



BBGI PUBLIC COMPANY LIMITED



RISK MANUAL

First Revision of 2024.
Prepared by: Corporate Strategy and Risk Management Division.
Date: November 27, 2024.

Preface.

The Risk Management and Corporate Governance Committee of BBGI Public Company Limited is committed to ensuring that the company maintains appropriate levels of governance and risk management. This includes awareness of economic, social, and environmental factors, as well as efforts to reduce carbon dioxide emissions and other pollutants. The company also places importance on human rights, labor health and safety standards, and relationships with surrounding communities. Through these actions, the company ensures effective operations and the achievement of organizational goals. To this end, the company has adopted and applied internationally recognized risk management frameworks, including COSO ERM and ISO 31000, to maximize benefits for the organization.

Risk management is a process established by the management team as a tool to manage risks arising from operational activities, which may be impacted by the constantly changing external factors such as economic, political, technological, environmental, and social conditions, as well as internal factors including strategic planning, organizational structure, and work processes. These risks can significantly affect the achievement of the organization's objectives. By managing these risks to an acceptable level, effective risk management helps strengthen corporate governance practices, enhance enterprise value, improve competitive advantage, and build organizational resilience and adaptability in the face of change.

The Company recognizes the importance of effective risk management and is therefore committed to embedding a risk management system into every stage of its operations, across all departments and at all levels—from executives to employees. This commitment is communicated through the “BBGI Enterprise Risk Management Handbook,” which has been updated for the year 2025. The handbook includes revisions to the risk management policy, the enterprise-wide risk governance structure, roles and responsibilities, and the risk management process. It is intended to ensure that all executives and employees are well-informed and are able to implement risk management practices correctly and consistently throughout the organization.

The Risk Management and Corporate Governance Committee sincerely hopes that the updated and enhanced content of this Risk Management Handbook—designed to be modern, clear, and user-friendly—will be of practical benefit to all executives and employees. It is expected that the handbook will be appropriately applied and contribute to achieving the greatest benefit for the Company.

Approved by the resolution of the Risk Management and Corporate Governance Committee.

at the meeting held on 27 November 2024.

Table of Contents.

Chapter 1 : Introduction.

| | |
|---|----|
| Risk Management Policy of BBGI Public Company Limited | 3. |
| Enterprise Risk Management Structure | 4. |
| Duties and Responsibilities | 5. |
| Definition of Risk Management | 7. |
| The Importance of Risk Management | 8. |

Chapter 2 : Enterprise Risk Management Approach.

| | |
|--|-----|
| Enterprise Risk Management Process | 9. |
| Levels of Enterprise Risk Management | 10. |
| Enterprise Risk Management Framework | 11. |

Chapter 3 : Enterprise Risk Management Process.

| | |
|---|-----|
| Enterprise Risk Management Process | 12. |
| 1. Objective Setting/Establishing the Context | 12. |
| 2. Risk Assessment | 13. |
| 3. Risk Mitigation / Risk Treatment | 18. |
| 4. Monitoring and Reporting | 23. |

Chapter 4 : Risk Management Models.

| | |
|---------------------------------|-----|
| Strategic Risk Management | 25. |
| Project Risk Management | 27. |
| Portfolio View of Risk | 29. |

Appendix.

| | |
|-------------------|-----|
| Definitions | 31. |
|-------------------|-----|

Chapter 1 : Introduction.

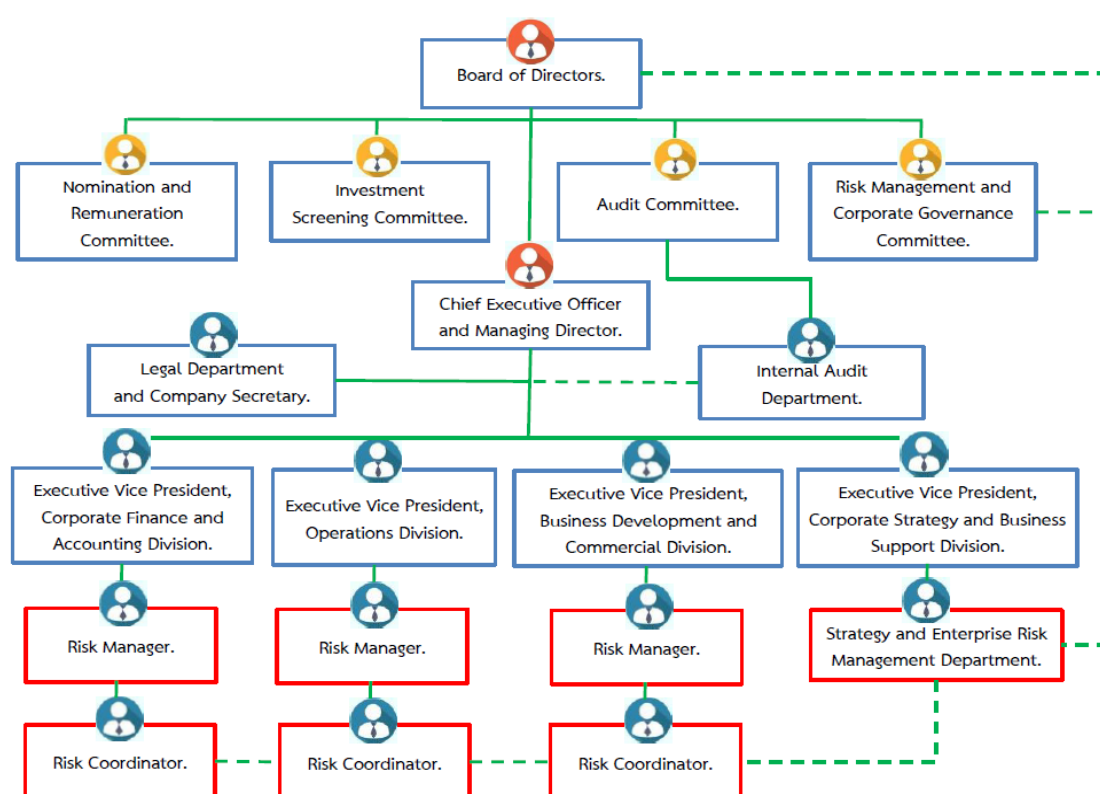
Risk Management Policy of BBGI Public Company Limited.

BBGI Public Company Limited ("the Company") has been continuously implementing risk management since 2017 to protect against the volatility of various factors that may affect the Company's performance. Subsequently, the Company has adopted internationally recognized risk management frameworks, namely COSO ERM and ISO 31000, to enhance the efficiency of its risk management processes. This is to prevent and mitigate the impact of potential risks that could hinder the achievement of the Company's objectives. All executives and employees play a role in managing risks within their respective areas of responsibility, under the continuous supervision of the Risk Management and Corporate Governance Committee. The Company has established an enterprise-wide risk management policy as follows:

1. The Company assigns executives and employees in each department to be responsible for risk oversight. They are expected to actively participate in the development of the Company's risk management practices and to clearly understand their roles and responsibilities related to risk management.
2. The Company has established an effective risk management process at every stage of operations, in accordance with the principles of Good Corporate Governance. Risk management is integrated with the Company's strategic planning process and information technology management to promote sound management practices. This integration helps reduce the likelihood and impact of risks on overall performance and enhances the potential for organizational success.
3. Promote and support the successful implementation of risk management across the entire organization by utilizing limited resources efficiently in the identification, assessment, and appropriate management of risks.
4. Encourage and foster a risk management culture within the organization by raising awareness among all personnel about the importance of risk management.
5. Executives and employees at all levels participate in supporting and encouraging subsidiaries and associated companies to recognize and prioritize risk management in their operations.
6. The Risk Management and Corporate Governance Committee, along with executives and employees at all levels, are involved in implementing a standardized risk management system. This includes auditing, monitoring, and evaluating risk management performance to ensure it is appropriate and aligned with the achievement of shared business objectives, as well as consistent with the Company's Environmental, Social, and Governance (ESG) policies.
7. The Risk Management and Corporate Governance Committee, along with senior management, is responsible for overseeing climate-related risks and opportunities, including physical risks and transition risks. This oversight includes reviewing, monitoring, and evaluating performance to support the achievement of carbon neutrality and net-zero greenhouse gas emissions targets.

Enterprise Risk Management Structure.

The Enterprise Risk Management Structure comprises the Board of Directors, executives, and all departments within the organization. The Risk Management and Corporate Governance Committee (RMC), appointed by the Board of Directors, is responsible for overseeing the implementation of an effective risk management system across the organization. The committee ensures that executives and employees are aware of potential risks that may impact the organization and that appropriate measures are in place to manage such risks effectively. To support this system, the Company has established a central coordinating unit — the Strategy and Risk Management Department (SR) — along with the Internal Control Unit. These units are responsible for coordinating and supporting executives, employees, and various departments in implementing the risk management and internal control processes effectively and continuously. The organizational structure is as follows:



Note: Risk Manager = Director by Position or Authorized Representative.

Risk Coordinator = Duties Assigned by the Executive Vice President / Senior Vice President.

Duties and Responsibilities.

1. Risk Management and Corporate Governance Committee.

1. Establish policies, strategies, and goals for enterprise-wide risk management.
2. Continuously develop and enhance the effectiveness of the enterprise-wide risk management system.
3. Support and promote collaboration in risk management at all levels of the organization.
4. Ensure that the company has an appropriate and effective risk management process.
5. The Chairman of the Enterprise Risk Management Committee shall report the meeting results to the Board of Directors at the subsequent meeting.
6. Perform duties as assigned by the Board of Directors.

2. Chief Executive Officer and Managing Director.

1. Monitor the organization's key risks and ensure that appropriate risk management plans are in place.
2. Promote the risk management policy and ensure that the risk management process is implemented throughout the organization.

3. Executive Vice President and Senior Vice President.

1. Monitor the organization's key risks and ensure that appropriate risk management plans are in place.
2. Promote a risk management culture and ensure that directors place appropriate importance on risk management within their respective areas of responsibility.

4. Strategy and Risk Management Department.

1. Act as the assistant secretary to the Risk Management and Corporate Governance Committee and be responsible for tasks as assigned.
2. Develop risk policies, frameworks, and processes for relevant departments, and submit them to the Risk Management and Corporate Governance Committee for approval.
3. Carry out day-to-day responsibilities on behalf of the Risk Management and Corporate Governance Committee.
4. Collaborate with various departments to identify and assess all types of risks across the organization.
5. Analyze the benefits of risk management and control options, including associated costs and administrative expenses, to support the selection of appropriate control methods.
6. Prepare risk reports for submission to relevant stakeholders.
7. Collaborate with departments to review risks in a standardized and systematic manner.
8. Monitor and coordinate with both internal and external parties in implementing risk management in accordance with policies and best practices, with a particular focus on enhancing the effectiveness and alignment of enterprise risk management with international standards.

9. Develop the risk management system, establish risk management policies, and set risk management objectives for the company's business operations, ensuring that business volatility has minimal impact on overall performance.
10. Prepare, review, and approve the annual operational risk management plans for each division, ensuring alignment with the five strategic perspectives: Financial & Market, Leadership & Governance, Workforce, Customer, and Product & Process. Monitor progress against the risk management plans.
11. Review changes in internal and external environments that may impact the company's short- and long-term operational objectives, in order to formulate strategic risk management plans and monitor their implementation.
12. Report performance results to the Executive Management Committee and the Risk Management and Corporate Governance Committee.
13. Promote and provide training to employees across the organization on enterprise-wide risk management.

5. Internal Audit Department.

1. Perform internal audits to provide assurance that the organization has adequate and appropriate internal controls for managing risks.
2. Communicate with the Strategy and Risk Management Department, as well as the Internal Control Department, to understand the organization's risks, conduct risk-based internal audits, and report findings to the Audit Committee.

6. Enterprise Risk Management Task Force

1. Develop the risk management plan and monitor the risk management performance of the company and its subsidiaries at all stages of operation, in accordance with the principles of good corporate governance, to reduce the likelihood and impact of risks and minimize uncertainties in overall performance.
2. Inspect, monitor, and assess the organization's risk management activities, providing quarterly reports to the Executive Management Committee for presentation to the Risk Management and Corporate Governance Committee.
3. The Enterprise Risk Management Task Force consists of the Strategy and Risk Management Department, the Internal Control Department, and risk managers and coordinators from each department, working together to manage and control organizational risks.

7. Internal Control Department

1. Establish internal control frameworks that cover all critical operational processes of the organization, such as production processes, sales processes, and procurement/purchasing processes, through self-assessment and internal control procedures known as Control Self-

Assessment (CSA). This includes monitoring and regularly reporting on the review of information, in accordance with the established risk assessment and control guidelines.

2. Provide recommendations for improving the internal control system to the company and its subsidiaries to ensure successful implementation of the risk management plan.
3. Raise awareness among executives and employees by regularly communicating information related to risk management and internal control practices.
4. Monitor and report on the implementation of risk management and internal control activities to the Executive Management Committee, the Audit Committee, and the Risk Management and Corporate Governance Committee.

8. Risk Manager.

1. Ensure that daily operations are sufficiently assessed, managed, and reported with regard to risks.
2. Promote awareness among employees in respective departments and functions regarding the importance of risk management.
3. Ensure that the risk management plan is fully implemented and regularly reviewed during departmental meetings.

9. Risk Coordinator.

1. Provide advice and coordinate with departments to ensure the implementation of risk management processes, including identifying, assessing, and managing various risks that may arise, to prevent or mitigate the level of risk.
2. Assist and support in organizing workshops to develop risk management plans at all levels.
3. Monitor and report on the progress of risk management plans at the departmental and functional levels.
4. Coordinate with the Strategy and Risk Management Department and the Internal Control Department.

Definition of Risk Management.

Risk is an uncertain event or situation that, if it occurs, could have a negative impact on achieving the organization's objectives and goals, including in areas such as strategy, operations, finance, compliance, and corporate reputation.

Risk can arise from changes in various factors, both external and internal, such as data errors, damage to information technology systems, fraud, new investments, price volatility and exchange rates, or natural disasters.

Risk management is the use of organizational culture, capabilities, and experience alongside the setting of objectives and strategic planning to assess the impact, the value of potential damage, and to prevent or mitigate the risks that may arise.

The Importance of Risk Management.

Risk management is an essential part of good corporate governance. It is a tool that helps organizations achieve their set objectives by preventing or minimizing the likelihood and impact of unexpected risks that affect the organization's operations, while also enabling the organization to capitalize on positive events (opportunities) quickly and effectively :

1. The ability to assess risks across all departments throughout the organization to analyze risks in a comprehensive manner and manage them integratively.
2. The ability to prioritize risks in order to use limited resources efficiently in managing those risks.
3. The board of directors and management have confidence in controlling operations in alignment with the business plan, with the remaining risks kept at an acceptable level.
4. Supporting the principles of good corporate governance, which can enhance the value of the business and build confidence among all stakeholders.

Effective risk management is driven by the following key factors:

- **Support.** – Senior management must provide support, demonstrate responsibility, and actively participate in risk management.
- **Processes.** – There must be effective risk management processes in place, which can be adapted to align with the organization's operations at all times, and be continuously implemented throughout the organization.
- **Personnel.** – Risk management occurs through cooperation and execution by employees at all levels, with clearly defined roles and responsibilities.
- **Communication.** – There must be regular communication of risk-related information, supported by training and the use of human resource management and information technology mechanisms to disseminate risk management information.

Chapter 2 : Enterprise Risk Management Approach.

Enterprise Risk Management Process.

The risk management process of BBGI Public Company Limited has adopted the principles of COSO Enterprise Risk Management (COSO ERM). The company has developed a process that is implemented by the Board of Directors, executives, and all personnel within the organization to identify, analyze, assess, prioritize risks that impact the achievement of the objectives of the department or organization. This includes the establishment of strategies and measures used to control and manage risks, as well as to monitor them, in order to ensure that the risks are managed within acceptable levels and to provide confidence in achieving the set objectives.

Risk management is an ongoing process linked to the strategic planning process. The identification of the organization's risks each year is based on the analysis and evaluation of various factors, including:

1. Consideration of the organization's 5-year long-term business strategy and risks related to key projects or plans that may hinder the success of each department's performance.
2. Analysis of global and national economic trends for the upcoming year that could potentially impact the company's operations.
3. Assessment of the impacts on the company's performance each year resulting from changes in internal and external risk factors.
4. Feedback from meetings of the Board of Directors, the Risk Management and Corporate Governance Committee, and the Audit Committee, including recommendations from external auditors.
5. Results of risk management, remaining risks (Residual Risk), obstacles, and lessons learned after managing risks in the previous year.

Levels of Enterprise Risk Management.

The company has categorized enterprise risk management into four levels: corporate level, business group and functional group level, project level, and process/department level. This structure ensures that the organization can achieve its objectives at every level of operation and enhance overall efficiency. The details are as follows:

- Corporate Risk.

Corporate risk refers to risks that may prevent the organization from achieving its overall business objectives. Examples include: Errors in setting strategic objectives at the corporate level, Investments in large-scale projects, Volatility in oil prices, exchange rates, interest rates, Changes in government policies or regulations, Opposition from society and local communities.

- Business Group/Unit Risk.

Risks that may hinder each business group or functional unit from achieving its objectives, such as planning errors, setting targets that are not aligned with the organization's strategic objectives, or implementing projects/activities that fail to meet customer needs or result in competitive disadvantages.

- Project Risk.

Risks that may cause a project to fail to meet its timeline, generate lower-than-expected returns, and/or exceed the allocated investment budget. Investment decisions for any project must be based on thorough and systematic project analysis to ensure that the project will achieve its objectives without causing negative impacts on the environment, society, and local communities. Project-related risks can arise at any stage of the project's lifecycle.

- Function Risk.

Risks that may prevent individual work processes—supporting the objectives of each business unit and the organization—from achieving their intended goals. Assessing these risks and implementing effective management plans, such as clearly defining approval authority, reviewing operational procedures, and conducting Control Self-Assessments (CSA), can help reduce recurring errors and mitigate various operational risks at this level.

Enterprise Risk Management Framework.

The company has established an Enterprise Risk Management Framework covering five key areas: Corporate Risk Management, Project Investment Risk Management, Business Continuity Management, Climate Risk Management, ESG Risk Management

- Corporate Risk Management.

It involves assessing risks from both internal and external factors, including future trends that may impact business operations, to ensure that the company can achieve its short-term and long-term goals. This risk management process is integrated and aligned with strategic objectives at the corporate, business group, division, and department levels. At the process level, risk management involves evaluating risks within operational workflows to identify areas susceptible to fraud, critical errors, accidents, or inefficiencies. Appropriate controls, preventive measures, or audit mechanisms are then implemented to mitigate these risks.

- Project Investment Risk Management.

All investment projects must have a risk management plan that aligns with the project's timeline and is appropriate to its nature. The plan should include an assessment of the resources required for managing those risks. For investment projects that require approval from the Board of Directors, the risk management plan must first be reviewed and approved by the Risk Management and Corporate Governance Committee before being submitted to the Board for investment approval.

- Business Continuity Management.

This involves assessing risks from various events that may disrupt business operations, and developing a Business Continuity Management (BCM) plan in conjunction with the Emergency Response Plan of the safety department. The objective is to ensure preparedness in terms of resources and response strategies in the event of a crisis. The organization also ensures regular monitoring and review of operational procedures in alignment with the Business Continuity Management Manual.

- Climate Risk Management.

This involves assessing climate-related risks or opportunities, categorized into Physical Risks and Transition Risks.

- ESG Risk Management.

This involves assessing risks or opportunities related to sustainability, which includes the following key areas:

1. Health & Safety Risk – This refers to the assessment of how well the organization cares for and prioritizes the well-being of its personnel, ensuring good health and the prevention of injuries or illnesses resulting from work activities.
2. Human Rights Risk – This involves assessing compliance with human rights principles to prevent violations of the rights of employees, business partners, and local communities.
3. Other ESG-Related Risks – This involves assessing risks or opportunities arising from emerging events or risk factors that may significantly impact business operations over the next three to five years. It includes the development of effective risk mitigation measures and continuous monitoring of emerging risks in both the medium and long term. The objective is to minimize the impact of these emerging risks and help the company achieve its strategic goals and defined direction.

Chapter 3 : Enterprise Risk Management Process.

Enterprise Risk Management Process.

1. Objective Setting/Establishing the Context.

The establishment of objectives at the organizational, business group/unit, department, or process level must align with and support the organization's Vision, Mission, Strategy, core policies, and key goals.

A well-defined objective should state what the organization or department expects to achieve, focusing on the desired 'outcome' rather than the 'process' of operations. Objectives can also be set based on new initiatives aligned with the organization's business direction, as well as regular tasks necessary for business continuity. Additionally, setting effective objectives should take into account the needs and expectations of the organization's various stakeholders.

The process of linking different levels of risks within an organization.



(It can be applied to an organizational structure that evolves with business expansion.)

In addition, the organization should clearly define objectives and strategies and communicate them to relevant departments within the organization to ensure mutual understanding, using the "SMART" principles.

- | | |
|----------------------|-----------------------------------|
| • S pecific | เฉพาะเจาะจง |
| • M easurable | สามารถวัดได้ |
| • A lignment | สอดคล้องกับนโยบายหรือเป้าหมายหลัก |
| • R ealistic | สามารถทำให้สำเร็จผลได้จริง |
| • T ime-bound | มีช่วงเวลากำกับที่แน่นอน |

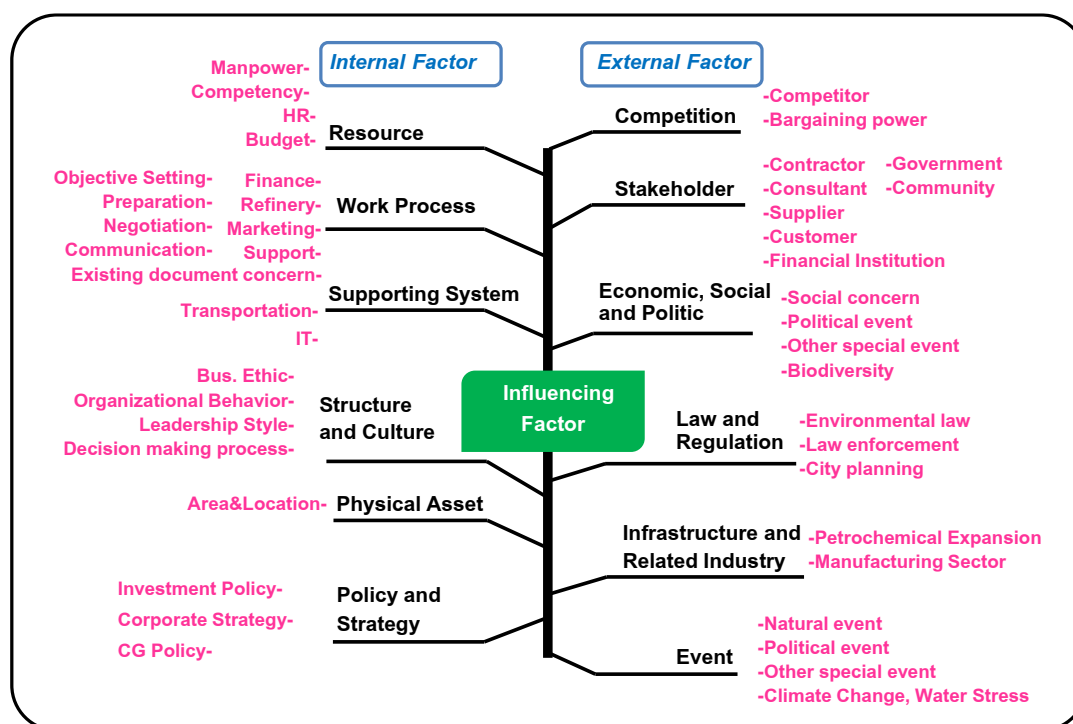
2. Risk Assessment.

The risk assessment process is divided into three sub-steps as follows:

2.1 Risk Identification It is the process of identifying the risks associated with the organization's operations, covering all types of risks, both internal and external. This includes identifying significant risks such as damages that may have a negative impact on the organization, uncertainties that could affect the achievement of objectives, and events that might cause the organization to miss opportunities to achieve its objectives.

The risks that an organization faces arise from risk drivers which stem from both internal and external factors. Internal factors include elements like organizational culture, human resources, and internal processes. External factors include influences such as technology, politics, economic conditions, and financial environments.

The different types of risk drivers can be illustrated as follows:



The company has categorized risks into four groups (SOFR), which are as follows: Strategic Risk, Operational Risk, Financial Risk, Reputational Risk

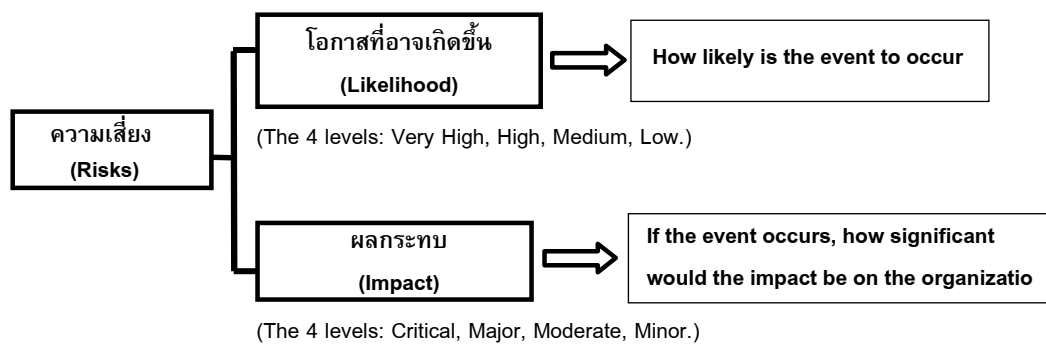
- Strategic Risk** refers to the changes in the business environment that impact an organization's ability to operate and achieve its strategic objectives. These changes can affect the organization's ability to implement its strategy both in the short and long term. Examples include shifts in global trends, technological advancements, competition, government policies, and investment risks resulting from changes in the business environment. These risks can have significant effects on long-term goals or plans, such as the volatility of oil prices, changes in government policies, or economic conditions. In summary, Strategic Risk is the risk that arises from the potential inability to achieve strategic objectives due to external or internal changes in the business environment.

- **Operational Risk** refers to the risk that impacts operations, affecting production processes, including risks related to the management of raw materials, such as issues with quantity, quality, personnel, work systems, and a lack of effective process controls. These risks can lead to errors in operational processes, which in turn affect business objectives.
- **Financial Risk** refers to the risk arising from changes in financial and economic conditions, such as fluctuations in exchange rates, interest rates, liquidity, and tax rates. It also includes risks related to cash flow management in operations.
- **Reputation Risk** refers to the risk arising from actions that affect the image and reputation of the organization. It includes risks related to the environment (Environment Risk) both within and outside the factory area, safety and health risks (Safety and Health Risk), as well as risks that may arise from fraud, corruption, or non-compliance with laws and regulations:
 - **Fraud and Corruption Risk** refers to the risk arising from actions or omissions in the performance of duties or the abuse of power in official positions, involving violations of laws, ethics, company regulations, or policies for personal gain. This includes activities such as requesting, receiving, offering, or providing assets, or any other benefits to government officials or individuals doing business with the company.
 - **Compliance Risk** refers to the risk arising from actions that do not comply with laws, regulations, or standards. This includes compliance with regulations from bodies such as the Stock Exchange of Thailand, or other relevant legal frameworks.

The important aspect of identifying and recognizing risks is to pinpoint the true root cause, rather than the consequences. In this step, it is common to find that existing problems, which require resolution, are mixed up with risks that need to be monitored. This can lead to the mismanagement of risk and deviating from the intended objectives. Therefore, it is essential to distinguish between problems and risks from the outset.

This can be analyzed based on the likelihood of the risk factor or event occurring. If the risk factor has a definite chance of occurring, it can be concluded as a "problem." However, if the factor has a possibility of occurring or not occurring, it should be categorized as a "risk." Then, the identified risk factor should be formulated into a Risk Statement accordingly to develop appropriate risk management measures.

2.2 Risk Analysis refers to the consideration of the risks that exist before any controls are implemented (Inherent Risk), under the current control activities, and the residual risk that remains after additional risk management plans are applied. It involves assessing the severity, including the magnitude of the impact caused by the risk, and the likelihood of that risk occurring. The analysis can be divided into two dimensions, where the company categorizes the levels of potential occurrence and impact into four levels as follows:



Example: Criteria for Assessing the Likelihood of Occurrence

| Level. | | Evaluation Criteria. |
|--------|------------|--|
| 4 | Very High. | <ul style="list-style-type: none"> - Likelihood of occurrence > 80%. - Likely to occur within this year. - Has occurred frequently in previous operations. |
| 3 | High. | <ul style="list-style-type: none"> - Likelihood of occurrence > 50-80%. - Might occur. - Has occurred several times in past operations. |
| 2 | Medium. | <ul style="list-style-type: none"> - Likelihood of occurrence 20-50%. - Might occur depending on certain factors. - Has occurred occasionally in past operations. |
| 1 | Low. | <ul style="list-style-type: none"> - Likelihood of occurrence < 20%. - Unlikely to occur this year. - Has rarely occurred in past operations. |

Example: Impact Assessment Criteria which can be categorized into 5 areas as follows: Financial & Market, Leadership & Governance, Workforce, Customer, Product & Process. Each area has specific criteria to determine the impact, as detailed below.

1. **Financial & Market** refers to risk factors that may impact:

- Profitability.
- Shareholder's Expected Return & Financial Ratio.
- Existing Market Share Growth.
- Profitability from Innovation.

2. **Leadership & Governance** refers to risk factors that may impact:

- Community Engagement & Corporate Social Responsibility.
- Environment.
- Strategic Objective, Deployment & Communication.
- Good Governance.

3. **Workforce** refers to risk factors that may impact:

- Capacity.
- Capability & Workforce Development.
- Workforce Climate.
- Engagement.

4. **Customer** refers to risk factors that may impact:





- Satisfaction / Dissatisfaction.
- Relationship, Retained Customer & Customer Activities.

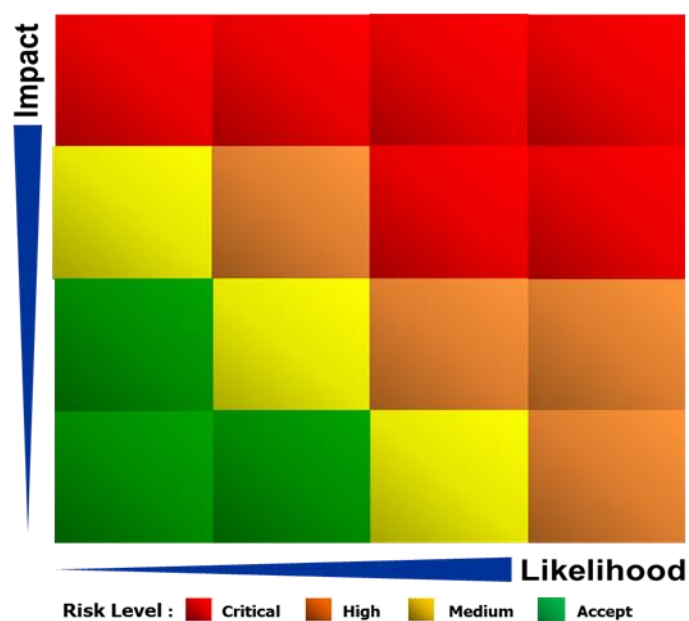
5. **Product & Process** refers to risk factors that may impact:

- Quality of Products and Services.
- Effectiveness / Efficiency of Production.
- Construction and Network Expansion.
- Safety & Emergency Preparedness.
- Innovation & Project Development.

In determining the Likelihood and Impact levels 1-4, there must be supporting evidence for the risk severity assessment criteria that have been defined. This may refer to past data, potential future scenarios, the development of probability models, interviews, or the establishment of comparative benchmarks, among others.

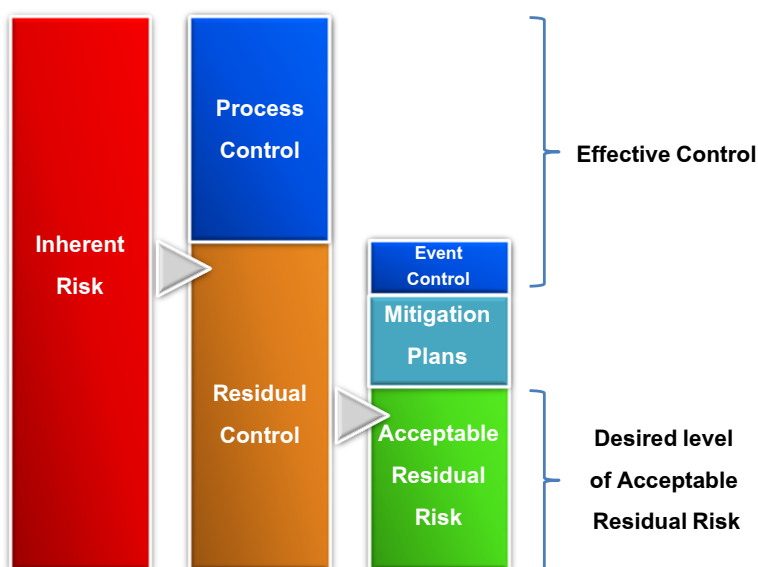
2.3 Risk evaluation is divided into 4 levels, as follows

-  - **Critical:** Extremely high risk, unacceptable as it has a significant impact on the organization. Management measures must be implemented and executed urgently to reduce the level of risk.
-  - **High:** Unacceptable high risk, as it has significant impacts on the organization. Management measures must be implemented to reduce the level of risk.
-  - **Medium:** Acceptable risk, but measures must be in place for monitoring, correction, and prevention to reduce potential losses.
-  - **Accept:** Acceptable risk, with minimal impact on the organization.



However, management should pay attention to risks that have a high level and a high likelihood of occurrence. They must also consider other factors, such as some types of risks that may have a high likelihood of occurring, even though the damage caused by such risks each time may be small. However, in the overall picture, it could lead to significant harm to the company (Black Swan Risk Management).

3. Risk Mitigation / Risk Treatment.



When starting without risk management, the company likely has some level of risk (Inherent Risk). Later, the company established a process to review risks at the process level and improved or controlled the processes (Process Control) by implementing control activities to reduce the likelihood of risks or errors in various tasks.

Control Activities refer to operational processes that are established by everyone in the organization, from the board of directors, executives, to all levels of employees, to provide reasonable assurance in achieving the organization's or unit's objectives. The primary goal of these control activities is to ensure that operations can achieve the set objectives and targets by minimizing errors. Additionally, they aim to improve operational efficiency and effectiveness, enhance the reliability of financial and operational data and reports, ensure compliance with laws and regulations, and oversee the organization's assets. Examples of control activities include:

- Establishing work procedures (QIP Work Process), defining job responsibilities (Job Description JD), and clearly outlining the approval authority in performing tasks.
- Establishing review steps in each operational process.
- Implementing IT systems to replace manual systems.
- Controlling access and inventory management of assets.
- Etc.

The principle in establishing these control activities should be integrated into the operations. The stringency of these control activities should depend on the importance, the assessed level of operational risk, and the organization's acceptable risk tolerance.

Once the organization has implemented risk management for its regular operations, reducing risks to a certain level, the organization also considers risks from abnormal events by developing a Business Continuity Management (BCM) plan to control such events (Event Control).

If the department assesses that the control activities and contingency plans prepared are still insufficient to bring the remaining level of risk (Residual Risk) to an acceptable level, the department must manage the risk by developing a risk mitigation plan (Mitigation Plan) to reduce the risk to the desired or acceptable level (Acceptable Residual Risk).

Risk Response is the process of defining actions to prevent potential risks and damages, using one or more methods combined, based on the 4Ts principles, which include:

| | |
|-----------|--|
| Take | Accepting the risk means using the same methods to manage the risk without taking any additional actions. |
| Treat | Finding additional control methods to manage or reduce undesirable outcomes by oneself, or reducing the risk to a desired level, such as implementing emergency plans, establishing safety standards, etc., with the following supporting measures: <ul style="list-style-type: none">- Directive.- Preventive.- Detective.- Reductive. |
| Transfer | Transferring the risk to others to share the responsibility, such as through insurance, outsourcing to external parties, or finding partners or joint ventures to share the risk. |
| Terminate | Not accepting the risk, which leads to a change in the originally defined objectives. |

Degree of Acceptance.

In determining risk management approaches, it is necessary to analyze the degree of acceptance or satisfaction with the existing measures (Degree of Acceptance) by comparing them with the level of risk and the available resources, using the following criteria:

| Degree Of Acceptance | Existing Risk Management Measures | Effectiveness of Risk Management | Level of Risk | Guidelines |
|----------------------|--|--|---------------------------------|--|
| Accepted. | Matches the cause of the risk and is effective. | Already producing good results. | At an acceptable level. | Continue implementation and monitor for any changes. |
| Mitigating. | Matches the cause of the risk but is not yet effective or fully implemented. | Results are still unsatisfactory; the plan must be enforced more strictly. | Not yet at an acceptable level. | Ensure existing measures are effectively implemented or intensify efforts. |
| Volatile. | Does not match the cause of the risk. | Results are still unsatisfactory; additional measures/plans need to be identified. | Not yet at an acceptable level. | Add measures that directly address the cause of the risk. |
| Unaccepted. | None. | Additional measures/plans need to be identified. | Not yet at an acceptable level. | Develop measures that directly address the cause of the risk. |

After prioritizing the remaining risks (Residual Risk) following the implementation of additional risk management plans, and identifying the risk management methods used to eliminate or reduce risks that the organization has considered but found to have no existing risk management plan or where the current activities are insufficient, the organization must study the feasibility and costs of each alternative to make a systematic decision on the risk management method, considering both costs and benefits.

Cost-Benefit Analysis.

In reality, every risk management method will incur direct or indirect costs that must be weighed against the benefits gained. Therefore, it is necessary to consider the initial costs (processes, people, and technology) involved in designing and implementing the chosen risk management method, as well as the costs required to maintain the method for continued use in the future. Costs and benefits can be measured either quantitatively or qualitatively, using units that are consistent with those used to define the relevant objectives and the acceptable risk deviation range. Proper risk management should not involve methods with costs higher than the benefits to be gained.

Considering the selection of a risk management method that provides more benefits than the costs or expenses required, and can maximize the use of limited available resources, involves the following key steps:

1. Identify the alternative risk management methods that can be used to manage the specific risk.
2. Identify the benefits that will be gained from each risk management method, both those that can be quantified in monetary terms and those that cannot, such as achieving objectives, improving work efficiency, saving time or resources within the organization, reducing impacts or the likelihood of risks, etc.
3. Identify the costs or expenses (Cost) required for each risk management method, both those that can be quantified in monetary terms and those that cannot, such as time, personnel, or other resources needed for managing the risk, as well as any limitations or obstacles in managing the risk, etc.
4. Consider the selection of a risk management method by comparing the benefits gained with the costs or expenses required:
 - **Benefits** include the immediate results that occur when the measure is implemented to reduce the risk, the reduction in expected damage (Expected Loss), returns, expansion of customer base, or long-term benefits, including future business opportunities. This is considered in both monetary and non-monetary terms, etc.
 - **Costs** include the costs, budget, personnel, technology, processes, time, or convenience that may be lost due to the risk, or the potential risk that may occur again in the future. This is considered in both monetary and non-monetary terms, etc.

Assigning responsibilities and defining the timeline for implementation.

Once the risk management method is selected, it is necessary to assign responsibility for implementing the measures and set a timeline for execution to ensure effective risk management.

Key Risk Indicator. (KRI)

Key Risk Indicator (KRI) is a tool used to measure activities that may increase an organization's risk exposure. There can be multiple KRIs, depending on the identification of risk causes. KRIs can be beneficial in the following ways:

1. Used to assess the direction of risk trends—whether risks are increasing or decreasing.
2. Serves as an early warning signal to help identify causes and implement timely corrective actions.
3. Supports quantitative risk measurement and internal control activities.
4. Demonstrates the interrelationship of risk management across different areas of the organization, such as operations and finance.
5. Used to monitor whether risk management efforts are meeting set objectives, enabling improvement or adjustment of risk management plans for greater effectiveness.

Examples of Key Risk Indicators:

| Risk. | Key Risk Indicators. |
|-------------------------------------|--|
| Revenue Volatility. | <ul style="list-style-type: none">• Ethanol Price.• Customer Satisfaction Rate.• Customer Complaint Rate.• Exchange Rate Volatility. |
| Production delays against the plan. | <ul style="list-style-type: none">• Delay in Raw Material Delivery Time.• Overtime Labor Cost Increase Rate.• Amount of Waste.• Unplanned Shutdown. |
| Shortage of qualified personnel. | <ul style="list-style-type: none">• Employee Turnover Rate.• Number of Training Hours. |

Risk Appetite and Risk Tolerance.

Risk Appetite It refers to the overall level of risk that the organization is willing to accept in pursuit of its mission or vision. It should be defined in alignment with KPI targets or the objectives outlined in the business plan.

Risk Tolerance It refers to the acceptable level of deviation from the criteria or performance indicators related to achieving the objectives. This should be defined in alignment with the KPI targets.

The determination of Risk Appetite and Risk Tolerance must be aligned with the organization's operational goals and objectives. The acceptable level of risk depends on the organization's risk response behavior, which can be categorized into three main groups:

- Risk Averse.
Conservative in nature; generally avoids taking risks. Well-established risk management and monitoring plans are in place to mitigate potential threats.
- Risk Neutral.
Accepts a moderate level of risk. Resources are allocated in a balanced manner to manage risks while maintaining operational efficiency.
- Risk Seeker
Tends to take high levels of risk and willingly accepts such risks without implementing specific mitigation or control measures.

4. Monitoring and Reporting.

This is the final process for regularly and continuously reporting risks from all departments across the organization. It ensures that risk management practices are implemented organization-wide and provides confidence to management to review the status of risks and make timely, effective decisions. A Risk Assessment Form (see example in the appendix) is used to monitor the implementation of risk management plans and to review the severity levels of risks. The process is carried out as follows:

Enterprise Risk.

1. Departments monitor Key Risk Indicators (KRIs), progress of risk management plans, and review risk levels during departmental meetings. (See examples of KRI monitoring in the appendix.)
2. The Strategy and Enterprise Risk Management Department tracks enterprise-level risks quarterly, based on reports from Risk Coordinators in each department.
3. The Strategy and Enterprise Risk Management Department consolidates and prepares enterprise risk reports to present to the Risk Management Committee and the Corporate Governance Committee for overall oversight, and subsequently presents the meeting summaries to the Board of Directors for their acknowledgement.
4. Communicate risk assessment results and committee feedback from the Risk Management Committee (RMC) meetings to the relevant departments.

Business Unit Level Risk.

1. Risk Owners report to the Risk Manager to review the implementation of risk management plans and to adjust risk levels according to the established plan.
2. The Strategy and Enterprise Risk Management Department monitors high-level risks at the business unit/department level and tracks the scheduled risk level reduction (Effective Date) from Risk Coordinators on a quarterly basis.
3. The Internal Control unit monitors risks at the business unit/department level from Risk Coordinators annually. If an increase in risk level is identified, coordination with the Strategy and Enterprise Risk Management Department is required to consider elevating the risk from the business unit/department level to the enterprise level.
4. The Enterprise Risk Management Working Group supports Risk Owners in raising risk awareness to enable proper and comprehensive application of risk management in their daily operations.

The diagram illustrates the Risk Management Framework (RMF) and its integration with the Risk Workshop. The framework is organized into three main horizontal layers: BoD (Board of Directors), RMC (Risk Management Committee), and CS (Chief Security Officer). The flow of information and decision-making is as follows:

- BoD Layer:**
 - เป้าหมายองค์กร/สายงาน/ส่วนงาน (Organizational/Divisional/Departmental Goals)
- RMC Layer:**
 - พิจารณาคัดเลือกเป้าหมายองค์กร (Consider and select organizational goals)
 - กำหนดเป้าหมาย (Set goals)
 - พิจารณา (Consider)
 - กำกับดูแล (Monitor and control)
- CS Layer:**
 - ประสานงาน/ควบคุม (Coordinate/Control)
 - ติดตาม/ควบคุม/ประเมินผล (Monitor/Control/Evaluate)

The **Risk Workshop** is a central component that feeds into the RMC layer. It includes:

- ความเสี่ยง (Risk):
 - ระดับองค์กร (Organizational level)
 - ระดับสายงาน (Divisional level)
 - ระดับส่วนงาน (Departmental level)
 - บริษัทในเครือ (Subsidiaries)

The Risk Workshop also feeds into the CS layer, specifically into the **ติดตาม/ควบคุม/ประเมินผล** (Monitor/Control/Evaluate) step, which includes:

- ดำเนินการตามแผนจัดการเพื่อลดระดับความเสี่ยง (Implement the plan to reduce risk levels)
- กำหนด/ให้ข้อมูล KRI (Determine/provide KRI information)

The diagram also shows a feedback loop between the CS layer and the RMC layer, and a feedback loop between the RMC layer and the BoD layer. The overall process is iterative and continuous.

Enterprise Risk Management Handbook of BBGI Public Company Limited.
Updated for the year 2024, dated 27 November 2024.

Chapter 4 : Risk Management Models.

Strategic Risk Management.

Strategic Risk Management refers to the management of risks that are most critical to the organization's survival. These risks directly impact the success or failure of the organization. Unlike other types of risks, strategic risks often lack quantitative tools for identification, analysis, and prioritization. However, while strategic risks can have negative effects on the organization, if managed well and leveraged appropriately, they can also become opportunities that drive the organization toward success.

Examples of Strategic Risks include:

1. Risks that may impact the success or failure of the organization, affecting the formulation or planning of strategies in various areas.
2. Risks that may affect the organization's ability to operate and achieve its strategic objectives or to implement its strategies effectively.
3. Risks that the strategies adopted and planned by the organization may become misaligned with changing circumstances or the operational environment.
4. Emerging risks that the organization must be aware of and prepare for, involving new events that have never occurred before but could cause significant harm, such as COVID-19 and Artificial Intelligence. (AI)
5. Sustainability risks (ESG Risks) that the organization must prioritize and manage internally, covering environmental, social, and corporate governance and economic dimensions.
6. Risks or opportunities related to climate change, as the world faces unavoidable environmental challenges, particularly climate risk. The company focuses on business operations that may pose risks related to climate issues, including transition risk and physical risk.

Therefore, effective strategic risk management requires a robust management system. It begins with identifying which changing factors could trigger risks and what impact those risks might have on the organization. Subsequently, the organization must develop a system to monitor these risks continuously. When there is a likelihood or trend indicating the potential occurrence of such risks, an alert system should notify management of the impending risks. The most critical factor for successful strategic risk management is the awareness and commitment of senior executives.

Useful tools that can be applied in identifying and managing strategic risks include conducting a SWOT analysis, which aims to identify the organization's Strengths, Weaknesses, Opportunities, and Threats. Additionally, strategic risk monitoring and surveillance involve Environmental Scanning, which consists of analyzing both the external and internal environments of the organization.

1. External Environment Analysis.

Refers to the examination of the general environment, which does not directly involve the organization but can impact it. The analysis is typically conducted using the PESTEL framework, which considers the following factors: Political (P), Economic (E), Social (S), Technological (T), Environmental (E), and Legal (L) environments.

2. Internal Environment Analysis.

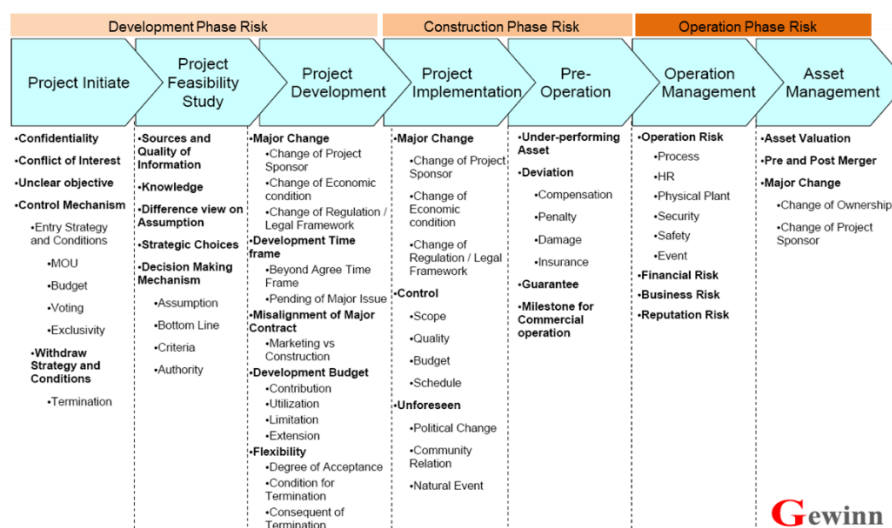
- **Analysis of the operational environment using The Five Competitive Forces Model**, which helps identify the capabilities of existing and potential competitors, understand customer demands, be cautious of customers shifting to substitute products, and foster collaboration with suppliers of raw materials.
- **Analysis of Critical Success Factors (CSFs)** involves identifying the essential factors that must be in place or achieved to realize success according to the organization's vision. This links the operations at all levels to move in the same direction, ensuring that staff and management understand what needs to be done to meet organizational objectives effectively and efficiently. Without these critical success factors, the organization's vision cannot be fulfilled as intended.
- **Understanding and analyzing the Value Chain** to comprehend the role of each unit in helping the organization create value for customers. The value created by the organization can be measured by the extent to which customers are willing to pay for its products or services.
- **Understanding and analyzing Core Business Processes**, which are the value-creating processes that connect suppliers, the organization, and customers, enabling product development, service delivery, and fulfillment of customer needs.

Project Risk Management.

Investment project risk management is a critical and essential aspect of business operations. It requires a clear and systematic analysis of the project to ensure confidence that the project will achieve its goals or objectives without adversely affecting the social and community environment. Risk considerations are categorized according to each phase of the project timeline as follows:

1. Development Phase Risk.
2. Construction Phase Risk.
3. Operation Phase Risk.

Additionally, the consideration of risks from natural disasters must also be included.



Project managers or investment project leaders must prioritize risk management by incorporating it as part of the project management plan. This includes risk assessment and analysis, prioritization, risk control, and continuous risk monitoring. Utilizing available resources efficiently within limited timeframes is essential to minimize the risk of project failure and to ensure the successful achievement of project goals with effectiveness and efficiency.

Therefore, the company requires all investment project developers to conduct a risk assessment of their projects as part of the budget or investment approval process. The details are as follows:

1. Every investment project must develop a risk management plan that aligns with the project timeline and is appropriate for the project's scope. The plan should include an assessment of the resources and costs required to manage the risks. This process should reference the risk management procedures outlined in Chapter 3 of the Enterprise Risk Management Manual. The risk management plan will serve as supporting documentation for the approval and allocation of the investment budget.
2. Investment projects requiring approval from the Company's Board of Directors must obtain endorsement of the project's risk management plan from the Risk Management and Corporate Governance Committee prior to submission for approval by the Board of Directors.
3. For other investment projects with budgets below the threshold requiring Board approval, the authorized investment approver may seek risk management opinions from the Risk Management and Corporate Governance Committee to support their investment approval decision.

Portfolio View of Risk.

This involves an overview of key organizational risks that significantly impact financial performance or operational results against set targets, aiming to keep deviations below the defined thresholds. Senior management and the company's board are responsible for this risk consideration. The risk evaluation process includes the use of a Risk Map to analyze the relationships among various risk factors, resulting in a set of risks that describe the overall risk profile. It also examines risk concentration to identify which risk areas carry the most weight. This information guides management in applying risk diversification principles to reduce the impact of overly concentrated risks in any single area. The goal is to ensure that any potential losses remain within acceptable levels. This concept is based on the belief and assumption that each business transaction carries different types of risk, and by diversifying transactions rather than concentrating them in one area, the concentration of risk can be minimized.

The classification of transactions may initially be divided into monetary-related transactions and non-monetary transactions. Alternatively, they may be categorized according to types of risk, such as credit risk, market risk, liquidity risk, operational risk, and compliance risk. Transactions can also be grouped based on different target groups or by geographic concentration. Regarding the level of risk concentration, whether it is acceptable depends on the risk tolerance policy of each organization, existing standards, or alignment with industry best practices.

Portfolio View of Risk is a type of risk assessment process that looks at the overall picture. It acts like a diary that helps provide clearer visibility of risks and demonstrates the organization's management capabilities. Therefore, the components of the Portfolio View of Risk consist of three main parts:

- Part 1 : Modeling the company's portfolio.
- Part 2 : Defining tools for risk management.
- Part 3 : Organizing the structure and responsibilities to support risk management.

Part 1 : Modeling the company's portfolio.

Since each organization has different missions and goals, the design to create a portfolio simulation may vary. This allows for uniqueness, with the size and structure of the portfolio tailored specifically to suit the risk management needs of each organization.

In practice, organizations should create and design portfolio simulations using data from risk status assessments, risk maps, and risk movement derived from the Risk Assessment process or the Risk Management and Corporate Governance Committee. This approach eliminates guesswork by relying on quantitative data and reduces individual discretionary judgment in scoring risks. Furthermore, the data used for portfolio simulation should be continuously updated to enable management to create appropriate and effective models.

Part 2 : Defining tools for risk management.

This part involves identifying methods to govern and control the entire risk portfolio. The organization must define strategies, approaches, and alternative measures to eliminate or mitigate risks. It should also assess the feasibility of implementing these measures in various scenarios, along with evaluating the costs or expenses associated with each option. Responsibilities and timelines must be assigned to develop an action plan and monitoring measures for tracking the progress of risk management. This plan will then be submitted for approval in accordance with the risk management process previously described.

Part 3 : Organizing the structure and responsibilities to support risk management.

The organizational structure and risk management responsibilities may need to be revised by involving personnel more clearly in the implementation of action plans or risk management processes. This should be done through cross-functional or cross-departmental collaboration.

Therefore, the results from the Portfolio View of Risk serve as information for communication and knowledge sharing among operational personnel within the organization. They support collaborative analysis of the impacts that risk governance and control activities have on the organization's mission, goals, and key performance indicators (KPIs), and help drive behavioral changes in future risk management practices.

Key Characteristics of an Effective Portfolio View of Risk:

- 1) It should present a clear, easy-to-understand view and highlight key or critical issues.
- 2) It is not necessary to include every activity or all types of sub-transactions in the overall portfolio view. Instead, the focus should be on the organization's core activities or key transactions that align with its mission or carry significant levels of risk. Clear risk management measures should be in place to monitor the movement of risk after response actions have been taken, as well as to track the progress of risk mitigation efforts.
- 3) It should be able to present the portfolio in multiple dimensions while emphasizing or highlighting a focus on risk management.
- 4) It should be able to demonstrate the rationale and basis for determining the level and magnitude of risk, in order to support the development of risk management measures, particularly those linked to objectives and risk deviations.
- 5) The format and purpose of presenting the Portfolio View of Risk should allow for changes during the year in the event of significant changes in the business operating model or organizational restructuring, in order to reflect a more accurate and up-to-date picture rather than being fixed to a static format.
- 6) The development of a risk management performance evaluation system based on the Portfolio View of Risk must ensure that it enables executives to learn from and utilize the information for decision-making in selecting appropriate risk management approaches. It must also reflect data indicating that those responsible for the respective activities or businesses have comprehensive risk management plans in place for all materially significant aspects.

Appendix.

Definitions.

| | |
|-------------------------|--|
| Risk | Uncertain events may occur and have a negative impact on achieving objectives and goals. |
| Opportunity | Uncertain events may occur and have a positive impact on achieving objectives. |
| Inherent Risk | The level of risk before control/management is applied. |
| Residual Risk | The residual risk level after control/management has been applied. |
| Likelihood | The likelihood or probability of an event occurring. |
| Impact/Consequence | The impacts of the event, both monetary and non-monetary. |
| Current Risk Response | The existing risk management plan. |
| Risk Identification | Risk identification is the process of determining which risk factors impact the objectives. |
| Risk Owner | The risk owner or those directly involved with the risk have the capability to manage and reduce the risk level. |
| Effective Date/Due Date | The completion date for implementing measures, used to specify the target date for risk reduction. |
| Degree of Acceptance | The level of risk acceptance. |
| Risk Map | A diagram illustrating the relationships between risk factors and their quantitative and qualitative impacts, showing how they are interconnected and affect the objectives of various units within the organization. A Risk Map can assist in developing a more effective and comprehensive risk management plan that covers all relevant risk factors. |
| Risk Profile | A set of risks that illustrates various risks which may impact the objectives of different units. This includes information indicating the nature of the risks, types of risks, potential impacts arising from those risks, as well as other relevant risk-related data. |
| Risk Appetite | The overall level of risk that the organization is willing to accept in order to pursue its mission or vision. |

| | |
|-------------------------|--|
| Risk Tolerance | The level of deviation that the organization is willing to accept from performance criteria or indicators related to achieving objectives. |
| KRI | Quantitative indicators, activities, or events that signify changes in key risks affecting objectives. These can be utilized in risk management to monitor whether risk management outcomes align with targets, allowing for improvements or adjustments to risk management plans for greater effectiveness. In cases where the indicators serve as leading indicators, they can also be used to develop an early warning system for proactive risk management planning. |
| Risk Driver | Risk causes, which may arise from internal factors such as organizational culture, structure, personnel, or from external factors such as politics, competitors, economic conditions, and so on. |
| Cost & Benefit Analysis | An analysis of benefits compared to costs, both monetary and non-monetary, to support decision-making in selecting the appropriate method. When deciding on a risk management approach, consideration should be given to the benefits of reducing impacts or likelihood, compared against the costs or expenses incurred from implementing that risk management method. The chosen approach should provide benefits that outweigh the associated costs or expenses. |
| Risk Matrix | A 2-dimensional chart sized 4x4, consisting of an impact axis and a likelihood axis. Each axis is divided into 4 levels of severity, with the purpose of measuring the level of risk. |



BBGI PUBLIC COMPANY LIMITED

