Carabao Group Public Company Limited

Risk Management Manual

Document Revision History

Revision No.	Revision on page No.	Revision details	Effective date
00		Document created	August 2019
01		Revised in accordance with COSO2017 guidelines	May 2021
02	6	Sustainability Risk category added	July 2022
	7	Name list of Risk Management Committee removed	

CONTENTS Page

Introduction 3

Risk Management Definition and Overview 4

Risk Management Structure 7

Roles and Responsibilities in Risk Management 8

Risk Management Principles 9

Risk Assessment Process 10

Gross Risk Assessment 10

Step 1 – Identifying Organizational Objectives or Processes 10

Step 2 – Identifying Risk 11

Step 3 – Identifying the Cause and Effect of the Risk 12

Step 4 – Gross Risk Assessment 12

Residual Risk Assessment 13

Step 5 – Identifying Internal Control 13

Step 6 – Evaluating Control Effectiveness 13

Step 7 – Residual Risk Assessment 14

Step 8 – Preparing Risk Mitigation Plan 14

Risk Parameter and Measuring Criteria 17

Risk Assessment Monitoring and Reporting 20

Tools for Risk Assessment and Risk Reporting 21

Introduction

The Board of Directors of Carabao Group Public Company Limited (the "Company") realizes that risk management is part of good corporate governance, which is an important foundation for achieving the Company's goals. Identifying and managing risks will support the Company to make better decisions, seek opportunities, including reducing the severity of impacts from significant events that may occur to the Company, shareholders and all stakeholders. Effective Risk Management requires everyone in the organization to be involved in assessing the Company’s risks and potential impacts on a regular basis. This includes control planning to manage risk to an acceptable level for the organization. The Board of Directors has established a Risk Management Policy and appointed the Risk Management Committee. They are assigned with the monitoring of the risk management plan and considering its appropriateness.

The Risk Management Committee has prepared this Risk Management Manual to serve as a guideline for executives to assess risks and prepare risk management plans. The Risk Management Committee will review the risk assessment criteria, the organization’s acceptable risk level, and risk assessment process as referred in this manual at least once a year to ensure that the Company's risk management framework is corresponding with the Company’s current situation and business plan.

Risk Management Definition and Overview

Key Definitions in Risk Management

- Risk refers to the possibility that an event will occur and affect the achievement of given business strategies and objectives. Risks may be applied to one or more potential events, or they may be applied to all potential events collectively that may affect the achievement of strategies and objectives. Additionally, the main components of risk consist of how likely an event will occur which will be referred as "likelihood", and severity of the risk impact on the organization which will be referred as "impact".
- Risk Factor refers to the cause of risk that will hinder the achievement of given objectives or goals. Identified risk factors should be the actual causes in order to appropriately assess and assign risk mitigation measures. Risk factors can be considered both by internal factors (Organization's rules and regulations, work system efficiency, personnel potential, etc.) and external factors (economic, political, social, etc.).
- Enterprise Risk Management (ERM) refers to culture, capabilities, and practices integrated with strategic setting and its performance, that the organizations rely on to manage risk in creating, preserving, and realizing value.
- Risk Assessment refers to the process of analyzing and prioritizing risks that affect the organization's achievement of objectives or strategies. Risk level assessment will be considered from its impact and its likelihood.
- Risk Appetite refers to the type and amount of risk, on a Board level, the organization is willing to accept in pursuit of value.
- Strategy refers to the organization's plan to achieve its mission and vision and apply its core values.
- Business Objective refers to the measurable steps that the organization takes to achieve its strategy.
- Internal Control refers to a process, effected by the Board of Directors, management, and the other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

Risk Management Overview

Under the Good Governance Guidelines, the Risk Management Committee establishes the risk management policy, Risk Assessment Criteria, Risk Assessment Process, and Risk Management Manual, to ensure that the organization can operate in accordance with the given strategies and objectives by managing risk within the risk appetite.

The Risk Management Committee places great importance on the risk management of the organization since risks cannot be eliminated even if the operation was perfect. There are risks in general business operations, including the fast-changing environment which further complicates the risk and creates emerging risks which could affect the organization's strategy and objectives. Therefore, risk management is a crucial tool for the organization to mitigate uncertainty and allow the organization to perform efficiently adapt and manage the risks in a timely manner which lead to sustainable value creation for the organization and stakeholders.

Additionally, the Risk Management Committee places importance on the development of a systematic and continuous risk management framework. We support the application of international standard frameworks in the development of risk management tools of the organization, especially the Risk Management Framework of the Committee of Sponsoring Organization of the Treadway Commission, or "COSO", which has developed an Enterprise Risk Management – Integrating with Strategy and Performance framework and emphasizes the importance of risk assessment both in operation planning and implementing operation. Therefore, this Risk Management Manual was developed according to COSO guidelines with risk management principles as specified under "Risk Management Principles".

Risk Management Committee defines risk management covering 5 main categories as follows;

1. Strategic Risk

   Risks arising from strategic planning, operation planning, inappropriate implementation or inconsistent implementation according to strategy, including strategies that do not align with the Company's vision, mission, and core values which will affect the achievement of the organization's vision, mission, and core values.

2. Operational Risk

   Risks related to efficiency, effectiveness, or performance that may involve internal operation processes, personnel, work systems, or external factors that affect targeted operations and performance.

3. Financial Risk

   Risks related to financial management that might be caused by internal factors such as liquidity management, credits, investments, or external factors such as interest rates, foreign exchange rates, as well as risks related to the credibility of financial reports.

4. Compliance Risk

   Risks related to non-compliance with laws, rules, regulations, policies, and regulations established both by the organization and external regulators.

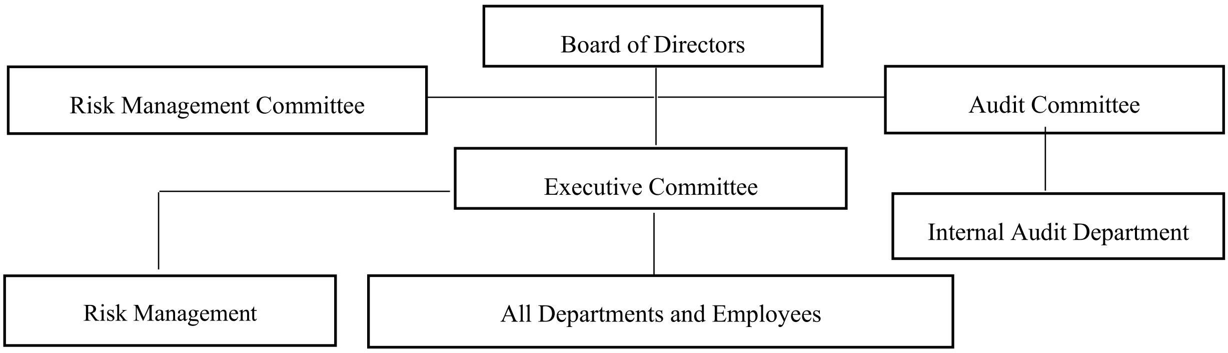
5. Sustainability Risk

   Risks related to "ESG" or environmental, social, and governance issues, also known as ESG Related Risk.

The Company has determined that risk management is the duty of everyone in the organization, so all departments must be aware of the risks within the performance of their departments and should regularly review all aspects of risk factors covering all types of risks (strategic risk, operational risk, financial risk, compliance risk, and sustainability risk) and must analyze and assess risks in order to find risk management mitigation and report risks to the Risk Management Committee on a regular basis.

Risk Management Structure

The Board of Directors realizes the importance of risk management and appoint the Risk Management Committee that consists of directors and executives, covering all major departments of the Company, to be responsible for assessing and managing risks throughout the organization as follows:


Board of Directors
Risk Management Committee
Audit Committee
Executive Committee
Internal Audit Department
Risk Management
All Departments and Employees

Roles and Responsibilities in Risk Management

The Company defines the roles, duties and responsibilities of each department in risk management as follows:

Audit Committee / Internal Audit Department

1. Reviewing the internal control system and risk management process according to acceptable international standards.
2. Providing an independent assurance on existing internal control's adequacy and effectiveness.

Risk Management Committee

1. Establishing policies, risk management frameworks, and organizational risk management structures.
2. Communicating organizational risk management policies and frameworks.
3. Defining the criteria for risk assessment, risk appetite, risk monitoring, and reporting guidelines.
4. Supporting executives in risk assessment as well as risk mitigation plan.
5. Monitoring progress and giving advice on risk management actions as necessary.

Executive Committee

1. Defining operational strategies by considering the risk appetite.
2. Promoting risk management culture within the Company.

Management of each function (risk owners)

1. Complying with the risk management policy and frameworks and communicating to create understanding among employees in the department.
2. Identifying and assessing risks.
3. Developing the risk register and risk mitigation plan.
4. Managing risks in accordance with the Company's framework to ensure that risks are identified, assessed, and responded to manage risks to an acceptable level.
5. Reporting risk and risk mitigation plan implementation progress.
6. Identifying emerging risks that may arise and reporting them in a timely manner.

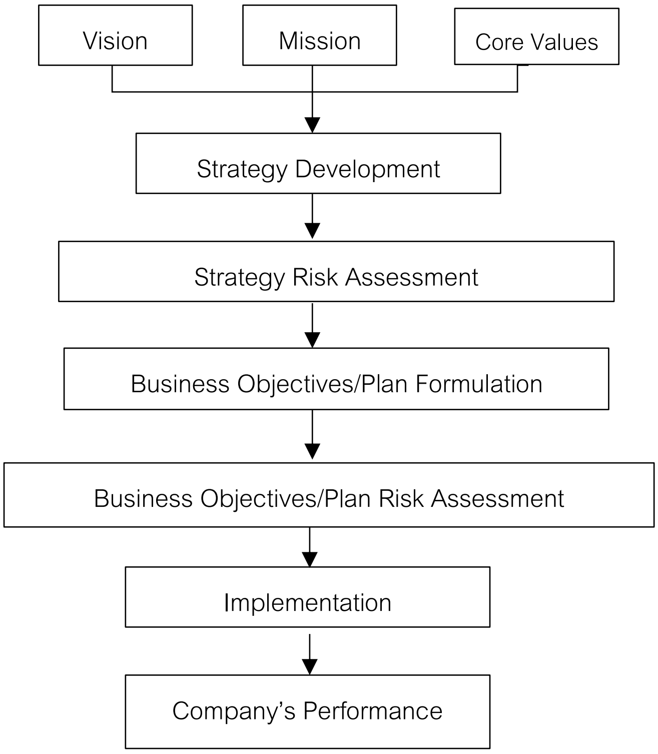
Employees

1. Executing the plan to ensure that risk management is part of daily operations.
2. Reporting significant risks or problems in risk management to supervisors in a timely manner.

Risk Management Principles

The Risk Management Committee is well aware of the increasing volatility, complexity, and ambiguity of the present business world which resulted in challenges for the organization that affect the confidence and trust of stakeholders. Therefore, stakeholders now play more roles, especially in seeking the company's transparency and responsibility in overall operation, including managing impact of organizational risk.

For this reason, the Risk Management Committee encourages the organization to prepare and adapt to changes, and think strategically about how to manage volatility, complexity, and ambiguity in the business world. The framework and principles of risk management that are integrated with strategies and overall operation to support performance growth are shown in the diagram below.



1. <u>The Organization's Vision, Mission, and Core Values</u>

The Company defines its mission, vision, and core values to show the Company's commitment to what we want to achieve in the future.

2. <u>Strategy Development</u>

The Company has set a strategy as a plan for the Company to achieve its mission and vision by applying core values. Therefore, the Company has to assess whether the adopted strategy supports its mission, vision, core values, and risk appetite. The Company also has to assess how the adopted strategy affects the company's risk profile, as well as, the possibility in coming out strategy formulation achieving its mission and vision.

3. <u>Defining Business Objectives</u>

The Company sets business objectives according to its strategy and distributes them to various business units and departments of the Company, from the management level to the operational level, including day-to-day job duties. Therefore, business objectives act as a link between strategies and practices. It is necessary for the Company to assess that the objectives are aligned with the strategy and risk appetite. This includes risks that affect the achievement of defined objectives.

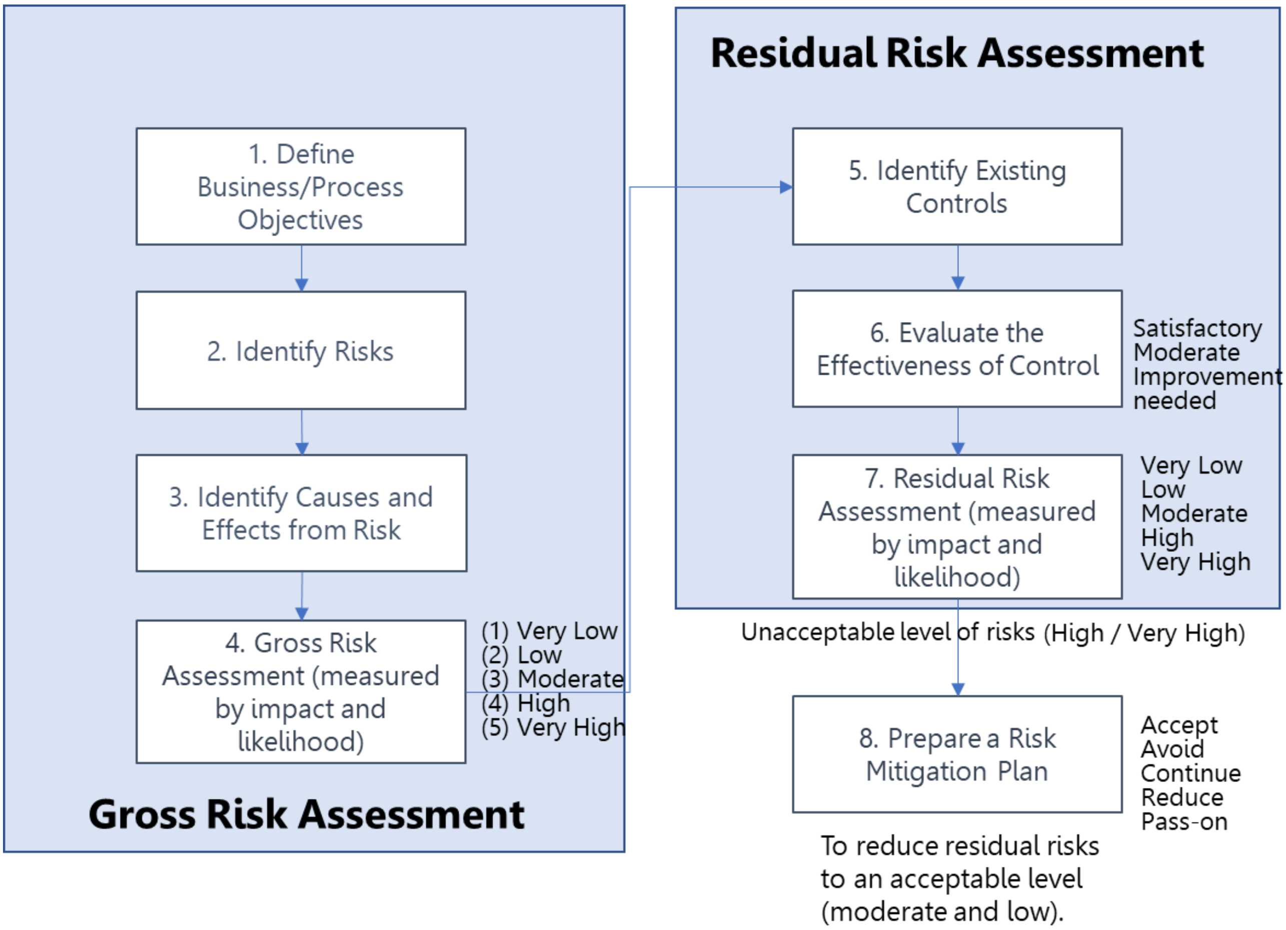
4. <u>Review and Revision</u>

The Company is required to identify and assess changes that may affect its strategy and objectives. Additionally, the Company must review its operating results, including considering risks that may cause the operation to not meet the target performance or prevent the Company from achieving its strategy and business objectives.

Risk Assessment Process

The Risk Assessment Process is divided into 2 main phases: Gross Risk Assessment, and Residual Risk Assessment. This may be done by arranging workshops or interviews with executives and/or related employees individually, whichever is appropriate.

The steps in the Risk Assessment Process are illustrated in the diagram below.


Residual Risk Assessment
1. Define Business/Process Objectives
2. Identify Risks
3. Identify Causes and Effects from Risk
4. Gross Risk Assessment (measured by impact and likelihood)
(1) Very Low
(2) Low
(3) Moderate
(4) High
(5) Very High
Gross Risk Assessment
5. Identify Existing Controls
6. Evaluate the Effectiveness of Control
Satisfactory
Moderate
Improvement needed
7. Residual Risk Assessment (measured by impact and likelihood)
Very Low
Low
Moderate
High
Very High
Unacceptable level of risks (High / Very High)
8. Prepare a Risk Mitigation Plan
Accept
Avoid
Continue
Reduce
Pass-on
To reduce residual risks to an acceptable level (moderate and low).

Gross Risk Assessment

Step 1 - Define Business /Process Objectives

The Company has defined a strategy to support the achievement of the mission and vision of the organization which complies with the level of risk acceptable to the organization. Then business objectives are set to identify the steps that follow the strategy. The company should distribute and communicate business objectives to departments at each level throughout the organization, so that they have the same understanding and are able to put the objectives into practice to support the success of the strategy. As a result, the identification of strategies and business objectives or processes is the first step in the risk management process. This step is to be used as a basis for identifying risks or events that may occur and negatively affect the achievement of strategies and objectives.

Step 2 - Identify Risks

This step is to identify risks or events that may arise from both internal and external factors, and are able to affect the achievement of a given objective or strategy. For the identification of risks, risk assessors should understand and know the objectives or clear goals of each job and any event or activity of the operational process that may lead to the achievement of work objectives. Risk assessors also need to have a clear understanding of the activities that are being carried out.

Examples of approaches that can be used to identify risks.

- Using the risk owners experience to identify events that have happened (Experience).
- Reviewing the Work Procedure Manual to determine what event may cause that activity to be halted or so erroneous that it can cause damage.
- Brainstorming Group consisting of employees who are involved in such activities both inside and outside the department. The group jointly consider whether there are any past events that have a negative impact on the work of which the group is in charge.
- Using Questionnaires to ask those in charge of such activities regarding problems, errors, risks of any kind, or the extent of damage caused by such activities. The Questionnaires can be applied to both past and future events.
- Cognitive Computing enables the Company to collect and analyze a large amount of data to detect future trends and provide insights to understand emerging risks, including changes in existing risks.
- Data Tracking from past events can help predict events that may occur in the future.
- Key Risk Indicators are used as early warning indicators to help identify events that may occur and negatively affect the activities or operations of the company.

Risks may come from internal and external factors, including:

Internal factors refer to internal risk factors that can be controlled, but can also negatively affect or hinder the implementation of the strategic plan to achieve a goal, for example,

- The organizational structure, operational procedures
- Adequacy or quality of personnel.
- Such factors arising from the information technology system include choosing inappropriate technology, the outdated technology due to the rapid emergence of new technologies, etc.
- Other examples are corporate culture, ethics of executives / employees / working environment.

External factors refer to obstacles from external factors that are difficult or unable to control, unable to turn into a favorable opportunity, or negatively affect and hinder the implementation of the strategic plan to achieve a goal, for example.

- Such factors arising from target customers include behavioral changes, attitudes, and lifestyles.
- Marketing examples are such as the competitiveness of the same product, substitute products, and new product groups.

- For technology, it can be the changes in related technologies.
- Politics and society factors include the continuity of government policy, outside interference, cooperation between stakeholders or related groups, protests, riots, or unemployment, insurgency, internal warfare, and border wars, etc.
- Environmental and natural disasters examples are such as floods, typhoons, mudslides, earthquakes, droughts, epidemics, lack of energy sources, etc.
- Financial and economic factors are such as labor shortages, consumer purchasing power, inflation, rising oil and energy prices, volatile interest rates and exchange rates, raw material price fluctuations, etc.
- Relevant laws, requirements, and regulations are such as ambiguity of relevant laws, changes in regulations, uncertainty about law enforcement, non-comprehensive laws, outdated regulations, changes to relevant resolutions, declaration of emergency which affects the business operations of the organization.

Step 3 - Identify Cause and Effect from Risk

This step is to analyze the cause or source of the risk, including potential effects from the cause of the risks. The underlying cause of the risk should be identified to analyze and determine measures to reduce risks correctly and appropriately.

Step 4 - Gross Risk Assessment

Gross Risk Assessment is a process that consists of analyzing, evaluating, and measuring risks affecting the achievement of the organization's work process objectives, without considering the existing controls. Two dimensions are considered to determine the risk level. Firstly, the effect or level of severity of risks and likelihood. There are 5 levels: very low (1), low (2), moderate (3), high (4), and very high (5).

However, the criteria for scoring in each level depends on the risk appetite of the organization. The Risk Management Committee has set a guideline in the topic of Risk Parameter and Measuring Criteria.

After considering the level, impact, and likelihood of the risk, the assessed risk levels will be shown in the diagram below, which are classified the risk levels into 4 levels: very high (red), high (orange), moderate (yellow). and low (green)

Diagram of gross risk levels

Assessment table		Probability of Occurrence				
Risk Level		**1 very Low**	**2 Low**	**3 Moderate**	**4 High**	**5 Very High**
Impact level	**5 Very High**	High	High	High	Very High	Very High
	4 High	Moderate	Moderate	High	High	Very High
	3 Moderate	Moderate	Moderate	High	High	High
	2 Low	Low	Moderate	Moderate	Moderate	High
	1 Very Low	Low	Low	Moderate	Moderate	Moderate

Residual Risk Assessment

Step 5 - Identify Existing Controls

This step is to identify the internal controls that exist or that management has established in the organization's operational procedures to reduce the impact and/or the likelihood that those risks may occur. Every risk that is identified is considered to determine the internal controls in relation to that risk. This information will be used to assess the effectiveness of the internal control in the next step.

Step 6 - Evaluate the Effectiveness of Control

After the activities and/or internal controls have been identified, the next step is to evaluate the effectiveness of the activities and/or existing internal control systems (identified in the previous step), considering the likelihood that such controls will be able to prevent potential risks, which may either mitigate the severity of the effects of the risks or reduce the likelihood of such risks. The effectiveness of the internal control is divided into 3 levels: satisfactory, moderate, and needing improvement.

Assessment of Control Effectiveness

Satisfactory	Controls are strong and operating properly proving a reasonable level of assurance that objectives are being achieved.
Moderate	Some controls weakness/inefficiencies have been identified. Although these are not considered to present a serious risk exposure, improvements are required to provide reasonable assurance that objectives will be achieved.
Improvement needed	Controls do not meet an acceptable standard, as many weakness/inefficiencies exist. Controls do not provide reasonable assurance that objectives will be achieved.

Step 7 - Residual Risk Assessment

In this step, the risk rating will be reviewed again to indicate the level of residual risk after considering the existing activities and/or internal control systems that can prevent potential risks and/or alleviate the severity of the impact when that risk occurs. The level of residual risk is measured from 2 dimensions, namely the impact and the likelihood of the risk occurring (scoring criteria for each level refer to the topic of Risk Parameter and Measuring Criteria)

Diagram of residual risk levels

Assessment table Risk Level		Probability of Occurrence				
		1 very Low	2 Low	3 Moderate	4 High	5 Very High
Impact level	5 Very High	High	High	High	Very High	Very High
	4 High	Moderate	Moderate	High	High	Very High
	3 Moderate	Moderate	Moderate	High	High	High
	2 Low	Low	Moderate	Moderate	Moderate	High
	1 Very Low	Low	Low	Moderate	Moderate	Moderate

The diagram above provides an example of measuring the level of residual risks in case an organization has effective internal controls. The initial risks which are previously assessed as having a very high level of risk appear in the upper right position of the risk table. Such risks can be moved to the moderate area. The details can be shown in the table if the organization has effective internal control.

Step 8 - Prepare a Risk Mitigation Plan

After assessing residual risks, the next step is to determine the level of residual risks whether it is at a level acceptable to the organization. If the remaining risk level still exceeds the level of risk appetite, management needs to develop a risk management plan to find ways to manage residual risks to be at an acceptable level for the organization.

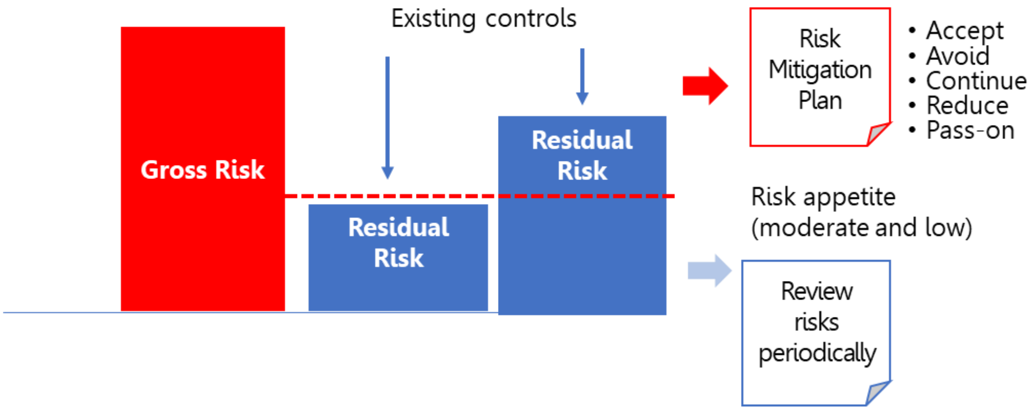
Assessment table Risk Level		Probability of Occurrence				
		1 Very Low	2 Low	3 Moderate	4 High	5 Very High
Impact level	5 Very High	High	High	High	Very High	Very High
	4 High	Moderate	Moderate	High	High	Very High
	3 Moderate	Moderate	Moderate	High	High	High
	2 Low	Low	Moderate	Moderate	Moderate	High
	1 Very Low	Low	Low	Moderate	Moderate	Moderate

Risk Mitigation Plan

Risk Appetite

Risk appetite refers to the type and amount of risk that an organization is willing to accept in pursuit of value. The Risk Management Committee determines the risk appetite for executives to use as a guideline for decision-making in formulating strategies, considering approval, and allocating resources in the organization. The Risk Management Committee determines the risk levels that the organization is willing to accept, namely the medium level (yellow) and low level (green) as shown in the diagram below. If the residual risk exceeds the acceptable level, that is, the high (orange) or very high (red) level, management should proceed with risk management plans to reduce the risk to the acceptable level. However, if the residual risk level is at an acceptable level (medium and low), the management is required to periodically review the risk to ensure that the residual risk level remains within the organization's acceptable level.

However, the management may review and adjust the acceptable risk level as necessary and appropriate in order to be in line with the current risk profile and risk management capabilities of the organization. The revised risk appetite then needs to be approved by the Risk Management Committee.



Risk Management Guidelines

There can be many approaches to managing risks, which may be considered from the Guideline for Risk Management to reduce the magnitude of the impact of damage and / or the likelihood of damage. Such consideration must take into account the cost-effectiveness and the benefits that will be obtained from such an approach.

Risk management approaches can be divided into 5 main approaches as follows:

1. **Accept** is to accept the risk. If such risks are within risk appetite, the organization may not have to do a risk mitigation plan. This may also be due to other reasons such as being unavoidable because it is a mission.
2. **Avoid** is a decision not to get involved in a risky situation or to stop conducting a risky activity. This often occurs in the event that the risk is higher than the risk appetite, and the cost of managing the risk may not be worth the benefits. Examples of avoiding are such as ceasing operations / activities that cause the risk or changes in business objectives, etc.

3. **Continue** is a decision to continue with the acceptance of a higher risk to achieve higher performance. It is necessary for management to understand the nature and extent of necessary changes during action in order to achieve the desired performance, while being careful not to exceed the boundaries of acceptable tolerance.
4. **Reduce** is to reduce the risk by defining control activities in order to reduce the "risk occurrence" or the "impact caused by the risk" such as the design of the internal control system, correction, improvement of work, etc. Control measures are divided into 4 types: preventive control, detective control, directive control and corrective control.
   - Preventive control is the control that is put in place to prevent risks and errors from occurring in the first place.
   - Detective control is the control to detect an error that has already occurred.
   - Directive control is the control that promotes or encourages the achievement of a desired objective.
   - Corrective control is the control that is put in place to correct an error that has occurred in order to prevent it from occurring again in the future.
5. **Pass-on** is the transfer of all or part of the risk to other agencies to manage or bear the burden of loss instead, such as taking out insurance hedging contracts, joint ventures, outsourcing, etc.

When applying any of the risk management methods mentioned above, risk management should be considered in the context of business, business objectives, performance goals, and the Company's risk appetite. Therefore, in some cases, management may need to consider other actions, including:

- Business Objective Review

  The severity of the identified risk and tolerance may cause the Company to choose to review and revise its business objectives. This may occur when the other categories of risk response do not represent the desired course of action for the entity.

- Strategy Review

  The severity of the identified risk and risk appetite may cause the Company to choose to review and revise its strategies. As with a review of business objectives,_this may occur when the other categories of risk response do not represent the desired course of action for the entity.

Risk Parameter and Measuring Criteria

The Risk Management Committee has set the criteria for assessing and measuring risks to provide guidance for risk assessors in measuring the level of risk. The following are considered the “impact (or severity) of the risk,” both financial and non-financial, and the “likelihood of risk”.

Financial Impacts

- Profit Targets
- Cashflow / Liquidity
- Project Cost

Score	Severity Level (*)	Impact on annual profit	Cashflow/Liquidity	Project Cost
1	Very Low	≤ 1%	Cashflow decreases by less than 1% from previous year./ No impact on financial liquidity.	Cost deviates from the budget not over than 1%
2	Low	> 1 - 2%	Cashflow decreases between 1 - 2% from previous year./ Little effects on financial liquidity, but normal operations can handle them.	Cost is higher than the budget within the range of 1% to 2%.
3	Moderate	> 2 - 5%	Cashflow decreases between 2 - 5% from previous year./ Some effects on financial liquidity.	Cost is higher than the budget within the range of 2% to 5%.
4	High	> 5 - 10%	Cashflow decreases between 5 - 10% from previous year./ Potentially severe effects on financial liquidity.	Cost is higher than the budget within the range of 5% to 10%.
5	Very High	> 10%	Cashflow decreases by more than 10% from previous year, causing a severe shortage of Financial liquidity	Cost is higher than the budget over 10%.

Non-Financial Impacts

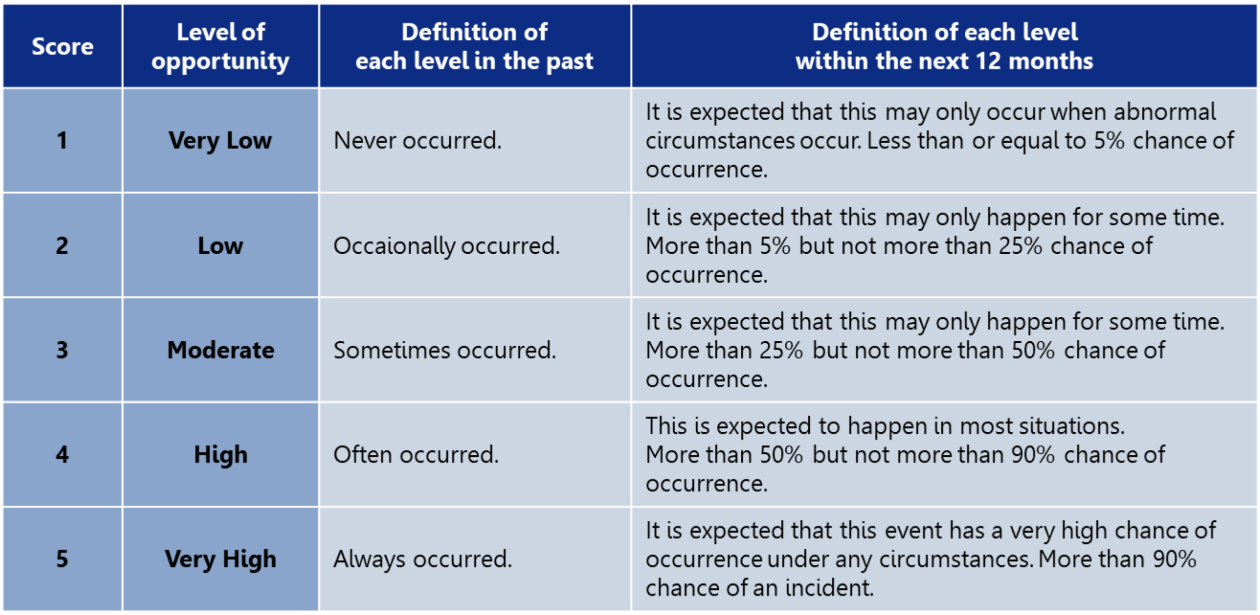
- Reputation, project delays, compliance with the law, personnel safety, business operations, information technology systems, and loss of personnel.

Score	Severity Level (*)	Image and reputation	Project delays	Non-compliance with relevant legal requirements	Safety of employees, customers, manufacturers, or third parties
1	Very Low	No news is published.	No more than 1 month delayed.	No effect	No injuries
2	Low	Limited news is published domestically for 1 day.	More than 1-3 months delayed.	Minor tendency to violating the law or regulations, still able to rectify.	Minor injuries, not severe.
3	Moderate	News is published in several domestic media outlets for 2-5 days.	More than 4-6 months delayed.	Minor violations of laws, regulations, or verbal warnings from regulatory authorities.	Injuries with outpatient medical treatment required.
4	High	News is widely distributed to domestic media and limited coverage by international media.	More than 6 months delayed.	Violations of laws, regulations, or written warnings from regulatory authorities.	Injuries with inpatient medical treatment required.
5	Very High	Headlines from both domestic and international media are widespread.	More than 1 year delayed.	Severe violations of laws and regulations, affecting the organization's financial and reputation and it may be sued or revoked.	Significant injuries or fatalities.

Score	Severity Level (*)	Business Operations	Information Technology System	Morale, or loss of personnel
1	Very Low	No impact to business operations.	insignificant incident.	Dissatisfaction with some groups of employees.
2	Low	Minor impact to business operations.	Minor incident which can be solved.	Dissatisfaction among some groups of employees, causing some resignations.
3	Moderate	Impact to business operations causing a disruption of more than 1 day but less than 3 days.	Some problems with the system, but not many losses.	Widespread dissatisfaction among employees and a large number of resignations.
4	High	Impact to business operations causing a disruption of more than 3 days but less than 1 week.	Critical problems with key IT and security systems, affecting the integrity of some data.	Resignations of some executive level employees.
5	Very High	Major impact to business operations causing a disruption of more than 1 week	Loss of all critical IT systems and significant damage to the security of customer or business data.	Numerous resignations of executive level employees.

Probability of Risk Occurrence

- Past events
- Future forecast



Score	Level of opportunity	Definition of each level in the past	Definition of each level within the next 12 months
1	Very Low	Never occurred.	It is expected that this may only occur when abnormal circumstances occur. Less than or equal to 5% chance of occurrence.
2	Low	Occaionally occurred.	It is expected that this may only happen for some time. More than 5% but not more than 25% chance of occurrence.
3	Moderate	Sometimes occurred.	It is expected that this may only happen for some time. More than 25% but not more than 50% chance of occurrence.
4	High	Often occurred.	This is expected to happen in most situations. More than 50% but not more than 90% chance of occurrence.
5	Very High	Always occurred.	It is expected that this event has a very high chance of occurrence under any circumstances. More than 90% chance of an incident.

In the event that the impact of the risk may occur in many forms, such as the risk of poor quality products, it can affect both the profit target and the reputation of the organization. The level of impact of the two factors may not be the same. In that case, assessors should use their judgment to select the most significant impacts to the activities or processes that are being assessed.

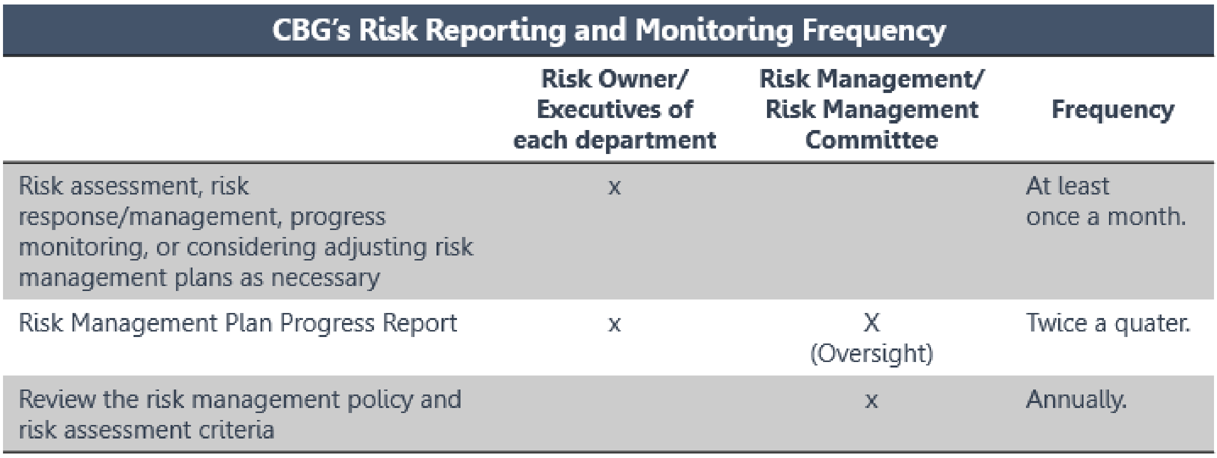
The above risk assessment criteria are established according to the risk appetite of the organization. The above evaluation criteria will be reviewed by the Risk Management Committee at least once a year.

Risk Assessment Monitoring and Reporting

For efficient risk management, continuous monitoring is required to ensure that.

- The risk management activities are executed as planned.
- Risk management results in achieving the goals and the risks are at an acceptable level. If problems are found, plans can be adjusted or additional measures can be adopted to deal with risks in a timely manner, including considering the need to review and revise strategies or business objectives.
- Potential risks are monitored on developments and trends.

Monitoring should be done regularly. The frequency of risk monitoring and reporting should be undertaken appropriately according to the nature, size, and complexity of activities in the organization. Risk reporting should be done at least quarterly. However, if it is in a high-risk situation, reporting should be made more frequently. The Risk Management Committee has set guidelines for monitoring and reporting as follows:

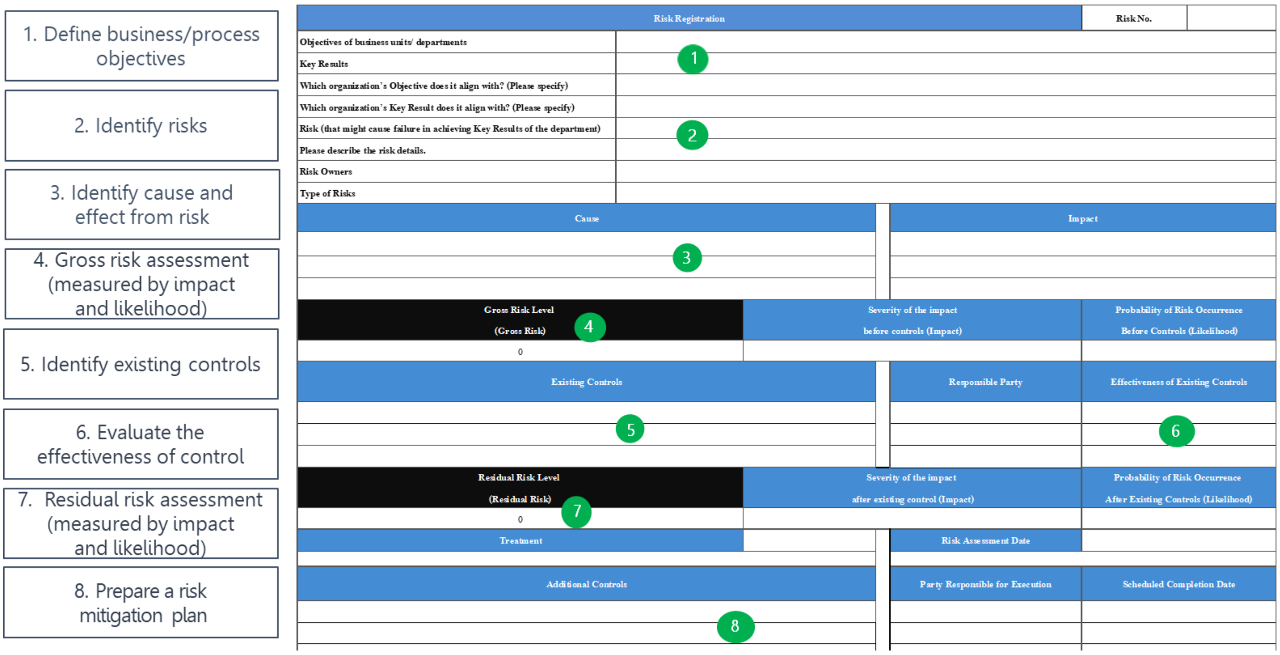


CBG's Risk Reporting and Monitoring Frequency

	Risk Owner/ Executives of each department	Risk Management/ Risk Management Committee	Frequency
Risk assessment, risk response/management, progress monitoring, or considering adjusting risk management plans as necessary	x		At least once a month.
Risk Management Plan Progress Report	x	X (Oversight)	Twice a quater.
Review the risk management policy and risk assessment criteria		x	Annually.

Tools for Risk Assessment and Risk Reporting

The risk register is the master document that each department used as the basis information for conducting each risk assessment step (8 steps) as shown in the diagram below.



1. Define business/process objectives

2. Identify risks

3. Identify cause and effect from risk

4. Gross risk assessment (measured by impact and likelihood)

5. Identify existing controls

6. Evaluate the effectiveness of control

7. Residual risk assessment (measured by impact and likelihood)

8. Prepare a risk mitigation plan

Risk Registration | Risk No.

Objectives of business units/ departments

Key Results

Which organization's Objective does it align with? (Please specify)

Which organization's Key Result does it align with? (Please specify)

Risk (that might cause failure in achieving Key Results of the department)

Please describe the risk details.

Risk Owners

Type of Risks

Cause | Impact

Gross Risk Level (Gross Risk) | Severity of the impact before controls (Impact) | Probability of Risk Occurrence Before Controls (Likelihood)

0

Existing Controls | Responsible Party | Effectiveness of Existing Controls

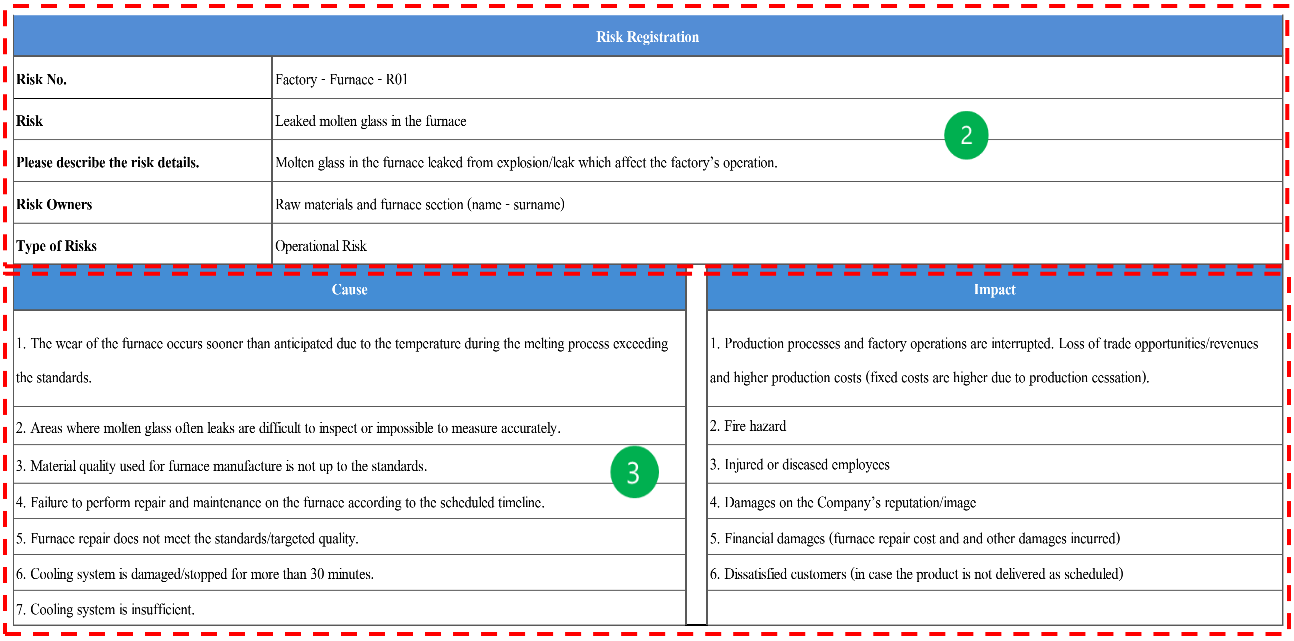
Residual Risk Level (Residual Risk) | Severity of the impact after existing control (Impact) | Probability of Risk Occurrence After Existing Controls (Likelihood)

0

Treatment | Risk Assessment Date

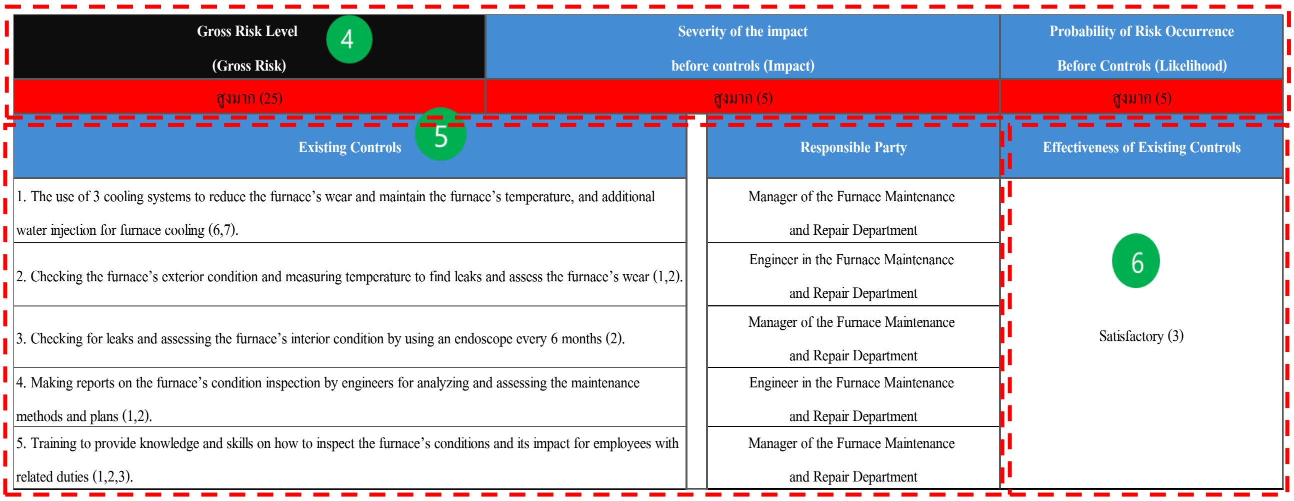
Additional Controls | Party Responsible for Execution | Scheduled Completion Date

Examples of risk assessments and recording of risk assessment information in the risk register



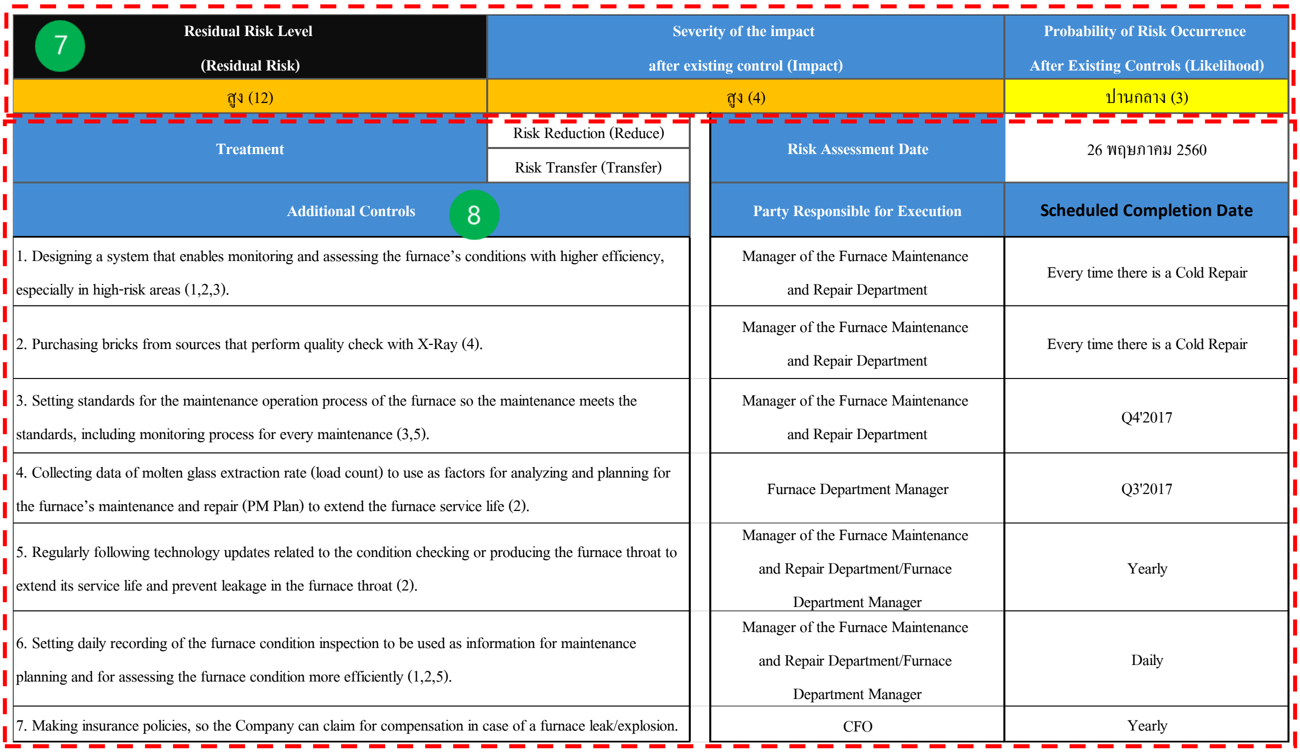
Risk Registration	
Risk No.	Factory - Furnace - R01
Risk	Leaked molten glass in the furnace
Please describe the risk details.	Molten glass in the furnace leaked from explosion/leak which affect the factory's operation.
Risk Owners	Raw materials and furnace section (name - surname)
Type of Risks	Operational Risk

Cause	Impact
1. The wear of the furnace occurs sooner than anticipated due to the temperature during the melting process exceeding the standards.	1. Production processes and factory operations are interrupted. Loss of trade opportunities/revenues and higher production costs (fixed costs are higher due to production cessation).
2. Areas where molten glass often leaks are difficult to inspect or impossible to measure accurately.	2. Fire hazard
3. Material quality used for furnace manufacture is not up to the standards.	3. Injured or diseased employees
4. Failure to perform repair and maintenance on the furnace according to the scheduled timeline.	4. Damages on the Company's reputation/image
5. Furnace repair does not meet the standards/targeted quality.	5. Financial damages (furnace repair cost and and other damages incurred)
6. Cooling system is damaged/stopped for more than 30 minutes.	6. Dissatisfied customers (in case the product is not delivered as scheduled)
7. Cooling system is insufficient.	



Gross Risk Level (Gross Risk)	Severity of the impact before controls (Impact)	Probability of Risk Occurrence Before Controls (Likelihood)
สูงมาก (25)	สูงมาก (5)	สูงมาก (5)

Existing Controls	Responsible Party	Effectiveness of Existing Controls
1. The use of 3 cooling systems to reduce the furnace's wear and maintain the furnace's temperature, and additional water injection for furnace cooling (6,7).	Manager of the Furnace Maintenance and Repair Department	Satisfactory (3)
2. Checking the furnace's exterior condition and measuring temperature to find leaks and assess the furnace's wear (1,2).	Engineer in the Furnace Maintenance and Repair Department	
3. Checking for leaks and assessing the furnace's interior condition by using an endoscope every 6 months (2).	Manager of the Furnace Maintenance and Repair Department	
4. Making reports on the furnace's condition inspection by engineers for analyzing and assessing the maintenance methods and plans (1,2).	Engineer in the Furnace Maintenance and Repair Department	
5. Training to provide knowledge and skills on how to inspect the furnace's conditions and its impact for employees with related duties (1,2,3).	Manager of the Furnace Maintenance and Repair Department	



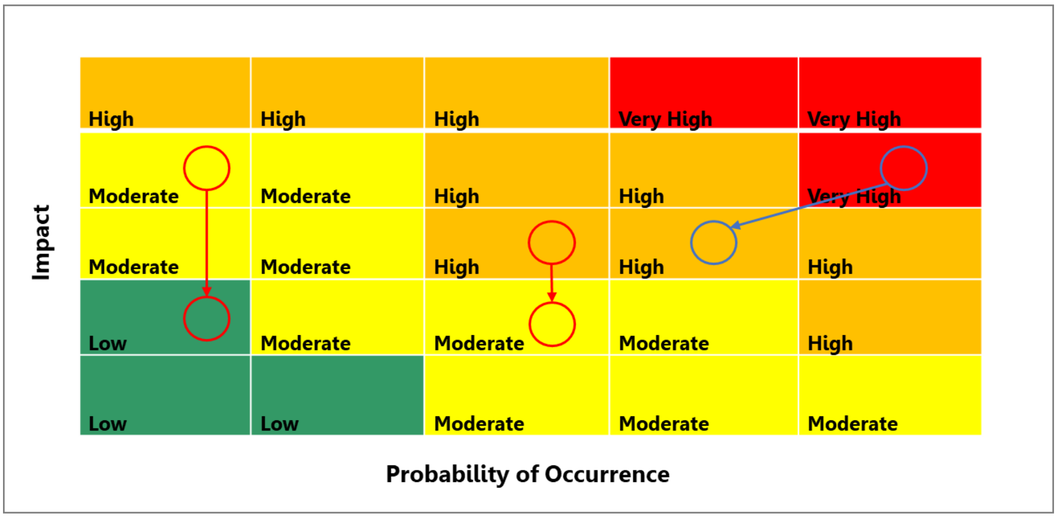
7 Residual Risk Level (Residual Risk)	Severity of the impact after existing control (Impact)	Probability of Risk Occurrence After Existing Controls (Likelihood)
สูง (12)	สูง (4)	ปานกลาง (3)

Treatment	Risk Reduction (Reduce) Risk Transfer (Transfer)	Risk Assessment Date	26 พฤษภาคม 2560

Additional Controls 8	Party Responsible for Execution	Scheduled Completion Date
1. Designing a system that enables monitoring and assessing the furnace’s conditions with higher efficiency, especially in high-risk areas (1,2,3).	Manager of the Furnace Maintenance and Repair Department	Every time there is a Cold Repair
2. Purchasing bricks from sources that perform quality check with X-Ray (4).	Manager of the Furnace Maintenance and Repair Department	Every time there is a Cold Repair
3. Setting standards for the maintenance operation process of the furnace so the maintenance meets the standards, including monitoring process for every maintenance (3,5).	Manager of the Furnace Maintenance and Repair Department	Q4'2017
4. Collecting data of molten glass extraction rate (load count) to use as factors for analyzing and planning for the furnace’s maintenance and repair (PM Plan) to extend the furnace service life (2).	Furnace Department Manager	Q3'2017
5. Regularly following technology updates related to the condition checking or producing the furnace throat to extend its service life and prevent leakage in the furnace throat (2).	Manager of the Furnace Maintenance and Repair Department/Furnace Department Manager	Yearly
6. Setting daily recording of the furnace condition inspection to be used as information for maintenance planning and for assessing the furnace condition more efficiently (1,2,5).	Manager of the Furnace Maintenance and Repair Department/Furnace Department Manager	Daily
7. Making insurance policies, so the Company can claim for compensation in case of a furnace leak/explosion.	CFO	Yearly

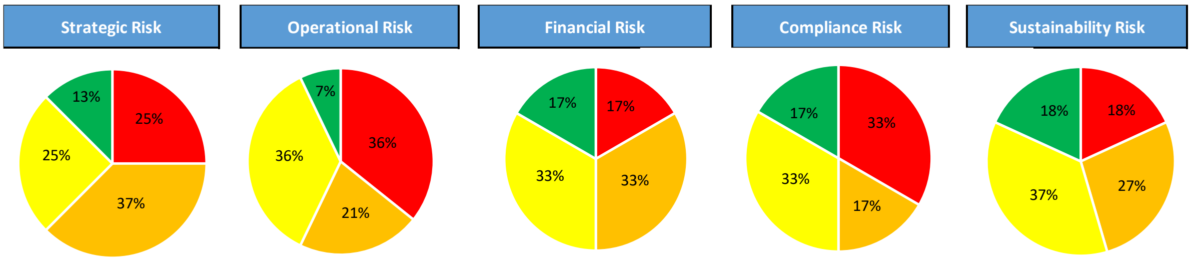
In addition to the risk register, management may choose to use other tools for reporting and monitoring risks, for example:

1. A risk diagram, a representation of the concentration of risks at an acceptable level for the organization or the extent exceeding the risk appetite. In addition, the risk diagram also shows the effectiveness of an organization's current internal controls, in reducing the risk level from the gross risk assessment (residual risk level).



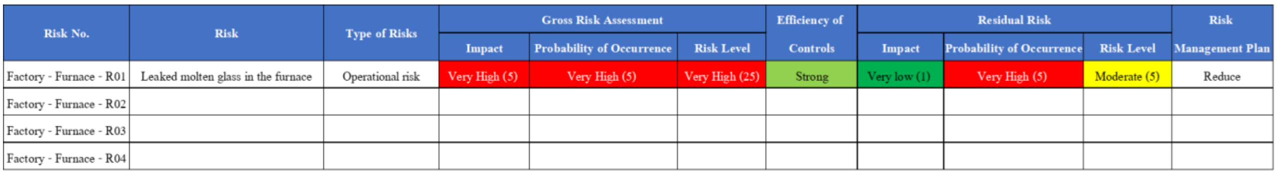
High	High	High	Very High	Very High
Moderate	Moderate	High	High	Very High
Moderate	Moderate	High	High	High
Low	Moderate	Moderate	Moderate	High
Low	Low	Moderate	Moderate	Moderate

2. The risk analysis chart is to show the risks in each type of organization (strategic risk, operational risk, financial risk, compliance risk, and sustainability risk). Executives can analyze the risks of each type of organization and risks that are beyond the risk appetite to find appropriate solutions to manage.



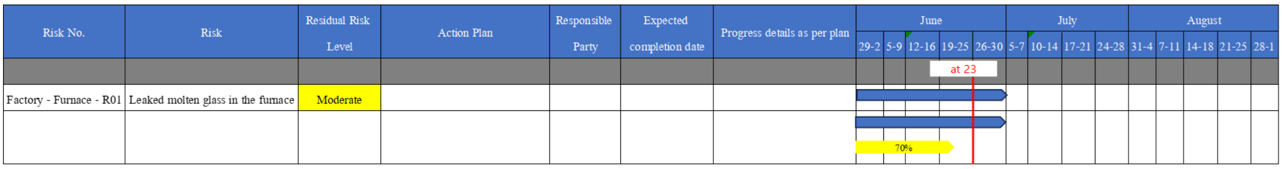
Residual Risk Level		Residual Risk Level		Residual Risk Level		Residual Risk Level		Residual Risk Level		Total
Very High	2	Very High	5	Very High	1	Very High	2	Very High	2	12
High	3	High	3	High	2	High	1	High	3	12
Moderate	2	Moderate	5	Moderate	2	Moderate	2	Moderate	4	15
Low	1	Low	1	Low	1	Low	1	Low	2	6
Risk amount	8	Risk amount	14	Risk amount	6	Risk amount	6	Risk amount	11	45

3. The risk summary report is a summary of the risk assessment results of each risk in the form of a table which consists of risk names, risk types, gross risk levels, the effectiveness of the existing internal control, the level of residual risk, and how to manage risks.



Risk No.	Risk	Type of Risks	Gross Risk Assessment			Efficiency of	Residual Risk			Risk
			Impact	Probability of Occurrence	Risk Level	Controls	Impact	Probability of Occurrence	Risk Level	Management Plan
Factory - Furnace - R01	Leaked molten glass in the furnace	Operational risk	Very High (5)	Very High (5)	Very High (25)	Strong	Very low (1)	Very High (5)	Moderate (5)	Reduce
Factory - Furnace - R02										
Factory - Furnace - R03										
Factory - Furnace - R04										

4. Report on Monitoring Risk Management Plan



Risk No.	Risk	Residual Risk Level	Action Plan	Responsible Party	Expected completion date	Progress details as per plan	June					July				August				
							29-2	5-9	12-16	19-25	26-30	5-7	10-14	17-21	24-28	31-4	7-11	14-18	21-25	28-1
										at 23										
Factory - Furnace - R01	Leaked molten glass in the furnace	Moderate																		
									70%											

Reference

Risk Register

Risk Register_template.xl

Risk Monitoring and Risk Reporting Form

Risk Monitoring_templat