Key Risk Indicators

7.4.1.1 Key Risk Indicators act as early warning signals by:

- Providing the ability to appreciate changes to CBB's risk profile due to shifts in established patterns and circumstances
- Informing and keeping management apprised to enable proactive action is implemented, hence preventing or reducing the impact of the risk.

7.4.1.2 Key Risk Indicators are divided into two (2) types, which are:

- Leading KRI – Measures a risk before it occurs & is forward looking. Leading KRI provides valuable insight in order to take timely action & improve results.
- Lagging KRI – Measures a risk after risk event occurred. Lagging KRI provides a backward looking perspective and is less likely to prevent risk from occurring.

7.4.1.3 Critical KRI Attributes

- KRIs should be agreed upon by the Risk owners & Risk Management Department as an effective measure of risks.
- KRI must be something that can be quantified and measured. It should not be a soft or subjective measure that is based on individual feedback.
- KRIs must be clearly linked to risks and objectives). There can be a many to one (i.e. many KRIs linked to 1 risk) or one to many (i.e.: many risks linked to the same KRI). However, the correlation must be clear and not too distant.
- The KRI details must be clearly documented so there is no ambiguity on the purpose of the KRI, what it measures, and implication should it be "triggered".
- The cost effectiveness of the KRI and its practicality to extract is vital in the selection of KRIs. There is no point selecting a nice-to-have KRI such as customer satisfaction if there is no economically feasible or practical manner to extract such KRIs on a regular basis. In situations like these, replacement KRI which may not be

so direct such as number of customer complaints might be a more practical measure. There is therefore a need to be creative in KRI identification & selection.

- There must be a clear tolerance level setting via a “trigger point” for each KRI where there is a prompting for investigation and action. The purpose is to initiate action and ensure issues are clearly addressed.
- There must be clear ownership of the KRI, whereupon the explanation for triggering of KRI, its trend must be available.
- The identification of KRI must be conducted continuously prior to the risk assessment workshop, during the workshop and after the workshop. The purpose is to independently validate the key measures that track the business and ensure critical risks are clearly measured.
- KRIs should be aligned to the KPIs used during the business planning process and that used management reporting. This is because KPIs track the critical measure of whether CBB is achieving its objectives, and KRIs are intended to actively measure and track risks which could prevent our strategic objectives from being achieved.

#### 7.4.1.4 Setting the Plan/ Target and the KRI trigger/tolerance

When setting up the KRI, one of the critical factors is to determine the two main measurable values:

- The Target or Planned value

This represents the planned value for achievement. Typical the target or planned value will have to be broken into annual value, and dissected into the frequency of reporting (either monthly, quarterly, half yearly or annually). For example, for system uptime, the target uptime may be set at 99.5% i.e. it is intended that the system be online for 99.5% of the time.

- The Risk Trigger or tolerance value

For each of the KRI, there is a need to identify the value below/above the planned or target value that the KRI is considered triggered.

For example, for the same KRI (System uptime), the risk trigger/ tolerance level may be set at 97%. i.e. if the system is online for anything less than 97% of the time, the risk of system failure is considered “triggered”.

Where there is no tolerance value determined, a default



CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

threshold of 20% below the planned / target may be used as guidance. However, this needs to be aligned to management requirements.

## **8.0 AMENDMENTS**

The Board is empowered to amend and/or modify this policy from time to time.

## **9.0 EXCEPTIONS**

Any exception from this Policy shall require the approval of CBB Board unless they are deemed as operational in nature.

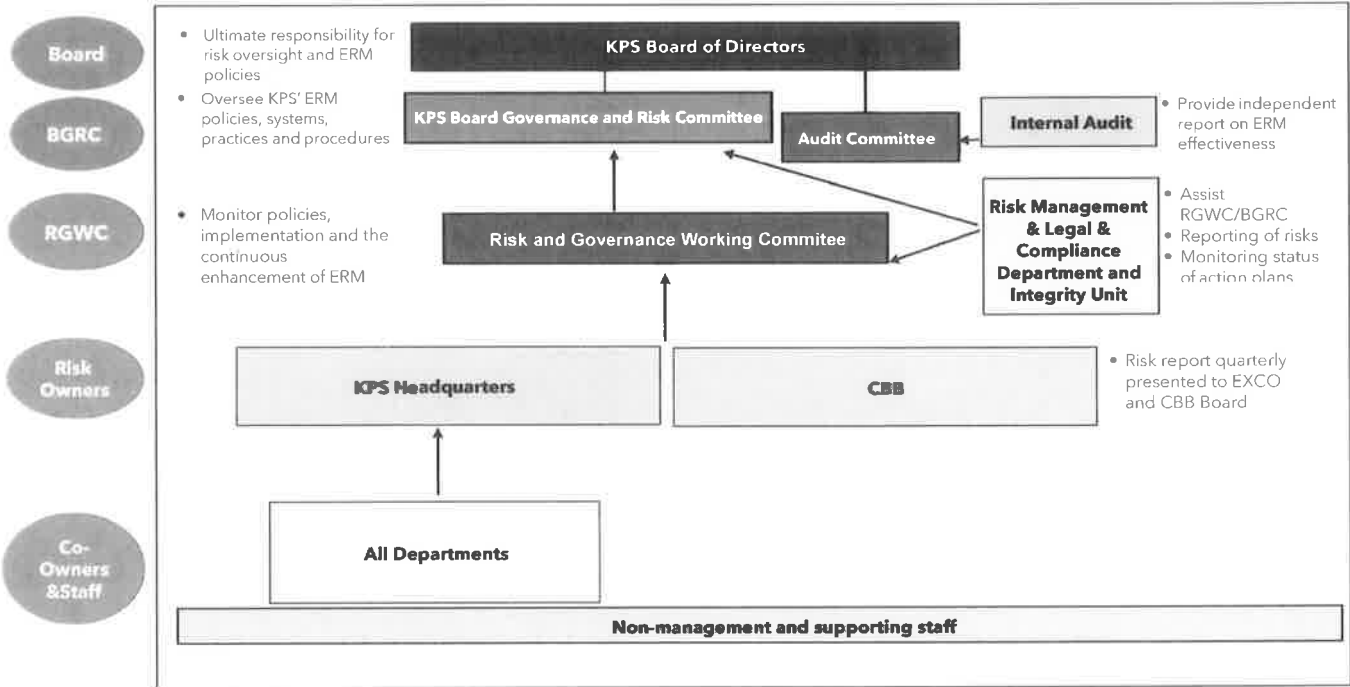
**Appendix I: Definition**

Terms	Definition
Enterprise Risk Management (ERM)	ERM is a method and process used by CBB to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organisation's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress.
Consequence	An event can lead to a range of consequences. A consequence can be certain or uncertain and can have positive or negative effects on objectives. Consequences can be expressed qualitatively and quantitatively. Initial consequences can escalate through knock-on effects.
Control	Controls include any process, policy, device, practice, or other actions which modify the risk. Controls may not always exert the intended or assumed modifying effect.
KPS	Kumpulan Perangsang Selangor Berhad
Level of Risk	Magnitude of risk or combination of risks, expressed in terms of the combination of consequences and their likelihood.
Likelihood	In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).
Monitoring	Continual checking, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected. Monitoring can be applied to a risk management framework, risk management process, risk or control.
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objective.
Risk Profile	The set of risks can contain those that relate to the whole organisation, part of the organisation, or as otherwise defined.
Risk Treatment	Risk treatment is a process to modify risk. Risk treatment can involve: <ul style="list-style-type: none"> <li>- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;</li> <li>- Taking and increasing risk in order to pursue an opportunity;</li> <li>- Removing the risk source;</li> <li>- Changing the likelihood;</li> <li>- Changing the consequence;</li> <li>- Sharing the risk with another party or parties (including</li> </ul>

CENTURY BOND BHD  
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

	<p>contracts and risk financing); and</p> <ul style="list-style-type: none"> <li>- Retaining the risk by informed decision.</li> </ul>
Risk Assessment (RA)	Overall process of risk identification, risk analysis and risk evaluation of a particular function, investment process, budgeting process, product or services of CBB.

Appendix II: KPS & CBB Risk Reporting Structure



## CENTURY BOND BHD

## ENTERPRISE RISK MANAGEMENT (ERM) POLICY

## Appendix III: CBB Risk Appetite Parameter

Factor	Impact				
	Insignificant	Minor	Moderate	Major	Catastrophic
Financial: RM/mill					
Revenue	Decreased by < than 2%	Decreased by 2% - 5%	Decreased by 5% - 10%	Decreased by 10% - 30%	Decreased by > than 30%
Total cost	Increased by < than 2%	Increased by 2% - 5%	Increased by 5% - 10%	Increased by 10% - 30%	Increased by > than 30%
PBT	Decreased by < than 2%	Decreased by 2% - 5%	Decreased by 5% - 10%	Decreased by 10% - 30%	Decreased by > than 30%
EBITDA	Decreased by < than 10%	Decreased by 10% - 20%	Decreased by 20% - 30%	Decreased by 30% - 50%	Decreased by > than 50%
ES2					
Cybersecurity	Financial loss up not more than RM 100,000	Financial loss within RM 100,000 to RM 500,000	Financial loss within RM 500,000 to RM 1,000,000	Financial loss within RM 1,000,000 to RM 5,000,000	Financial loss up more than RM 5,000,000
Non-financial					
Legal / Regulatory / Compliance	No litigation consequences	<ul style="list-style-type: none"> <li>Issuance of advice letter</li> <li>Minimum fine</li> </ul>	<ul style="list-style-type: none"> <li>Issuance of private reprimand / warning letter</li> <li>Moderate fine</li> </ul>	<ul style="list-style-type: none"> <li>Multiple issuance of public reprimand / warning letter</li> <li>Heavy fines</li> <li>Suspension of trading</li> </ul>	<ul style="list-style-type: none"> <li>Delisting</li> <li>Closure of operations</li> <li>Jail sentence for directors</li> </ul>
Reputation / Media	No permanent damage in the short or long term	Minor impact due to complaints/unfavorable media coverage but would not disrupt the organizations' routine operations	Significant media coverage/ complaints to authority/ stakeholders/ press that could disrupt the organizations' operations in short or medium term	Unfavorable publicity or media coverage affecting corporate image that requires immediate remedial actions or response	Unfavorable publicity or media coverage with long term adverse effects on corporate reputation and disruption of business that require immediate remedial actions or response
Anti-Bribery / Corruption	<ul style="list-style-type: none"> <li>Minimal local media attention quickly contained, short term recoverability</li> <li>Notice of violations/ warnings requiring administrative action and minimal penalties</li> <li>Minimal customer complaints and recovery costs</li> </ul>	<ul style="list-style-type: none"> <li>Local market impact on Department's brand and reputation</li> <li>Routine governing body</li> <li>Investigations subject to moderate fines and penalties may be subject to regulatory proceedings and/or hearings</li> <li>Minimal decline in customer relationships and some recovery costs</li> </ul>	<ul style="list-style-type: none"> <li>Sustained local press coverage with escalating customer implications</li> <li>Routine litigation subject to substantial fines or penalties, subject to regulatory proceedings and/or hearings</li> <li>Loss or decline of customer relationships and moderate recovery costs</li> </ul>	<ul style="list-style-type: none"> <li>National or sustained regional press coverage with long-term damage to public image</li> <li>Potentially a significant governing body scrutiny, investigations subject to substantial fines and penalties, which may include some criminal charges, subject to regulatory proceedings and/or hearings</li> <li>Strained key customer relationships and significant recovery costs and threat to future growth</li> </ul>	<ul style="list-style-type: none"> <li>Global Media Coverage</li> <li>Major scrutiny, investigations subject to substantial fines and penalties including criminal charges, and/or cease and desist orders, possible regulatory action</li> <li>Loss of major customer relationships and serious threat to future growth</li> </ul>
Operational Downtime (IT)	Able to recover within 12 hours	Able to recover within 12 to 24 hours	Able to recover within 24 to 48 hours	Able to recover within 48 to 96 hours	Able to recover in more than 96 hours
Operational Downtime (OT)	Able to recover within less than 30 minutes	Able to recover within less than 6 hours	Able to recover within 12 hours	Able to recover within 12 hours	Able to recover within 1 day Able to recover with more than 1 day
Data Loss	Non to minimal data loss.	Loss of publicly accessible information (Open Data)	Loss of restricted and internal information (For Internal Use Data)	Loss of confidential information (Confidential Data)	Loss of top secret information (Secret Data)

### Appendix III: CBB Risk Appetite Parameter (Cont'd)

Factor	Impact				
	Insignificant	Minor	Moderate	Major	Catastrophic
<b>Non-Financial</b>					
Cybersecurity - Reputation / Media	No coverage in national news media and no impact to public confidence in KPS products or services. Will not require an official response from KPS.	Little to no coverage in national news media resulting in minimal to no loss of public confidence in KPS products and services. Will not require an official response from KPS Board or Management.	Sporadic coverage in national news media resulting in minor loss of public confidence in KPS products and services. Unlikely to require an official response from KPS Board or Management.	Moderate coverage in national news media resulting in short term loss of public confidence in KPS products and services. May require an official response from KPS Board or Management.	Widespread coverage in national news media resulting in permanent loss of public confidence in KPS products and services. Will require an official response from KPS Board or Management.
Risk impact description	An event where the impact can be absorbed / managed through routine activity.	An event where the impact can be absorbed / managed with minimum management effort.	An event that causes the business to sustain negative financial / non-financial impacts that would require some work / planning from Management to manage the issue.	An event that could lead the business to sustain huge adverse financial / non-financial impacts that would require hard work from Management to manage the issue.	An event that could potentially cripple the entire business in the long-term.

### Appendix III: CBB Risk Appetite Parameter (Cont'd)

<u>Almost Certain</u>	<ul style="list-style-type: none"><li>•Likelihood of occurrence within 80.1% - 99.9%.The risk will occur in most circumstances or at frequent intervals. E.g. On monthly basis or probability is more than 80.1 %</li></ul>
<u>Likely</u>	<ul style="list-style-type: none"><li>•Likelihood of occurrence within 60.1% - 80%.The risk is expected to occur in most circumstances.E.g.: several times in a year or probability is between 60% to 80%</li></ul>
<u>Possible</u>	<ul style="list-style-type: none"><li>•Likelihood of occurrence within 40.1% - 60%. The risk may occur at some period</li><li>•E.g.: Once every 3 years or chances between 40% to 60%.</li></ul>
<u>Unlikely</u>	<ul style="list-style-type: none"><li>•Likelihood of occurrence within 20.1% to 40%. The risk is to occur less frequently.</li><li>•E.g.: Once every 5 years or chances of probability between 20% to 40%</li></ul>
<u>Rare</u>	<ul style="list-style-type: none"><li>•Likelihood of occurrence within 0.1% -20%. The risk may occur in exceptional circumstances. E.g.: Once in every 10 years or chance of probability less than 20%</li></ul>

Appendix IV: CBB Risk Prioritisation Matrix

